Dissertation

AASA
(Analysis, Assess, Security and Awareness)

A protocol for
Network Security Assessment Methodology

Hemanta Raj Baral
(www.hemantabaral.com)

Stu_Ref_No. **0925055**, E-mail: **hemantabaral@yahoo.com**

Under the supervision of,
Mike Smith
Supervisor (MSc in Computer Network Security)

In partial fulfillment of the requirements
for the Degree of MSc in Computer Network Security

Anglia Ruskin
University

Anglia Ruskin University
Chelmsford, United Kingdom
www.anglia.ac.uk

Submission Date: **21 May 2010**

[Word Counts: 24,985]

ABSTRACT

With the increase of hacking, different attacks, viruses, worms and other networking threats, security is a major problem in today's networks. 10, 15 years ago, security was a simple issue requiring simple solutions. In those days, the internet was small and had only a small number of businesses, organizations, universities and government agencies connected to it. Aging passwords were used to protect accounts, and simple packet-filtering firewalls were used to restrict traffic flows.

The emergence of the internet, the proliferation of software applications, and the ingenuity of hackers, security has become a complex problem and it requires a well-thought-out security solution to deal with it. The security solution must be capable of dealing with the security threats that the networking system will face.

To secure the information and the entire network system, one specific methodology is required which can be capable of providing the complete security solution.

Bearing this fact in mind, a network security assessment protocol called **AASA (Analysis, Assess, Security and Awareness)** is designed, which is helpful to analyze, assess the network security vulnerabilities, secure the network system and provide an essential awareness to the network security people.

A – Analysis : helps to identify network vulnerabilities, threats and loopholes
Tools: Penetration Testing, Vulnerability Scanner

A – Assess : helps to assess network vulnerabilities, threats and attacks
Tools: Nmap, Superscan, GFI Languard, Nessus etc…

S – Security : helps to mitigate the network risks
Tools: Different preventive and mitigation techniques

A – Awareness : provides awareness, precautions, and risk management techniques to the network security people

This protocol outlines a basic network security assessment protocol including the use of no-cost supplementary network security tools in an effort to build a universal network security protocol that is affordable and executable by everyone from the basic user to network security engineer.

The main purpose of this case-study research is to provide a complete roadmap to the network security people to analyze, assess and secure the network system by implementing this proposed protocol **AASA** in the live scenario (CASE-STUDY) to prove its effectiveness with the help of freely available network security tools. It also provides the essential awareness, precautions and security tips to the network users.

Once this research is completed, there will be a specific security assessment methodology, called AASA, in hand which will be the complete roadmap for network security people to carry out the complete security process of the entire network.

ACKNOWLEDGEMENT

I was very interested in the field of Information Communication and Technology (ICT) from my childhood and have been learning computer studies since 1992. Since that time I was very curious about the new development in the field of ICT. I have also written some computer operation manuals in the field of computer software and hardware/networking using my own experience and knowledge without any proper education. During that period, all the time my dream was to get a higher education in the UK because of its high academic standard and internationally recognized qualifications.

Today, I am on the way to achieve my destination. Anglia Ruskin University is fulfilling my dream; thank you Anglia.

I would like to thank Mr. Mike Smith, supervisor of my dissertation, for his great support and proper guidelines. Without his support it was almost impossible.

I am thankful to Stratford College London and all the staffs for the great support which can not be expressed in words. I got good support from them to complete my dissertation and also they helped me a lot providing the platform to conduct my research.

The final tribute and greatest appreciation, however, is reserved for my wife RANJU; without her persuasion, cooperation and timely help, this dissertation would not have seen the light of day.

Although every care has been taken to check for errors, yet it is difficult to claim perfection. I beg your pardon if there are any mistakes.

Thank you.

Hemant

Hemanta Baral
0925055/MSc in Computer Network Security
Anglia Ruskin University

21st May 2010

To my Parents,
Gurus and
beloved wife

Permission letter from Stratford College London

Table of Contents

ABSTRACT

ACKNOWLEDGEMENT

INTRODUCTION......1

What is AASA?......2

Analysis:......2

Assess:......2

Security:......2

Awareness:......2

What other models exist?......2

Why AASA?......4

Objectives of this research......5

Literature review......7

Network Security, its importance and purpose......7

What is Network Security?......7

Importance of Network Security......7

Purpose and goal of Network Security......7

Network Security Factors......8

1. Vulnerabilities......8
2. Threats......9

2.1. Threats to Physical Infrastructure......9

2.2. Threats to Networks......10

3. Attacks......11

Classification of Attacks......11

Active Attack......11

Passive Attack......12

Types of Attacks......12

3.1 Reconnaissance/Network Enumeration (Preliminary Survey)......12

3.2 Access Attacks (Hacking/Cracking)......14

3.3 Spoofing Attacks......17

3.4 Dos/DDoS Attacks......21

3.5 Malicious Code (Malware) Attacks......25

Social engineering......**30**

Attackers Profile (categories)......31

1. White Hat......31
2. Black Hat......31

2.1 Cracker......31

3. Hacker (Sneaker)......31

3.1 Hacktivist......32

4. Spammer 32
5. Phisher (phishing – social engineering) 32
6. Phreaker 32
7. Script Kiddie 32

Network Infrastructure 33
Computer Networks based upon geographical area 33
1. LAN (Local Area Network) 34
2. MAN (Metro Area Network) 36
3. WAN (Wide Area Network) 36
Network topologies 39
1. BUS Network 39
2. STAR Network 40
3. RING Network 40
4. MESH Network 41
5. TREE or HIERARCHICAL Network 41

Computer Network Devices and Transmission Media 42
Network Interface Card (NIC) 42
Hub/Switches 43
MoDem 43
Router 44
Firewall 45
Repeaters 46
Bridges 47
Data transmission media 48
Electrical: 48
Radio or Microwave 50
Infra-Red/Bluetooth 50

Open System Interconnection Reference Model 51
High Level Protocols 52
Medium Level Protocols 52
Low Level Protocols 52
1. Application Layer (Layer 7) 52
2. Presentation Layer (Layer 6) 53
3. Session Layer (Layer 5) 53
4. Transport Layer (Layer 4) 54
5. Network Layer (Layer 3) 55
6. Data Link Layer (Layer 2) 56
7. Physical Layer (Layer 1) 57
Function of OSI Model 58

RESEARCH METHODOLOGY **59**
Deductive Approach 59
Inductive Approach 59

AASA (Analysis, Assess, Security & Awareness) **60**
1. Analysis 60
A. Identifying assets and a security perimeter 60
B. Identifying the area of threats and creating a list 61
C. Identifying Vulnerabilities 61
D. Prioritizing Assets & Vulnerabilities 62
2. Assess 62
Vulnerability Assessment Methodology: 62
Assessing the Network Risk 63
a. Discovery 63
b. Device profiling 64
c. Scanning 64
d. Validation 64
3. Security 64
4. Awareness 65
NO-COST Network Security Tools: **65**

CASE-STUDY **67**

Implementation of AASA protocol (Stratford College London) **68**

1. ANALYSIS **68**
Penetration Testing 69

2. ASSESS **74**
PING 74
TRACEROUTE (TRACERT) 77
IPCONFIG 78
NSLOOKUP 79
NETSTAT 80
Nmap 81
Zenmap 83

3. SECURITY **87**
1. Developing a Security Policy 87
2. Security of Physical threats 88
a. Physical threat mitigation 88
b. Environmental threat mitigation 88
c. Electrical threat mitigation 88
d. Maintenance threat mitigation 89
3. Data Security 89
4. Application Security 90
5. Network Security 90
Protect yourself from 92
1. How to protect your system from crimeware? 92

2. How to protect your system from hackers? 92
3. How to protect from a phishing attack? 93
4. How to protect from Spam? 94
5. How to protect from Identity Theft? 95
6. To protect against malicious code attacks: 96
Securing wireless network 96

4. AWARENESS 98
How to choose secure passwords? 98
How to keep your passwords safe? 98
Top Security vulnerabilities 98
Common security lapses 99
Mistakes made by Users 99
Mistakes made by Senior Executives 99
Network Administration Tips 100
Things to know about network administration 103

FINDINGS AND CONCLUSION 104

RECOMMENDATION 106

REFERENCES/BIBLIOGRAPHY

INTRODUCTION

The advancement in technology has led humanity to a sophisticated culture. Now, everyone wants everything sitting at home. Nobody wants to join the long queue for buying products, banking transaction, paying bills and so on. They do not want to waste their time. Similarly, on the other hand, most of the businesses, organizations are trying to provide their services quickly and effectively using ONLINE and SECURE systems as per customers' demand and interests. Faster internet services and secure networking systems have become the backbone of every modern business and organization. So, the security of each and every piece of information is very essential these days.

Securing information is not an easy task due to the different threats, vulnerabilities, exploits and loopholes. The key for building a secure network is to define what security means to the organization. Many businesses and organizations pay lip service to security, and do not want to be bothered with it when it gets in their way. It is important to build systems and networks in such a way that the user is not constantly reminded of the security system around them.

Network security means to secure electronic data while **stored in networked computers** or, **transmitted through networks** from vulnerabilities, threats, attacks and exploits.

The main goal of network security is

> **"To give people the freedom of using and enjoying computer networks without fear of compromising their rights and interests." (**Wang, 2009)

This goal can be achieved by providing Confidentiality, Integrity, and Availability of useful data that are stored in networked computers and transmitted in open networks.

Confidentiality Data cannot be read by any unauthorized users during transmission and storage state.

Integrity Data cannot be modified or fabricated by any unauthorized user during transmission or storage in a local device or networked devices.

Availability Data always should be available for authorized users.

To achieve this goal, Network Security Personnel must be familiar with different types of network security factors like network vulnerabilities, all kinds of threats, exploits, attacks and their impacts. Along with this, they should know the security procedure and the precautions required for the whole process.

So, one proper and specific methodology is important to secure the entire network system effectively for network security people. Without a well defined methodology, it is difficult to achieve the desired goal. **Keeping these facts in mind, this specific Network Security Assessment protocol called AASA is designed.**

What is AASA?

AASA Defined;

Analysis: Identifying assets & security perimeters, identifying threats & creating list, identifying vulnerabilities and prioritizing assets & vulnerabilities.

Assess: Assessing network security **Vulnerabilities** (Technological, Configuration, Security Policy Weaknesses), **Threats** (Human: Unstructured, Structured, Internal, External; Physical: Hardware, Maintenance, Natural, Environmental), **Attacks** (Reconnaissance/Network Enumeration, Access Attacks – Hacking/Cracking, DoS/DDoS attacks, Malicious Code attacks).

Security: Securing the system using different preventive and mitigation techniques

Awareness: To provide the essential awareness about the security system to the Network Administrators and Security Engineers. It includes precautions, acceptance, avoidance and, transference techniques.

What other models exist?

1. **'Vulnerability Assessment: Towards an Integrated Security Infrastructure'**

   - C. Onwubiko, A. Lenaghan

   Proceedings of the 1st International Conference on Computer Science & Information Systems (ICCSIS 2005)

   Computer Science and Informaiton System ATINER, June, Athens, Greece, pp. 157-172. ISBN/ISSN 960-88672-3-1 (2005)

   Onwubiko and Lenaghan (2005) in their research paper state:

   > *"A security vulnerability methodology is developed which is use in an integrated security infrastructure to conduct security vulnerability assessment that assists in countering emerging intrusive security threats. An integrated security infrastructure is a unified approach composed of detector, analysis and response capabilities, that aid to collectively*

> *gather, analyse and counter threats coming from multiple distributed attack sessions. Central to the Integrated Security Infrastructure is a security vulnerability evaluation, which classifies threats and recommends appropriate countermeasures. The vulnerability evaluation methodology is developed using OCTAVE – Operationally Critical Threat, Asset, and Vulnerability Evaluation….."*

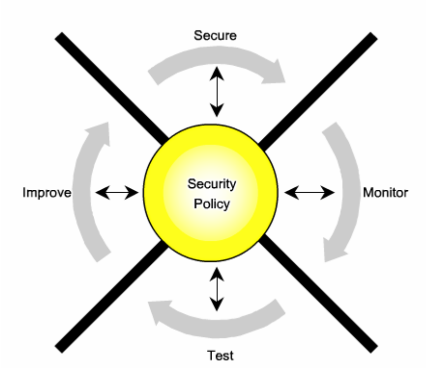
2. B.A.S.E – A Security Assessment Methodology

Prepared By: Gregory Braunton
GSEC Practical Assignment Version 1.4b, Option 1
Submitted September 29th, 2004
© SANS Institute

Braunton (2004) in his research paper states:

> *"A fundamental tenet of security is that a chain is only as strong as its weakest link and a wall is only as strong as its weakest point. Smart attackers are going to seek out that weak point and concentrate their attentions there ……*
>
> *….. The purpose of this case study, then, is to propose and practically apply an elementary information security assessment protocol called BASE. BASE stands for **B**aseline, **A**udit and Assess, **S**ecure, **E**valuate and Educate. It outlines a basic Information Assurance (IA) vulnerability assessment protocol including the use of supplementary no-cost tools in an effort to build a universal information security "forge" that is affordable and executable by everyone from the home user to enterprise security engineer. The goal of all this? To evangelize the concepts of BASE to strengthen the collective security posture of the Internet."*

3. CISCO Network Security Wheel



Source:*http://netlab.anglia.ac.uk/uc/en_EWAN_v40_Linux/theme/cheetah.html?cid=140000000&l1=en&l12=none&chapter=1*

This security model states that –

"To begin the Security Wheel process, first develop a security policy that enables the application of security measures. A security policy includes the following:

- *Identifies the security objectives of the organization.*
- *Documents the resources to be protected.*
- *Identifies the network infrastructure with current maps and inventories.*
- *Identifies the critical resources that need to be protected, such as research and development, finance, and human resources.*

The security policy is the hub upon which the four steps of the Security Wheel are based. The steps are secure, monitor, test, and improve.

Step 1: Secure

Secure the network by applying the security policy…

Step 2: Monitor

Monitoring security involves both active and passive methods of detecting security violations. The most commonly used active method is to audit host-level log files. Most operating systems…….

Step 3: Test

In the testing phase of the Security Wheel, the security measures are proactively tested. Specifically…

Step 4: Improve

The improvement phase of the Security Wheel involves analyzing the data collected during the monitoring and testing phases. This analysis contributes …..."

(http://netlab.anglia.ac.uk/uc/en_EWAN_v40_Linux/theme/cheetah.html?cid=140000000&l1=en&l12=none&chapter=1 [Accessed May 19, 2010])

Why AASA?

AASA covers all the network security elements required for the whole security process. It starts from analyzing network security factors after then assessing the network security vulnerabilities and then securing the system and finally ends with providing the essential awareness to the network security personnel.

The other (above mentioned) models cover the following areas:

Vulnerability Assessment: Towards an Integrated Security Infrastructure only covers detecting, analyzing and responding to the network security vulnerabilities

B.A.S.E – A Security Assessment Methodology provides the Baseline of network security factors, Audit & Assessing the risks, Secure and Evaluate the risks & Educate the users.

CISCO Network Security Wheel covers securing network by applying security policy, monitoring the security violation, testing the security measures and finally improves after analyzing the data collected during the monitoring and testing phase.

Objectives of this research

The main objective of this case study research is to implement the concept of AASA to develop a network security framework which helps to strengthen the collective security posture of the computer network.

Inside this project

Besides Abstract and the Introduction sections, there are Literature Review, Methodology, Findings/Conclusion and Further Recommendation sections.

LITERATURE REVIEW section provides the details about:

Network Security, its importance and purpose

Network Security Factors

1. Vulnerabilities
2. Threats
3. Attacks

Types of Attacks

Reconnaissance/Network Enumeration (Preliminary Survey)

Access Attacks (Hacking/Cracking)

Spoofing Attacks

Dos/DDoS Attacks

Malicious Code (Malware) Attacks

Social engineering

Attackers Profile (categories)

Network Infrastructure

Categories of Computer Network

Types of Computer Networks based up on geographical area

Network Topologies

Computer Network Components and Transmission Media

Network Interface Card (NIC)

HUB

SWITCH

MoDem

Router

Firewall

Repeaters

Bridges

Open System Interconnection Reference Model

1. Application Layer (Layer 7)
2. Presentation Layer (Layer 6)
3. Session Layer (Layer 5)
4. Transport Layer (Layer 4)
5. Network Layer (Layer 3)
6. Data Link Layer (Layer 2)
7. Physical Layer (Layer 1)

Function of OSI Model

In the METHODOLOGY section,

- Implementation of AASA in the live scenario is discussed.
- **CASE STUDY** of Stratford College London on the basis of AASA protocol using freely available network security tools. and;
- Basic network security techniques and required precautions/awareness to be taken by the network security professional are discussed in this chapter.

Finally, the FINDINGS/CONCLUSION section gives the output and brief summary of the overall research project.

LITERATURE REVIEW

This section covers:

Network Security, its importance and purpose

- What is Network Security?
- Importance of Network Security
- Purpose and goal of Network Security

Network Security Factors

1. Vulnerabilities
2. Threats
3. Attacks

- Types of Attacks
    - 3.1 Reconnaissance/Network Enumeration (Preliminary Survey)
    - 3.2 Access Attacks (Hacking/Cracking)
    - 3.3 Spoofing Attacks
    - 3.4 Dos/DDoS Attacks
    - 3.5 Malicious Code (Malware) Attacks
- Social engineering

Attackers Profile (categories)

Network Infrastructure

- Computer Networks based upon geographical area
    1. LAN (Local Area Network)
    2. MAN (Metro Area Network)
    3. WAN (Wide Area Network)
- Network topologies

Computer Network Devices and Transmission Media

Open System Interconnection Reference Model

1. Application Layer (Layer 7)
2. Presentation Layer (Layer 6)
3. Session Layer (Layer 5)
4. Transport Layer (Layer 4)
5. Network Layer (Layer 3)
6. Data Link Layer (Layer 2)
7. Physical Layer (Layer 1)

- Function of OSI Model

Network Security, its importance and purpose

What is Network Security?

Network security refers to any activities designed to protect your network. It consists of the technologies and processes that are deployed to protect networks from internal and external threats. Network security involves all activities that organizations, enterprises, and institutions undertake to protect the value and ongoing usability of assets and the integrity and continuity of operations. Effective network security targets a variety of threats and stops them from entering or spreading on your network.

Importance of Network Security

Network security is important for a variety of reasons. First of all, it is important to ensure that the company's reputation will not be marked by a security breach leaking customer's information. Large, small, known and unknown companies are all at risk to an attack led by a hacker. One security breach and the reputation of the company can immediately take a turn for the worse. Once a company is educated about their network's strengths and weaknesses, they will gain a better understanding of areas they may be at risk to an attack and be able to take appropriate measures to pinpoint areas where security needs to be reinforced.

Network Security helps to protect the network and the network-accessible resources from unauthorized access, and consistent and continuous monitoring and measurement of its effectiveness (or lack) combined together.

Purpose and goal of Network Security

The primary goal of network security is to provide controls at all points along the network perimeter which allow access to the network and only let traffic pass if that is authorized, valid and of acceptable risk.

The purpose of network security is to protect networks, network devices and network messages from unauthorized access, usually by outsiders.

Objective 1: To provide control at all points along the network perimeter in order to block network traffic that is malicious, unauthorized or that otherwise presents risk to the network.

Objective 2: To detect and respond to attempted and actual intrusions through the network.

Objective 3: To prevent network messages that is sent across networks from being intercepted or modified.

Network security controls cannot completely eliminate risk. The goal is to minimize risk as much as possible and to avoid unnecessary or excessive risk. The goal of network security is really to 'enable' network connectivity. Without network security, the risks/costs of network connectivity would be very expensive.

Network Security Factors

Vulnerabilities || Threats || Attacks

1. Vulnerabilities

What is vulnerability?

"Weakness in an information system that enables an attack."
(Aura T., Microsoft Research, UK)

Vulnerability is a weakness which allows an attacker to unauthorized access to other's system to reduce system's Information Assurance. Vulnerability is the intersection of three elements: a system flaw (gap/weakness), attacker access to the flaw (gap), and attacker capability to exploit the flaw i.e. use that gap for attacker's benefit.

There are four primary causes for network security threats:

1.1. Technological Weaknesses

Computer and network technologies have basic security weaknesses in the following areas:

- TCP/IP
- Operating System
- Network equipments like switches, routers, firewalls etc…

1.2. Configuration Weaknesses

Many security problems are often caused by the following configuration weaknesses:

- Unsecured accounts
- System accounts with weak passwords
- Misconfigured Internet services
- Misconfigured network equipments

1.3. Security Policy Weaknesses

Security problems can be caused by security policy weaknesses:

- Lack of a written security policy
- Politics – politics clash and staff conflicts
- Frequent replacement of personnel
- Software and hardware installation/changes do not follow policy
- Lack of Disaster recovery plan

1.4. Human Error

Human/user error is a large cause of breaches of network security. If staff tells confidential information to friends, family or other coworkers, security has been breached. Unauthorized access to networks can be gained in many different ways:

- Accident
- Ignorance
- Workload
- Dishonesty
- Impersonation
- Dissatisfied employees

2. Threats

What are Threats?

Bad event that might happen.

Threats are the people interested and qualified in taking advantage of each security weakness. Such individuals can be expected to continually search for new exploits and weaknesses.

The threats use a variety of tools, scripts, and programs to launch attacks against networks and network devices. Typically, the network devices under attack are the endpoints, such as servers and desktop computers.

2.1. Threats to Physical Infrastructure

When you think of network security, or even computer security, you may imagine attackers exploiting software vulnerabilities. A less glamorous, but no less important, class of threat is the physical security of devices. An attacker can deny the use of network resources if those resources can be physically compromised.

The four classes of physical threats are:

2.1.1. Hardware threats

Hardware threats are simply the threat of physical damage to physical infrastructure such as servers, routers, switches, cabling plant, and workstations etc…

2.1.2. Environmental threats

Not only do you need to secure your systems from human interference, but you also need to secure them from the interference of natural disasters such as fires, hurricanes, tornados, and flooding, which fall under the realm of environmental threat. Environmental issues also come from extreme temperature (too hot or too cold) or humidity (too wet or too dry).

2.1.3. Electrical threats

Electrical vulnerabilities are seen in things such as spikes in voltage to different devices and hardware systems, or brownouts due to an insufficient voltage supply. Electrical threats also come from the noise of unconditioned power and, in some extreme circumstances, total power loss.

2.1.4. Maintenance threats

Maintenance threats are due to poor handling of key electrical and electronic components, which cause ESD (electrostatic discharge), the lack of critical spare parts, poor cabling, poor device labeling etc…

2.2. Threats to Networks

Network security threats can be categorized as external versus internal and unstructured versus structured.

2.2.1. Internal threats

An internal security threat occurs when someone from inside your network creates a security threat to your network. Interestingly, the CSI (Computer Security Institute) study has found that, of the 70 percent of the companies that had security breaches, 60 percent of these breaches come from internal sources. Some of these security breaches were malicious in intent; others were accidental.

2.2.2. External threats

External threats can arise from individuals or organizations working outside of a company who do not have authorized access to the computer systems or network. They work their way into a network mainly from the Internet or dialup access servers. External threats can vary in severity depending on the expertise of the attacker-either amateurish (unstructured) or expert (structured).

2.2.3. Unstructured threats

Unstructured threats are not organized and do not target a specific host, network, or organization.

An unstructured security threat is one created by an inexperienced person who is trying to gain access to your network. A good security solution easily should thwart this kind of attack.

2.2.4. Structured threats

Structured threats are organized efforts to attack a specific target.

Structured threats come from individuals or groups that are more highly motivated and technically competent. They break into business and government computers to commit fraud, destroy or alter records, or simply to create destruction.

3. Attacks

Someone intentionally causes the bad thing to happen.

Common methods of attacks

a. **Reconnaissance/ Network Enumeration**
Discovering information about the intended target.

b. **Vulnerabilities Analysis**
Identifying potential ways of attacks.

c. **Exploitation**
Attempting to compromise the system by employing the vulnerabilities found through the vulnerabilities analysis. In other words, the act of using something in a cruel manner.

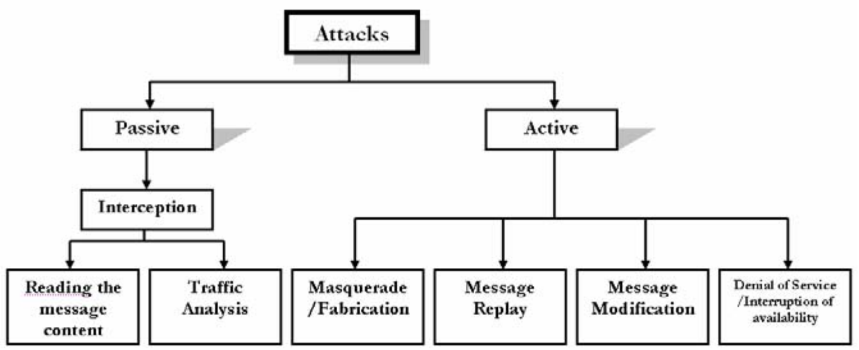
Classification of Attacks

In general, attacks on data networks can be classified as either **active** or **passive**.

Active Attack

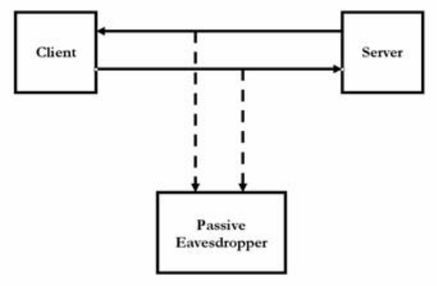
An active attack is one in which an unauthorized change of the system is attempted. This could include, for example, the modification or deletion of transmitted or stored data, or the creation of new data streams. This is one of the most serious forms of attack since many companies' operations critically depend on data.

Masquerade or Fabrication, Message Replay, Message Modification and Denial of Service or Interruption of Availability; are some types of active attacks.



Passive Attack

A **passive attack** is characterized by the interception of messages without modification. There is no change to the network data or systems. An unauthorized can go into a computer network which reads the data passing along some of the transmission line without modifying it. The message itself may be read or its occurrence may simply be logged. Identifying the communicating parties and noting the duration and frequency of messages can be of significant value in itself. From this knowledge certain deductions or inferences may be drawn regarding the likely subject matter, the urgency or the implications of messages being sent. This type of activity is termed traffic analysis. Because there may be no evidence that an attack has taken place, prevention is a priority.



Types of Attacks

3.1 Reconnaissance / Network Enumeration (Preliminary Survey)

Reconnaissance is the unauthorized discovery and mapping of systems, services, or vulnerabilities. It is also known as information gathering and, in most cases, it precedes another type of attack. Reconnaissance is similar to a thief casing a neighborhood for vulnerable homes to break into, such as an unoccupied residence, easy-to-open doors, or open windows.

Common tools, commands, and utilities that are used for scanning and enumeration include ping, Telnet, nslookup, finger, rpcinfo, File Explorer, srvinfo, and dumpacl. Other third-party public tools include Sniffer, SATAN, SAINT, NMAP, and netcat. In addition, custom scripts are used in this process.

Reconnaissance attacks can consist of the followings:

- Internet information queries
- Ping sweeps (Address Sweeps)
- Port scans
- Packet sniffing (Information Gathering, Information Theft)

3.1.1 Internet Information Queries

Internet Information means to determine IP addresses and all the details of any organization, corporation, firms or entities. Free Internet tools or commands such as the nslookup, ipconfig and whois utilities are used to easily determine the IP address and all the details assigned to a given corporation or entity. Once Internet Information is determined, the intruder uses ping sweeps methods - ping (fping, gping) to identify active IP addresses.

Tools: WHOIS (http://www.whois.net/, http://whois.domaintools.com/)
Nslookup
IPconfig, IPconfig/all

3.1.2 Ping Sweeps

Ping sweeps principally is intended to discover whether specific Internet Protocol addresses in the network are associated with active computers. As a legitimate network management technique, this can be part of network discovery. To monitor the use of address space allocations, the address registries that allocate the addresses may scan organizations to see if they are using all their space, a scarce resource with Internet Protocol version 4.

Once the active IP addresses are identified, the intruder uses a port scans (nmap, superscan) to determine which network services or ports are active on the live IP addresses. It helps to identify the open ports, versions, operating systems etc…

Tools: PING (fping, gping)
Nslookup
IPconfig, IPconfig/all

3.1.3 Port Scans

Port scanning actually covers a wide range of activities involving sending a stimulus to the Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) identifiers of specific services on specific computers. If a ping sweep is analogous to checking if a building exists at a given street address, a port scan is closer to testing the doors to see if they are locked, or at least to see if specific apartments or rooms exist.

Tools: Nmap (www.nmap.org)
Superscan/Fport (www.foundstone.com)

3.1.4 Packet Sniffing (Packet Analyzing) - Eavesdropping

"Sniffing" is observing packets passing by on a network. Sniffing is a popular way to steal data from a network, usually in form of passwords, ID names, etc. The person who is sniffing a network obtains data by actually sniffing the network for packets. The data is usually cached thus hackers look for user ID and the password of a legitimate user and uses the user's information to log on to the network. Once logged into the network, the hacker sniffs transmissions of packets. With this method the hacker can gather needed information about the network.

Packet sniffing is a method of capturing all of the data packets, which can be used to capture important valuable information like username, password, IDs etc... A "Packet Sniffer" is a utility that sniffs without modifying the network's packets in any way. Packet sniffers merely watch, display, and log this traffic.

Two common uses of eavesdropping are as follows:

- **Information gathering -** Network intruders can identify usernames, passwords, or information carried in a packet.
- **Information theft -** The theft can occur as data is transmitted over the internal or external network. The network intruder can also steal data from networked computers by gaining unauthorized access. Examples include breaking into or eavesdropping on financial institutions and obtaining credit card numbers.

Tools: wireshark (www.wireshark.org)
Snort (www.snort.org)

3.2 Access Attacks (Hacking/Cracking)

System access is the ability for an intruder to gain access to a device for which the intruder does not have an account or a password. Entering or accessing systems usually involves running a hack, script, or tool that exploits a known vulnerability of the system or application being attacked.

Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services to gain entry to web accounts, confidential databases, and other sensitive information.

3.2.1 Password attacks (Dictionary or Brute-force attacks)

A password attack is indicated by a series of failed logins within a short period of time by an attacker. Typically a user will get a note on screen regarding how many failed attempts have been at your account: If there is a series of failed attempts that you do not remember then it is quite probable that the attacker successfully reached your account. In the event of this happening, you should immediately change your password. These repeated attempts are called dictionary attacks or brute-force attacks.

To conduct a dictionary attack, attackers can use tools such as L0phtCrack or Cain. These programs repeatedly attempt to log in as a user using words derived from a dictionary. Dictionary attacks often succeed because users have a tendency to choose simple passwords that are short, single words or are simple variations that are easy to predict, such as adding the number 1 to a word.

Another password attack method uses rainbow tables. A rainbow table is pre-computed series of passwords which is constructed by building chains of possible plaintext passwords. Each chain is developed by starting with a randomly selected "guess" of the plaintext password and then successively applying variations on it. The attack software will apply the passwords in the rainbow table until it solves the password. To conduct a rainbow table attack, attackers can use a tool such as L0phtCrack.

A brute-force attack tool is more sophisticated because it searches exhaustively using combinations of character sets to compute every possible password made up of those characters. The downside is that more time is required for completion of this type of attack. Brute-force attack tools have been known to solve simple passwords in less than a minute. Longer, more complex passwords may take days or weeks to resolve.

Tools: Cain and Abel (www.oxid.it)
John the Ripper (www.openwall.com/john)
L0phtcrack (www.l0phtcrack.com)
Rainbow Table

3.2.2 Trust Exploitation

The goal of a trust exploitation attack is to compromise a trusted host, using it to stage attacks on other hosts in a network. If a host in a network of a company is protected by a firewall (inside host), but is accessible to a trusted host outside the firewall (outside host), the inside host can be attacked through the trusted outside host.

3.2.3 Port redirection

A port redirection attack is another type of attack based on trust exploitation. The attacker uses a compromised host to gain access through a firewall that would otherwise be blocked.

Look at it this way; the host on the outside can get to the host on the public services segment, but not the host on the inside. If an intruder is able to compromise the host on the public services segment, the attacker could install software to redirect traffic from the outside host directly to the inside host. Although neither communication violates the rules implemented in the firewall, the outside host has now achieved connectivity to the inside host through the port redirection process on the public services host. An example of a tool that can provide this type of access is **Netcat.**

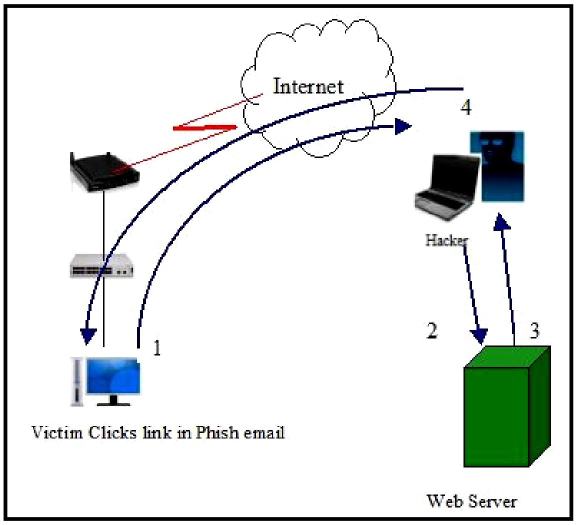
Tools: Serial Port Redirector

3.2.4 Man in the middle attack (Spoofing)

A man in the middle attack is one in which the attacker intercepts messages in a public key exchange and then retransmits them, substituting his own public key for the requested one, so that the two original parties still appear to be communicating with each other.

A man-in-the-middle (MITM) attack is implemented by intruders that manage to position themselves between two legitimate hosts. The attacker may allow the normal communication between hosts to occur, but manipulates the conversation between the two. There are many ways that an attacker gets position between two hosts. A very good example is called the transparent proxy. The attacker prey their victims by sending a phishing email or by defacing a legitimate website. When the victim loads the URL of a defaced webpage, the attackers URL is added to the front of it.

For example: let say http://www.hemantabaral.com / is a legitimate URL. But when website's URL is hacked it becomes http://www.theattacker.com/ http://www.hemantabaral.com



Source: *http://www.orbit-computer-solutions.com/Man-in-the-Middle-Attack.php*

1. When a victim requests a webpage, the host of the victim makes the request to the host of the attacker's.
2. The attacker's host receives the request and fetches the real page from the legitimate website.
3. The attacker can alter the legitimate webpage and apply any transformations to the data they want to make.
4. The attacker forwards the requested page to the victim.

Man-in-the middle attacks have a variety of applications, including:

- Web spoofing
- TCP session hijacking
- Information theft
- Many other attacks, including denial-of-service attacks, corruption of transmitted data, or traffic analysis to gain information about the victim's network.

Man-in-the middle attacks can be accomplished using a variety of methods (any person that has access to network packets as they travel between two hosts can accomplish these attacks):

- ARP poisoning
- ICMP redirects
- DNS poisoning

3.3 Spoofing Attacks

Spoofing is a method of attacking a network in order to gain unauthorized access.

In a spoofing attack, the intruder sends messages to a computer indicating that the message has come from a trusted system. To be successful, the intruder must first determine the IP address of a trusted system and then modify the packet headers to that it appears that the packets are coming from the trusted system.

In essence, the attacker is fooling (spoofing) the distant computer into believing that they are a legitimate members of the network. The goal of the attack is to establish a connection that will allow the attacker to gain root access to the host, allowing the creation of a backdoor entry path into the target system.

There are mainly FOUR types of Spoofing Attacks. They are:

- IP Address Spoofing
- ARP Poisoning
- WEB Spoofing
- DNS Spoofing

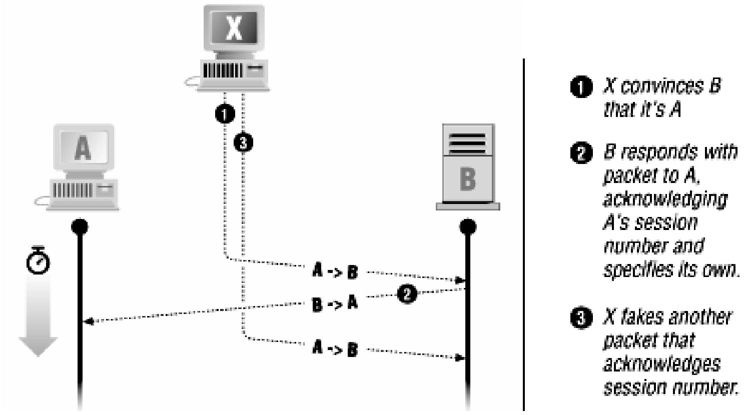
3.3.1 IP Address Spoofing

All computers connected to the Internet are identified to accessed websites by a unique number known as an IP address. This allows websites to identify the computer connected to that website, but access can also be denied by blocking that particular IP address, or the block of IP addresses into which it falls. IP spoofing allows people to log onto a website with a different IP address if they find an IP block has been placed on their connection, by using a Proxy Server.

In other words, IP address spoofing (IP spoofing) refers to the creation of Internet Protocol (IP) packets with a forged source IP address, called spoofing, with the purpose of concealing the identity of the sender or impersonating another computing system.

In this attack,

1. The attacker identifies a target, the victim of the attack, and a machine that is trusted by the victim.
2. The attacker disables the trusted machine's ability to communicate by flooding it with SYN packets.
3. The attacker uses some mechanism to determine the sequence numbers to be used by the victim. This could involve sampling packets between the victim and trusted hosts.
4. The attacker spoofs the source IP address of the trusted host in order to send his or her own packets to the victim.
5. The victim accepts the spoofed packet and responds. Although the network infrastructure automatically routes the victim's reply packets to the trusted host, the trusted host is unable to process the packets because of the SYN flood attack against it.
6. Blind to the victim's response, the attacker must guess its contents and craft an appropriate response, again using a spoofed source address and a guessed sequence number.


X
A
B
1
3
A -> B
B -> A
2
A -> B
1 X convinces B that it's A
2 B responds with packet to A, acknowledging A's session number and specifies its own.
3 X fakes another packet that acknowledges session number.

Source: *http://oreilly.com/catalog/crime/chapter/f_02_05.gif*

Tools: SpoofMAC, Macspoofing, TotalSpoof etc.

3.3.2 ARP Poisoning

Address resolution protocol (ARP), is used on LANs to map a host's IP address with its physical address (also known as a MAC address).

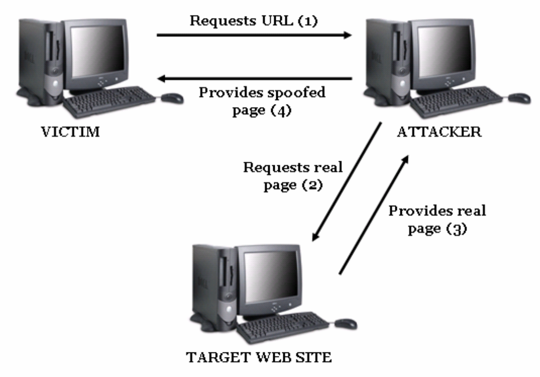
ARP spoofing involves constructing forged ARP replies. By sending forged ARP replies, a target computer could be convinced to send frames destined for computer A to instead go to computer B. When done properly, computer A will have no idea that this redirection took place. The process of updating a target computer's ARP cache with a forged entry is referred to as "poisoning".

Tools: ARPoison
Parasite
Ettercap (http://ettercap.sourceforge.net/)

These tools are able to spoof ARP packets to perform man-in-the-middle attacks, redirect transmission, or to simply intercept packets.

3.3.3 WEB Spoofing (Phishing)

Web spoofing allows an attacker to create a "shadow copy" of the entire World Wide Web. Accesses to the shadow Web are funneled through the attacker's machine, allowing the attacker to monitor the all of the victim's activities including any passwords or account numbers the victim enters. The attacker can also cause false or misleading data to be sent to Web servers in the victim's name, or to the victim in the name of any Web server. In short, the attacker observes and controls everything the victim does on the Web.

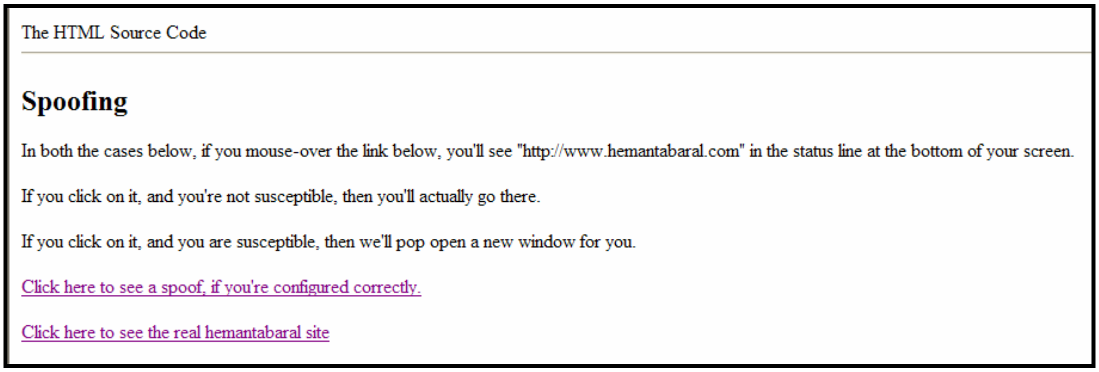


Example of WEB Spoofing

Web spoofing Demonstration

```
<HTML>
    <HEAD>
    .. <TITLE>Web Spoofing Demonstration</TITLE>
    </HEAD>
<BODY onload=init()>
    <HR>
    <H2>Spoofing</H2>
<P>In both the cases below, if you mouse-over the link below,
you'll see "http://www.hemantabaral.com" in the status line at
the bottom of your screen.
<P>If you click on it, and you're not susceptible, then you'll
actually go there.
<P>If you click on it, and you are susceptible, then we'll pop
open a new window for you.

<P><A onclick="return openWin();
"href="http://www.hemantabaral.com/"> Click here to see a
spoof, if you're configured correctly.</A></P>
<P><A onclick="javascript:openRealWin();return false;"
href="http://www.hemantabaral.com/">Click here to see the real
hemantabaral site</A></P>
<P>
</BODY>
</HTML>
```

Output



The HTML Source Code

Spoofing

In both the cases below, if you mouse-over the link below, you'll see "http://www.hemantabaral.com" in the status line at the bottom of your screen.

If you click on it, and you're not susceptible, then you'll actually go there.

If you click on it, and you are susceptible, then we'll pop open a new window for you.

Click here to see a spoof, if you're configured correctly.

Click here to see the real hemantabaral site

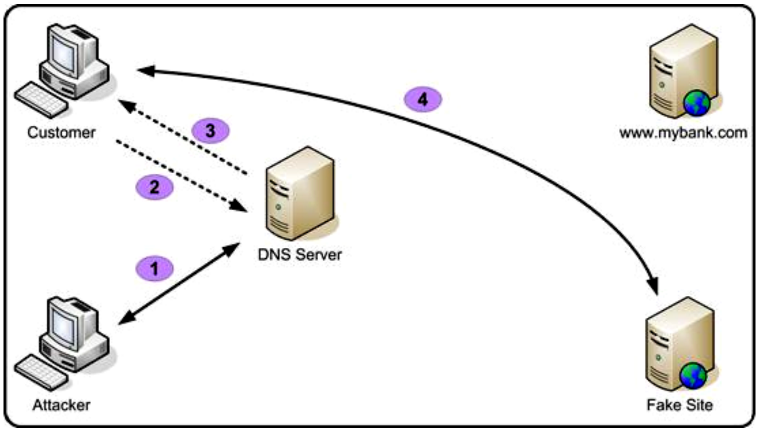
3.3.4 DNS Spoofing

DNS spoofing has similar effects and objectives as Web spoofing. It can be used to direct users to a compromised server where they enter sensitive information, or it can be used to redirect corporate e-mail through a hacker’s server where it can be copied or modified before sending the mail on to its final destination.

DNS spoofing is accomplished in one of the following three ways:

- The attacker compromises the victim organization’s Web server and changes a hostname-to-IP address mapping. When users request the hostname, they are directed to the hacker’s server, rather than the authentic one.
- Using IP spoofing techniques, the attacker’s DNS server instead of an organization’s real DNS server answers lookup requests from users. Again, the hacker can direct user lookups to the server of his or her choice instead of to the authentic server.

- When the victim organization's DNS server requests lookups from authoritative servers, the attackers "poisons" the DNS server's cache of hostname-to-IP address mappings by sending false replies. The organization's DNS server stores the invalid hostname-to-IP address mapping and serves it to clients when they request a resolution.



Source: *http://www.technicalinfo.net/papers/images/pharming030.jpg*

3.4 Dos/DDoS Attacks

A Denial-of-Service (DoS) attack is designed to hinder or stop the normal functioning of a web site, server or other network resource. There are various ways for hackers to achieve this. One common method is to flood a server by sending it more requests than it is able to handle. This will make the server run slower than usual (and web pages will take much longer to open), and may crash the server completely (causing all websites on the server to go down).

Denial of service (DoS) is when an attacker disables or corrupts networks, systems, or services with the intent to deny services to intended users. DoS attacks involve either crashing the system or slowing it down to the point that it is unusable. But DoS can also be as simple as deleting or corrupting information. In most cases, performing the attack involves simply running a hack or script. For these reasons, DoS attacks are the most feared.

It is important to note the difference between a DDoS and DoS attack. If an attacker mounts an attack from a single host it would be classified as a DoS attack. In fact, any attack against availability would be classed as a Denial of Service attack. On the other hand, if an attacker uses a thousand systems to simultaneously launch smurf attacks against a remote host, this would be classified as a DDoS attack.

A DoS attack can be perpetrated in a number of ways. The five basic types of attack are:

1. Consumption of computational resources, such as bandwidth, disk space, or processor time
2. Disruption of configuration information, such as routing information.
3. Disruption of state information, such as unsolicited resetting of TCP sessions.
4. Disruption of physical network components.
5. Obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

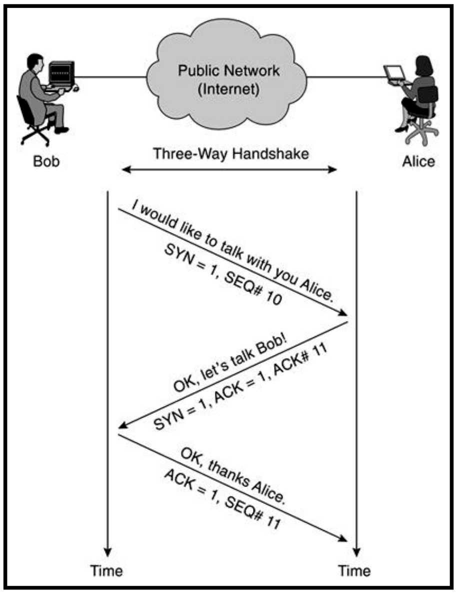
3.4.1 SYN Flood

A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system. When a client attempts to start a TCP connection to a server, the client and server exchange a series of messages which normally runs like this:

1. The client requests a connection by sending a SYN (synchronize) message to the server.
2. The server acknowledges this request by sending SYN-ACK back to the client.
3. The client responds with an ACK, and the connection is established.

This is called **the TCP three-way handshake**, and is the foundation for every connection established using the TCP protocol.

The SYN flood is a well known type of attack and is generally not effective against modern networks. It works if a server allocates resources after receiving a SYN, but before it has received the ACK.

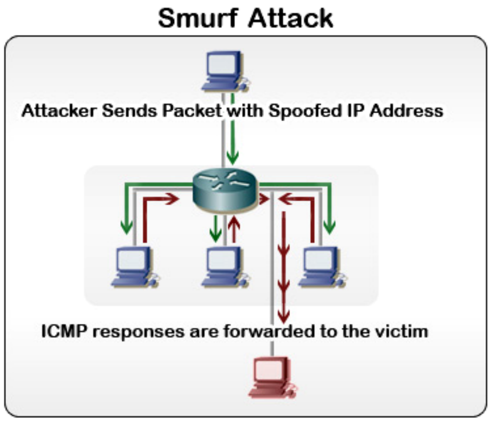


Source: *http://mudji.net/press/wp-content/uploads/2006/11/3way.JPG*

3.4.2 SMURF Attack / Fraggle Attack (ICMP/UDP Echo request - Bandwidth Consumption)

The **Smurf attack** is a way of generating significant computer network traffic on a victim network. This is a type of denial-of-service attack that floods a target system via spoofed broadcast ping messages.

Using this technique, the hacker cannot only overwhelm the computer system receiving the flood of echo packets, but the hacker can also saturate the victim's Internet connections with bogus traffic and therefore delay or prevent legitimate traffic from reaching its destination.


Smurf Attack
Attacker Sends Packet with Spoofed IP Address
ICMP responses are forwarded to the victim

Source: *http://learn-networking.com/wp-content/uploads/2008/02/smurf-attack.jpg*

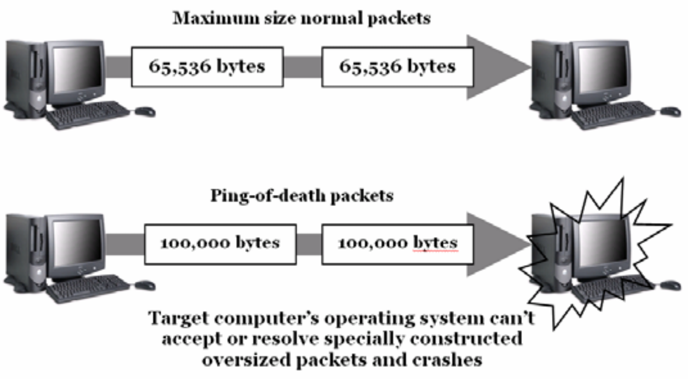
If an attacker sends a large amount of UDP echo traffic to IP broadcast addresses, all of it having a fake source address the its called a **Fraggle Attack.**

3.4.3 IP Fragmentation Attack (Ping of Death/ Ping Flood/ Buffer Overflows)

This **ping of death** is a well-known exploit that uses IP packet fragmentation techniques to crash remote systems. In this attack, the large IP packets are transmitted across networks.

The maximum size of an IP packet is 65,536 bytes, but packets that large cannot be transmitted on many network topologies. To transmit a large IP packet across a LAN, hosts and routers fragment IP packets into smaller Ethernet frames, and then reassemble the fragments at the destination. Each fragment contains an offset value that tells the receiving host where to insert its data into the reassembled packet.

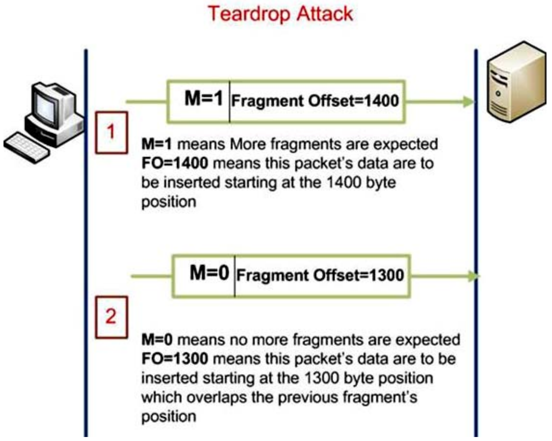
In this attack, a very large ICMP (ping) packet is crafted and transmitted to the victim, fragment by fragment. With each fragment, the size of the reassembled ping grows to near the 65,536 byte size limit of the IP packet. When the final fragment arrives, its offset value forces the packet to grow beyond the IP size limit, causing the victim host to crash.


Maximum size normal packets
65,536 bytes
65,536 bytes
Ping-of-death packets
100,000 bytes
100,000 bytes
Target computer's operating system can't accept or resolve specially constructed oversized packets and crashes

Example of Ping of Death attack

3.4.4 Teardrop Attack

A Teardrop attack involves sending mangled IP fragments with overlapping, over-sized payloads to the target machine. This can crash various operating systems due to a bug in their TCP/IP fragmentation re-assembly code.


Teardrop Attack
M=1
Fragment Offset=1400
1
M=1 means More fragments are expected
FO=1400 means this packet's data are to be inserted starting at the 1400 byte position
M=0
Fragment Offset=1300
2
M=0 means no more fragments are expected
FO=1300 means this packet's data are to be inserted starting at the 1300 byte position which overlaps the previous fragment's position

Source: *http://www.trainsignaltraining.com/wpnew/wp-content/uploads/2009/05/6.jpg*

3.4.5 DDoS Attacks

A distributed-Denial-of-Service (DDoS) attack differs only in the fact that the attack is conducted using multiple machines. The hacker typically uses one compromised machine as the 'master' and co-ordinates the attack across other, so-called 'zombie', machines. Both master and zombie machines are typically compromised by exploiting a vulnerability in an application on the computer, to install a Trojan or other piece of malicious code.

Depending on the type of agent software installed, the attacker has a number of attack types:

- **Tribe flood Network (TFN)**

  The Tribe Flood Network or TFN is a set of computer programs to conduct various DDoS attacks such as SYN flood, Smurf attack.

- **Stacheldraht**

  Stacheldraht is a classic example of a DDoS tool. It utilizes a layered structure where the attacker uses a client program to connect to handlers, which are compromised systems that issue commands to the **zombie agents*,** which in turn facilitate the DDoS attack. Agents are compromised via the handlers by the attacker, using automated routines to exploit vulnerabilities in programs that accept remote connections running on the targeted remote hosts. Each handler can control up to a thousand agents.

  * A zombie is a computer attached to the Internet that has been compromised by a hacker, a computer virus, or a trojan horse.

- **MyDoom**

  Malware can carry DDoS attack mechanisms; one of the better-known examples of this was MyDoom. Its DoS mechanism was triggered on a specific date and time. This type of DDoS involved hardcoding the target IP address prior to release of the malware and no further interaction was necessary to launch the attack.

3.5 Malicious Code (Malware) Attacks

The primary vulnerabilities for end-user workstations are malicious code attacks.

Malware, short for **mal**icious soft**ware** - is a special kind of software program or file deliberately designed to perform an unauthorized and often harmful action in a computer system. Malware includes viruses, worms, torjan horses, crimeware, adware, spyware etc…

It was once sufficient to call something a 'virus' or 'trojan horse', but infection methods and vectors evolved and the terms virus and trojan no longer provided a satisfactory definition for all the types of rogue programs that exist.

Malicious software can be inserted onto a host to damage or corrupt a system, replicate itself, or deny access to networks, systems, or services.

3.5.1 Viruses

Keep in mind that not everything that goes wrong with a computer is caused by a computer virus or worm. Both hardware and software failure is still a leading cause of computer problems.

A virus is malicious software that is attached to another program to execute a particular unwanted function on a computer system. It is a parasitic program written intentionally to alter the way your computer operates without your permission or knowledge.

A virus is a self-replicating program that spreads by inserting copies of itself into other executable code or documents on a host computer system. When one of these infected programs is run, the virus is surreptitiously activated, enabling it to infect other programs in turn. Viruses generally either cause annoyance or physically damage the infected PC.

Virus Classification

Viruses can be subdivided into a number of types,

- Boot sector viruses
- Macro viruses or file viruses
- Program viruses
- Logic bombs and time bombs etc…

- **Boot sector viruses**

A boot sector virus alters or hides in the boot sector, usually the 1st sector, of a bootable disk or hard drive. This virus attacks the vulnerable boot program that is stored on every bootable floppy disk or hard disk. This code is executed by the system when the PC is started up, making it a juicy target for virus writers: by installing themselves here they guarantee that their code will be executed whenever the system is started up, giving them full control over the system to do what they wish. They are spread most commonly through infected bootable floppy disks.

- **Macro viruses (also called File virus)**

Macro viruses are small programs that are written in the macro language of an application such as Microsoft Word, Excel and that can normally only spread within documents of this application. Because of this, they are also called document viruses. In order to be active, they need that the corresponding applications are activated and that one of the infected macros has been executed.

- **Program viruses**

These viruses directly attack and modify program files, which are usually .EXE or .COM files. When the program is run, the virus executes and does whatever it wants to do. Usually it loads itself into memory and waits for a trigger to find and infect other program files. These viruses are commonly spread through infected floppy disks, over networks, and over the Internet.

- **Logic or Time Bombs**

A **logic bomb** is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. The resolution of the conditions will trigger a certain function (such as printing a message to the user and/or deleting files). An example of a logic bomb would be a virus that waits to execute until it has infected a certain number of hosts. A *time bomb* is a subset of logic bomb, which is set to trigger on a particular date and/or time.

Many viruses attack their host systems on specific dates, such as Friday the 13th or April Fool's Day. Trojans that activate on certain dates are often called "time bombs". Some logic bombs can be detected and eliminated before they execute through a periodic scan of all computer files, including compressed files, with an up-to-date anti-virus program.

3.5.2 Worms

A **worm** executes code and installs copies of itself in the memory of the infected computer, which can, in turn, infect other hosts.

A worm is a piece of software that uses computer networks and security flaws to create copies of itself. A copy of the worm will scan the network for any other machine that has a specific security flaw. It replicates itself to the new machine using the security flaw, and then begins scanning and replicating a new.

3.5.3 Trojan Horse

A **Trojan horse** is different from a worm or virus only in that the entire application was written to look like something else, when in fact it is an attack tool.

A Trojan horse is any program that, once run, does something that the user doesn't want or request. The program doesn't necessarily infect other files or spread to other systems. It is the generic term to refer to any software that is intentionally coded to do something other than what it is supposed to. Some people think of viruses as a special form of trojan horse: one that can infect other files (thus turning them into trojan horses) and duplicate itself. Trojan horses are sometimes just called "trojans" for short.

3.5.4 Spyware

Spyware is a program that gathers information about a computer user without permission

As the name suggests, this is software that is designed to harvest your data and forward it to a third party without your consent or knowledge. Such programs may monitor key presses ('keyloggers'), collect confidential information (passwords, credit card numbers, PIN numbers, etc.), harvest e-mail addresses or track browsing habits. In addition to all of this, spyware inevitably affects your computer's performance.

- **Key loggers**

  These are programs which record key presses (i.e. what a user types on the keyboard) and can be used by a hacker to obtain confidential data (login details, passwords, credit card numbers, PINs, etc.). Backdoor Trojans typically come with an integrated keylogger.

3.5.5 Adware

Adware is the general term applied to programs that either launch advertisements (often pop-up banners) or re-direct search results to promotional web sites that appear on a computer screen. Those advertising spots usually can't be removed and are consequently always visible. The connection data allow many conclusions on the usage behavior and are problematic in terms of data security.

Adware is often built into freeware or shareware programs: if you download a freeware program, the adware is installed on your system without your knowledge or consent. Sometimes a Trojan will secretly download an adware program from a web site and install it on your computer.

3.5.6 Backdoor

A backdoor can gain access to a computer by going around the computer access security mechanisms.

A backdoor is a way of accessing a computer without going through the normal access routines such as entering a name and password. It can be installed by a virus or even by legitimate programs.

3.5.6.1 Rootkit

A rootkit is a collection of tools (programs) that enable administrator-level access to a computer or computer network. Typically, a cracker installs a rootkit on a computer after first obtaining user-level access, either by exploiting a known vulnerability or cracking a password. Once the rootkit is installed, it allows the attacker to mask intrusion and gain root or privileged access to the computer and, possibly, other machines on the network.

A rootkit may consist of spyware and other programs that: monitor traffic and keystrokes; create a "backdoor" into the system for the hacker's use; alter log files; attack other machines on the network; and alter existing system tools to escape detection.

Social engineering

Social Engineering is the act of tricking computer users into performing actions or revealing private and confidential information, e.g. passwords, email addresses, etc, by exploiting the natural tendency of a person to trust and/or by exploiting a person's emotional response. Phishing, Scamming, Spamming are some techniques used for Social Engineering.

- ### Phishing

> **"There may be no fish or rod in sight, but there is often a 'catch of the day' for criminals. Using this technique, they steal by tricking internet and email users into disclosing their personal details."** [1]

Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to attract the unsuspecting public. Phishing is typically carried out by e-mail or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

- ### Masquerading (Identity Theft)

Masquerading is the malicious theft and consequent misuse of someone else's identity to commit a crime. Identity theft often involves cracking into a system to obtain personal information, such as credit card numbers, birth dates, and social insurance or social security numbers of targets and then using this information in an illegal manner, such as buying items with the stolen identity or pretending to be someone else of higher professional status in order to gain special privileges. Identity theft is one of the fastest-growing crimes around the globe.

- ### Scamming

Scamming is the process of defrauding a person or group by gaining their confidence using some fraudulent tricks/game/scheme. Confidence men exploit human characteristics such as greed and dishonesty, and have victimized individuals from all walks of life.

[1] http://www.kaspersky.co.uk/phishing

- **Spamming**

Spamming is the act of sending a message or advertisement to a large number of people who did not request the information, or to repeatedly send the same message to a single person.

Spam is the abuse of electronic messaging systems to send unsolicited bulk messages indiscriminately. Spam is an unspecified, unsolicited (unwanted) bulk email like the physical junk mail delivered through the post. It is sent out in mass quantities by spammers who make money from the small percentage of recipients that actually respond. Spam is also used for phishing and to spread malicious code.

Attackers Profile (categories)

1. White Hat

An individual who looks for vulnerabilities in system or networks and then report these vulnerabilities to the owners of the system so that they can be fixed.

2. Black Hat

An individuals who use their knowledge of computer system to break into system or networks that they are not authorized to use, usually for personal or financial gain.

A cracker is an example of a Black Hat.

2.1 Cracker

A more accurate term to describe someone who tries to gain unauthorized access to network resources with malicious intent.

3. Hacker (Sneaker)

A general term that has historically been used to describe a computer programming experts. More recently, this term is often used in negative way to describe an individual that attempts to gain unauthorized access to network resources with malicious intent.

The term hacker was once used to describe a clever programmer. Today, it's applied to those who exploit security vulnerabilities to break into a computer system. You can think of it as electronic burglary. Hackers regularly break into both individual computers and large networks. Once they have access, they may install malicious programs, steal confidential data, or perhaps use compromised computers to distribute spam.

3.1 Hacktivist

A hacktivist is a hacker who utilizes technology to announce a social, ideological, religious, or political message. In general, most hacktivism involves website defacement or denial-of-service attacks. In more extreme cases, hacktivism is used as tool for Cyberterrorism. Hacktivists are also known as Neo Hackers.

4. Spammer

An individual who sends large quantities of unsolicited (not requested) e-mail messages using viruses programs.

5. Phisher (phishing – social engineering)

An individual who uses e-mail or other means to trick others into providing sensitive information such as credit card numbers or passwords. A phisher masquerades as a trusted party that would have a legitimate need for the sensitive information.

6. Phreaker

An individual who manipulates or breaks the phone network to make free long distance calls.

7. Script Kiddie

An immature individual who uses scripts or programs developed by others to attack computer systems and networks. Generally they are teenagers who want the power of the hacker without the discipline or training involved.

Network Infrastructure

Networking is the process of connecting one computer terminal with the others. A communication system that supports many users can be called a Network or we can say network is a communication system, which interconnects many users who have something in common, either with respect to the type of data being sent or to the geographic areas that the users cover. Networks can be used between people, between people and computers, between computers and equipment or between computers. Today, organizations use networks in all possible ways. Depending on the application, the network needs different speed, degree of reliability, and cost.

It is an interconnection between computers through physical and logical components. These components are as follows:

- Network topologies
- Cabling
- Network Interface cards
- Protocols
- Hub / Switches
- Modems
- Routers etc…

Basic components for every network:

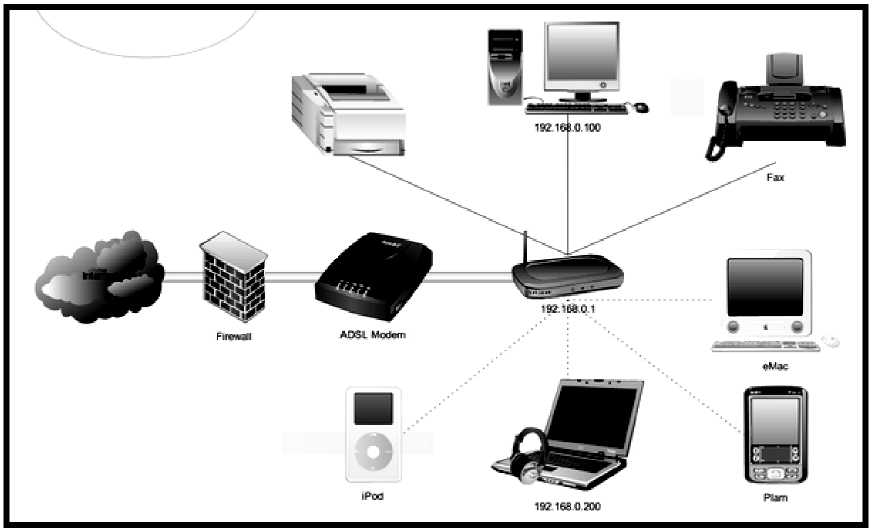
- At least two computers (Server or Client workstation)
- Network Interface Card (NIC)
- A connection medium, usually a wire (or cable), although wireless communication is possible.
- Network operating system software, such as Microsoft Windows NT/2000/2003/2008, Novell NetWare, Unix and Linux

Computer Networks based upon geographical area

1. LAN (Local Area Network)
    a. WLAN (Wireless Local Area Network)
2. MAN (Metro Area Network)
3. WAN (Wide Area Network)
    a. Internet (Interconnection network)
    b. Intranet
    c. Extranet
    d. VPN (Virtual Private Network)

1. LAN (Local Area Network)

A Local Area Network (LAN) is a network where two or more computers directly linked within a small well-defined physical area such a room, home, office building, school/campus or an airport. A LAN can be made up of microcomputers or any combination of microcomputer and large system. Main benefit of a LAN is the reduction of hardware and software cost because user can share several computers, peripheral devices such as HDD, modem, and LAN platform software. Another benefit is that the user can share the same data.

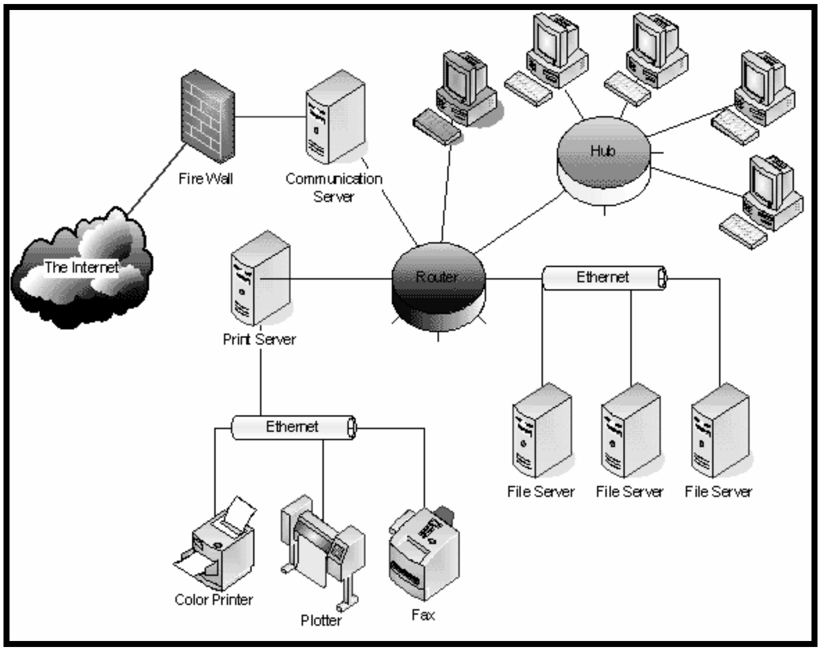


Example of Home Network (LAN)
Source: *http://www.edrawsoft.com/images/network/Wireless%20Network_Full.png*

Ethernet over twisted pair cabling, and Wi-Fi are the two most common technologies currently in use for Local Area Networking. They allow for the speedy transfer of data — up to 10Gbit/s. Most LANs are based on Ethernet technology. Wireless Local Area Networks are known as WLANs.

A LAN generally consists of the following:

1. Two or more computers.
2. A diameter of not more than few kilometers
3. Software to control the operation of the computers.
4. Peripheral devices such as modem, router etc.
5. Co-axial or fiber optic cables are usually used to connect the computers and other devices.
6. A plug in board (NIC) to handle the data transmissions.

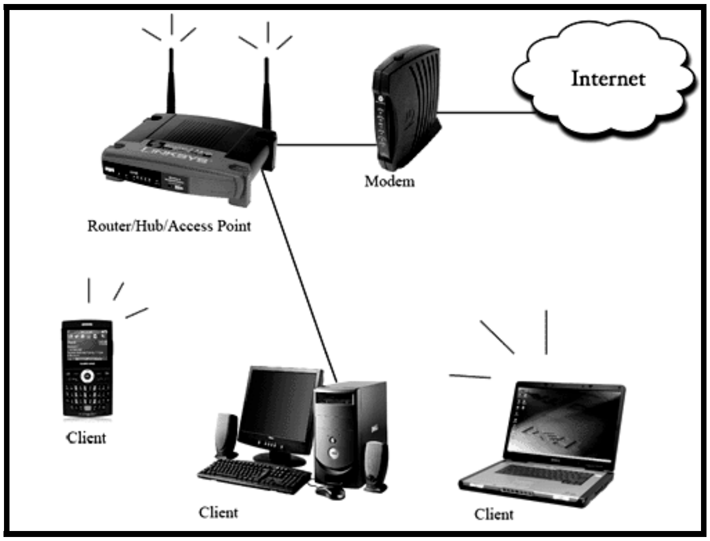


Example of simple office LAN
Source: *http://ops.fhwa.dot.gov/publications/telecomm_handbook/images/fig2-14.gif*

a. WLAN (Wireless Local Area Network)

WLANs provide wireless network communication over short distances using radio or infrared signals instead of traditional network cabling.

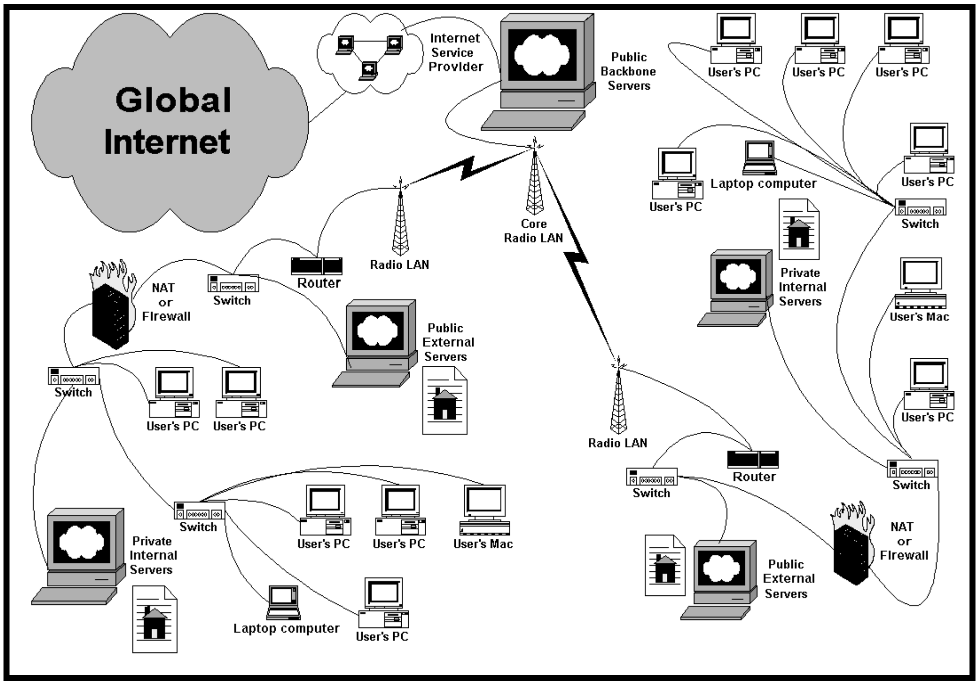
A WLAN typically extends an existing wired local area network. WLANs are built by attaching a device called the access point (AP) to the edge of the wired network. Clients communicate with the AP using a wireless network adapter similar in function to a traditional Ethernet adapter.



Example of WLAN
Source: *http://www.impulseportal.com/images/WLAN.gif*

2. MAN (Metro Area Network)

A Metropolitan Area Network (MAN) is a larger computer network than LAN that spans a metropolitan area or city. Cable Television (CATV) networks are examples of Metro Area Networking for television distribution. It is called Metropolitan since it normally covers the area of a city. It is a new physical network technology that operates at high speeds (usually hundreds of megabit per second through several gigabits per second) over distances sufficient for a metropolitan area. MAN technology has developed significantly in recent years with smaller networks within a MAN often interconnected wirelessly using radio, microwave or infra-red laser links.

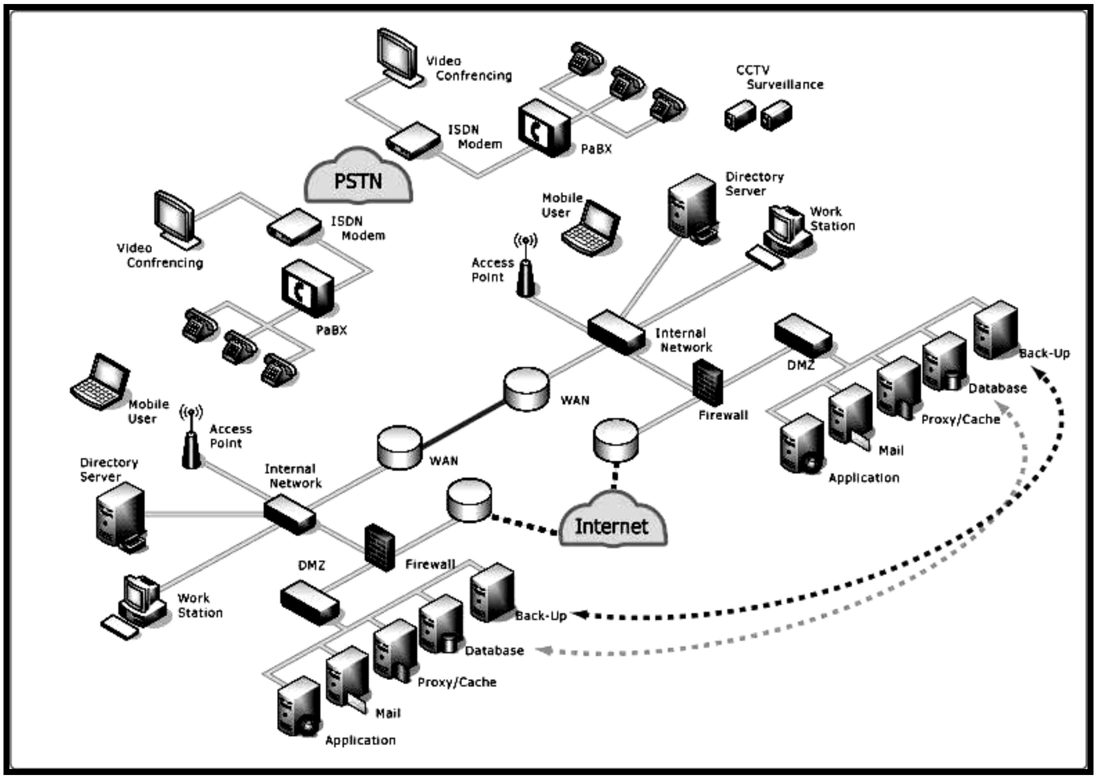


Example of MAN
Source: *http://www.overmet.net/nans/images/metro_network.gif*

3. WAN (Wide Area Network)

A Wide Area Network (WAN) is a two or more geographically isolated Local Area Network, linked by communication facilities such as telecommunication (dedicated leased phone lines, dial-up phone lines, satellite links or data packet carrier services). It covers a broad area and large distances such as states, countries, continents.

In other words one of the most significant aspects of a Wide Area Networking while comparing it with freedom of local area network is the involvement of public telecommunications authority. WAN is usually limited to use by large organization and government agencies due to high costs involved in building and maintaining them. A Wide Area Network (WAN) typically consists of TWO or more LANs. The computers are farther apart and are linked by telephone lines, dedicated telephone lines, or radio waves. The **Internet** is the largest Wide Area Network (WAN) in existence.



Example of WAN
Source: *http://www.viadex.com/img/WAN.jpg*

a. Internet (Interconnection network)

Internet is the largest computer network system in the world. It is a global network of computer networks. Millions of Computers around the world can share information at the same time by using this worldwide network system. The Internet is an ocean of information accessible to people across the world, but the way it can be used on various platform is different.

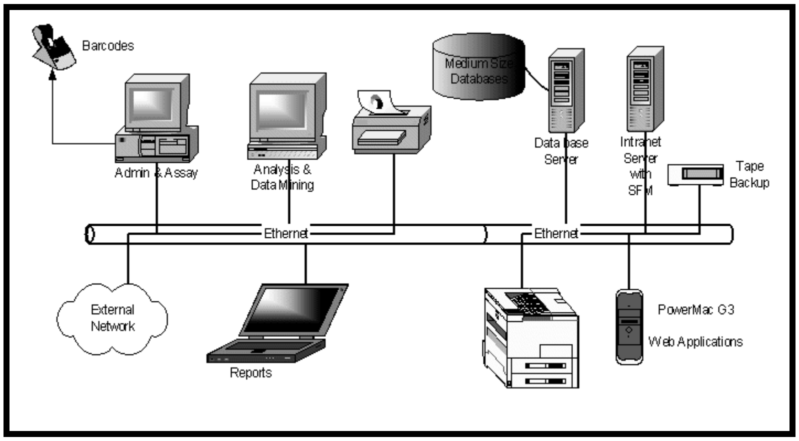
b. Intranet

"An internet-based technologies within an organization to facilitate communication and access to information." OR 'The corporate 'information network'.

An intranet is a set of networks, using the Internet Protocol and IP-based tools such as web browsers and file transfer an application, which is under the control of a single administrative entity. That administrative entity closes the intranet to all but specific, authorized users. Most commonly, an intranet is the internal network of an organization. A large intranet will typically have at least one web server to provide users with organizational information.

How Intranet differ from Internet?

- An intranet has common IP protocol suite with the internet but offers significant differences
- Packets are private rather than public
- More focused Enterprise based management
- Stronger policies and a controlling organisation
- Cost borne by single organisation
- Stronger enforcement of policies
- More control of the network

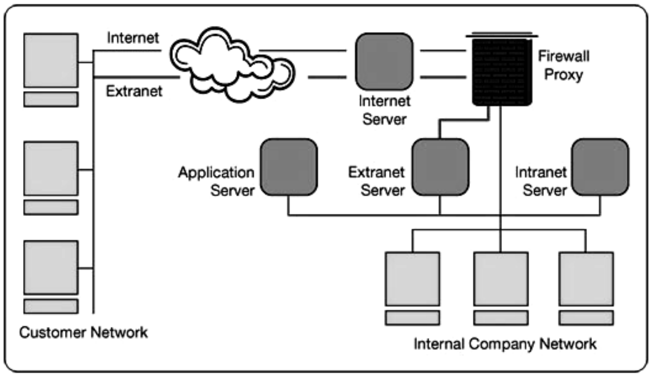


Example of Intranet
Source: *http://www.bioxing.com/images/Research%20HW%20System%20with%20Intranet.gif*

c. Extranet

An extranet is similar to an intranet but it is made accessible to selected external partners such as business partners, suppliers, key customers etc… for exchanging data and applications and sharing information.

As with an intranet, an extranet can also provide remote access to corporate systems for staff that spends lots of time out of the office, for instance those in sales or customer support, or home workers.

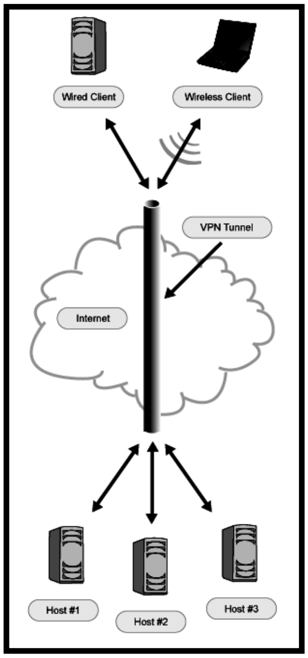


Example of Extranet
Source: *http://www.weldingandgasestoday.org/content/2q09/images/extranet/extranet.jpg*

d. VPN (Virtual Private Network)

A virtual private network (VPN) is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. A virtual private network can be contrasted with an expensive system of owned or leased lines that can only be used by one organization. The goal of a VPN is to provide the organization with the same capabilities, but at a much lower cost.

Example of VPN ➔



Source: *http://www.sonic.net/features/vpn/vpn-diagram-vertical-shorte.gif*

Network topologies

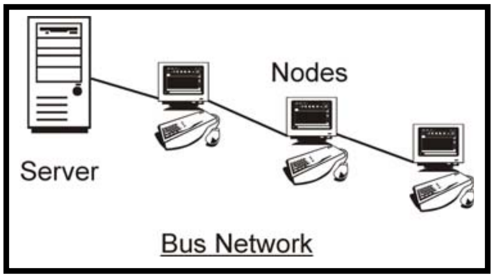
Network topology is the physical interconnections of the elements (links, nodes etc.) of a computer network. On the base of topology used, computer networks can be classified as:

1. BUS Network
2. STAR Network
3. RING Network
4. MESH Network
5. TREE or HIERARCHICAL Network

1. BUS Network

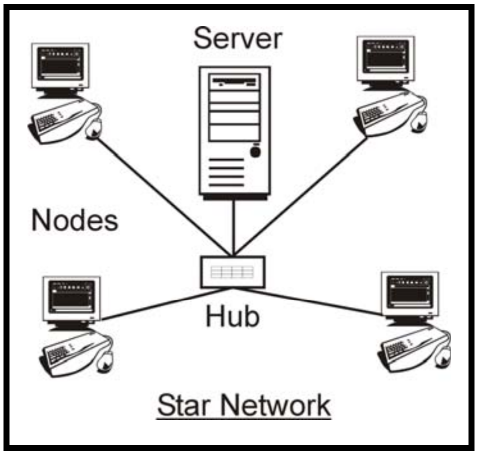
The simplest and easiest topology to implement a bus network consists of a single cable to which the client Computers and servers connect.

A bus network has open end. Each PC is connected to the network via a network card. Each peripheral, such as printers, can also be added to the network. Each connected computer or peripherals is called terminal or node. Each end of the network is connected by a terminating resistor, which prevents signal interference. The most common example of this type of network is Ethernet network.



2. STAR Network

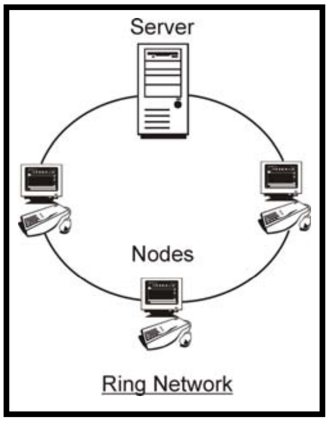
In a star network, several devices or computer are connected to one centralized computer as shown in figure. The advantage of star networks is that none of the other computer can communicate with each other if the central computer breaks down. If it is desired to transmit information from one computer to another. Only sending the details the central computer can do it, which in turn send them to the destination. A star network is used in banking sector for centralized record keeping in an on-line office environment.



A star network has characteristic that make it more efficient that bus or token ring networks. Data exchanges are better organized and more efficient, because they are supervised by a controller. Furthermore, because each node is linked to the controller by a different cable, there's risk of collision. However, this type of architecture is more expensive: it requires extra cables and a controller. To optimize the function of a network without incurring exorbitant costs, several Network Architecture can be used at the same time. Then the various networks can be linked by an inter-networks link.

3. RING Network

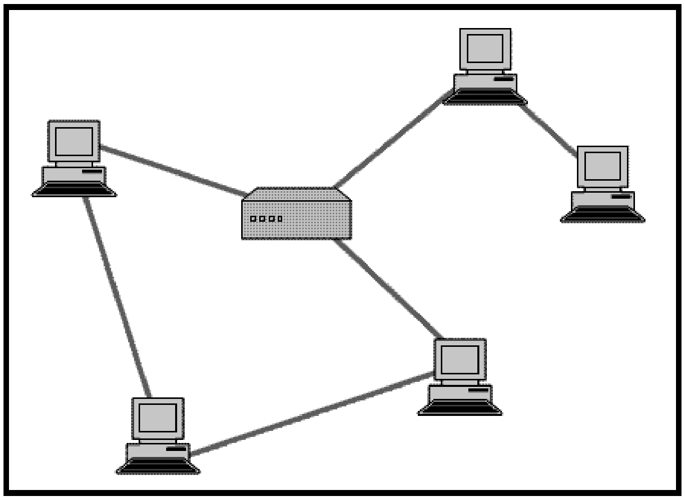
A Ring network is form of circle, at least as for as the nodes are concerned. Network transmissions travel from node to node, in one direction only, in a closed, round robin loop. When a transmission has traveled the full circuit, it has moved from the node that started the transmission to the Computer connected to that node and so on until it has gone around the loop and returned to the starting node.



4. MESH Network

Mesh topologies involve the concept of routes. Unlike each of the previous topologies, messages sent on a mesh network can take any of several possible paths from source to destination. (Recall that even in a ring, although two cable paths exist, messages can only travel in one direction.) Some WANs, most notably the Internet, employ mesh routing.

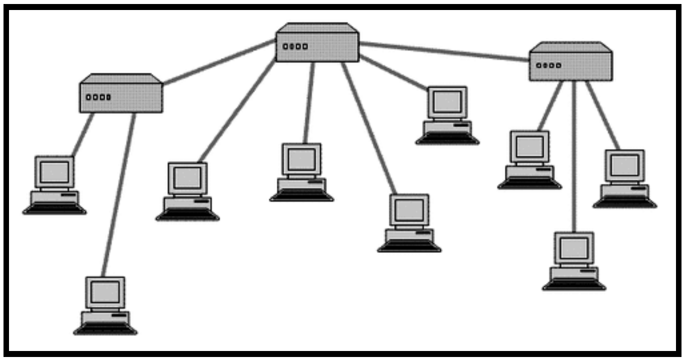
A mesh network in which every device connects to every other is called a full mesh. As shown in the illustration below, partial mesh networks also exist in which some devices connect only indirectly to others.



Example of MESH Network

5. TREE or HIERARCHICAL Network

In a tree network, several devices or computer are linked in a hierarchical fashion as shown in figure. Tree network is also known as Hierarchical network. This type of distribution system is commonly used in the organization where headquarters communicate with regional office and regional offices communicate with district offices & so on.



Example of TREE or HIERARCHICAL Network

Computer Network Devices and Transmission Media

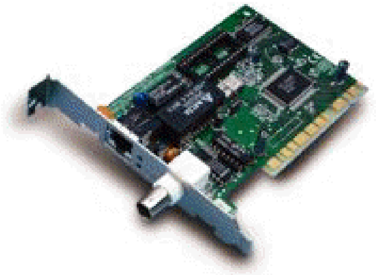
- NIC (Network Interface Card)
- HUB/Switches
- MoDem
- Routers
- Firewalls
- Repeaters
- Bridges
- Cables/Jack

Network Interface Card (NIC)–Wired or Wireless (Wi-Fi)

A NIC or Network Interface Card is a circuit board or chip, which allows the computer to communicate to other computers on a Network. The best means of connecting a computer to a network is through a Network Interface Card (NIC). A NIC will allow a computer to send and receive electrical or radio signals in a manner that other computers can understand. Most modern computers come with Ethernet NICs installed by default. Laptops usually even come with wireless NICs.

NIC provides the hardware interface between a computer and a network. Most NICs support either wired Ethernet or WiFi wireless standards. Ethernet NICs plug into the system bus of the PC and include jacks for network cables, while WiFi NICs contain built-in transmitters / receivers (transceivers). All NICs feature a speed rating such as 11 Mbps, 54 Mbps or 100 Mbps that suggest the general performance of the unit.

Network cards are required in every machine connected to the network. They allow the signal from the network to be transmitted to the machine – this could be via a fixed cable, infra red or radio waves.



A network card that uses a standard cable network socket.

A Wi-Fi network card with an external aerial for the signal.

Hub / Switches

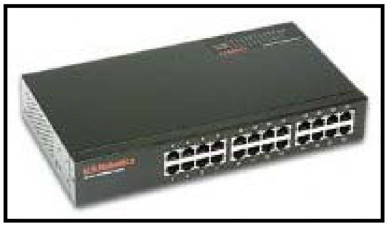
HUB

In order to connect more than two computers together, a device that distributes packets, or blocks of data, must be used. A hub is the most basic of these devices. When a computer connected to a network makes a request for data from another computer, that request will be sent to the hub. The hub will then send that request to every computer it is connected to, including the originating computer. Most of the computers on the network will ignore the request. The computer that the request is being sent to will accept the data packet and send out a reply packet. The reply packet will then be sent to every computer by the hub. One problem with hubs is that they often cause collisions between packets. As a result, data is lost in transmission and must be re-sent.

The network 'Hub' allows computers to share data packets within a network.

SWITCH

A switch is a device that distributes packets, or blocks of data, between computers in a network. Switches function in a similar fashion to hubs, but are much more efficient. A switch can send a packet directly to a specific destination, instead of sending it to every computer in a network.



A network cable can only have one data packet in it at any instant. So if two or more computers want to place a data packet on to the network at exactly the same time, then a 'data collision' will take place. The network protocol is set up to deal with this. Basically it declares the collided data as unusable and forces the two computers to re-send their data packets at a slightly different time.

A switch has a number of ports and it stores the addresses of all devices that are directly or indirectly connected to it on each port. As a data packet comes into the switch, its destination address is examined and a direct connection is made between the two machines.

MoDem

A modem is a device that allows you to connect to your Internet service provider and browse the Internet. Because modems only provide one IP address each, the best way to use a high-speed modem is to share its services among computers.

Originally engineers called it the '**MO**dulation - **DEM**odulation' box. But it was such a mouthful that naturally they ended up calling it the MODEM. A modem converts the digital data from the computer into a continuous analogue wave form that the telephone system is designed to deal with (MODulation). The reason for this is that the telephone system was originally designed for the human voice i.e. continuous signals. The modem also converts the analogue signal from the telephone network back into digital data that the computer can understand (DEModulation).

Standard modems come in two forms. An external box that links to your computer either through a serial or USB port, or an internal modem that is plugged directly to the motherboard inside the computer.

An internal Modem

An external modem

Wi-Fi modems

In addition to telephone modems, radio has now become very popular as a means of connecting to the internet. The device that allows you to do this is called the Wi-Fi modem

Router

A router is a device that joins two different networks together. Home networks usually employ routers to connect to the Internet. The majority of routers contain a switch within them so that all of the computers on a network can communicate. It is a device that transfers data from one network to another in an intelligent way. It has the task of forwarding data packets to their destination by the most efficient route.

A router allows connectivity to one or more computers, helping create a network. For home users, these are particularly useful for taking a single broadband internet account, and spreading it to at least two or more computers. Standard routers require the internet connection from a standalone modem, but modem-routers are increasing in popularity, which can be plugged into any broadband-enabled phone line, reducing cable clutter, and only taking up one power socket.

Wireless routers have become more common. A wireless router does exactly the same job in the home as a regular wired (Ethernet) router, with the difference that a computer can be connected to it without needing to run Ethernet cable between the computer and the router. All you need is a wireless network adapter in each PC you want to connect, usually in the form of a card in your PCI slot (or a laptop's PCMCIA card slot) or an adapter for USB. Wireless routers generally have four ports to connect Ethernet cable as well, so computers can be connected by whatever means is most convenient - you might want to use a cable for your desktop PC which sits right next to the router, but use the wireless adapter in your laptop.

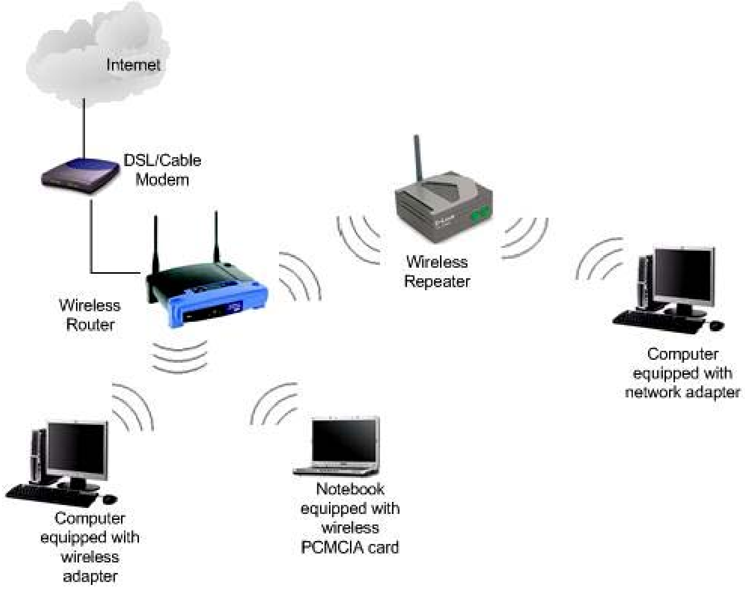
Routers operate at the network level of the OSI model.

Firewall

A firewall is a protective system that lies, in essence, between your computer network and the Internet. When used correctly, a firewall prevents unauthorized use and access to your network. The job of a firewall is to carefully analyze data entering and exiting the network based on your configuration. It ignores information that comes from unsecured, unknown or suspicious locations. A firewall plays an important role on any network as it provides a protective barrier against most forms of attack coming from the outside world.

Repeaters

A repeater is a device, which copies or repeats signals that it receives. However a repeater also amplifies all received signals before re-transmission. This means a repeater increases the size of Analog waveforms it receives. By increasing the size of the waveform (without changing its frequency) or we can say that a repeater strengthens an increasing signal before sending the signal on its way. By strategically placing repeaters along a network bus, Engineers can extend the distance between adjacent computers.

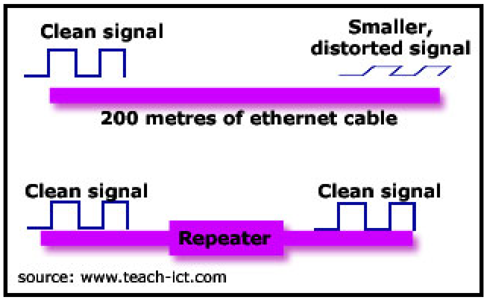

Internet
DSL/Cable Modem
Wireless Router
Wireless Repeater
Computer equipped with network adapter
Computer equipped with wireless adapter
Notebook equipped with wireless PCMCIA card

Source: *http://www.home-network-help.com/images/wireless-repeater-network.jpg*

All signals fade as they travel from one place to another. Each type of network cable has a maximum useable length. If you go beyond that length, the signal will be too weak to be useful.

Of course, computers on a real network can easily be more than 200 metres apart. Therefore the network cable is split up into segments. Each segment is less than the maximum length allowed. Joining the segments together is a device known as a 'Repeater'.

Source: *http://www.slipperybrick.com/wp-content/uploads/2007/06/sirius-echo-home-repeater-system.jpg*


Clean signal
Smaller, distorted signal
200 metres of ethernet cable
Clean signal
Clean signal
Repeater
source: www.teach-ict.com

A Repeater boosts the signal back to its correct level.

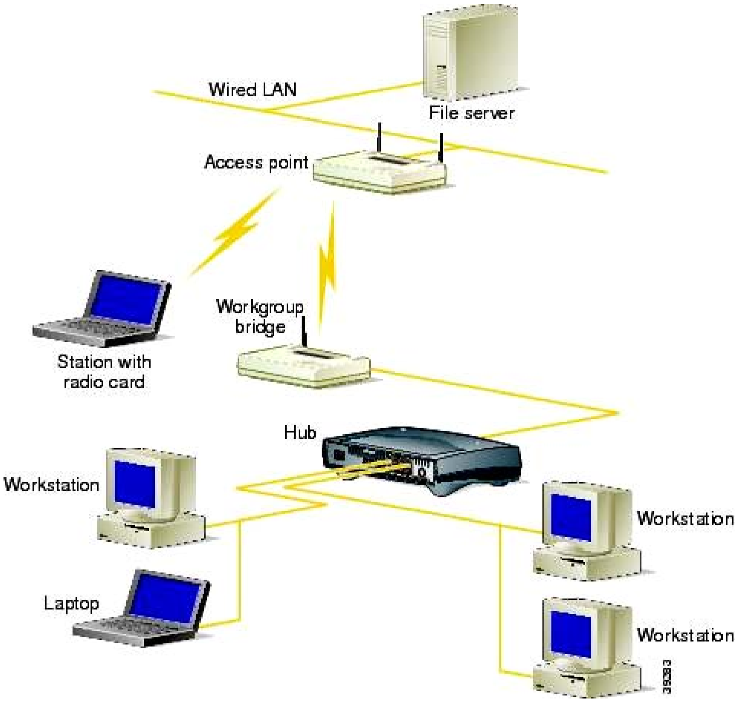
Bridges

A bridge device filters data traffic at a network boundary. Bridges reduce the amount of traffic on a LAN by dividing it into two segments.

Bridges operate at the data link layer (Layer 2) of the OSI model. Bridges inspect incoming traffic and decide whether to forward or discard it. An Ethernet bridge, for example, inspects each incoming Ethernet frame - including the source and destination MAC addresses, and sometimes the frame size - in making individual forwarding decisions.

A bridge interconnects two networks that use the same technology (such as ARCNET or Ethernet). When a bridge interconnects two networks called "Westside" and "eastside". In addition to interconnecting networks, Bridges often boost performance security and reliability. For example, we know that a collision detection system required a computer to delay transmission after a data collision occurs. As we add more computers to a network, the number of data collision rises.

Network administrators often use a bridge to create two or more small networks even if performance is not a problem on this network. As we have learned in a ring or bus topology, a single break in a data bus stops all network communication. By partitioning a single LAN into multiple LANs (connected by a bridge), a Network administrator reduces the impact of a break in the data bus.



Source: *http://www.cisco.com/en/US/i/000001-100000/35001-40000/39001-39500/39283.jpg*

Data transmission media

There are three main methods of transferring data:

- Electrical
- Radio or Microwave
- Infrared

Electrical:

A multi-wired cable with a socket at each end is used to connect the various devices together e.g. computer to hub, hub to switch or switch to router etc.

The Ethernet network cable (shown above) transfers data by means of electrical signals. A typical network cable called 'Cat 5' is used which is especially designed to carry the signal as efficiently as possible.

The data requires some media to travel & the cables provide this platform with the help of the microwaves also but it is too much expensive. Commonly the cables are used they are as follows.

Coaxial Cable:

Coaxial cable, often referred to as BNC cable (the initials refers to the Bayonet-Naur Connector – a bayonet-shaped connector for thin coaxial cables), is made of a single copper wire encased in insulation and then covered with a layer of aluminum or copper braid that protects the wire from outside interference.

Coaxial cable has four parts:

Inner Conductor: A central wire

Dielectric: A layer of insulation that surrounds the inner conductor.

Shield: A layer of foil or metal braid that covers the dielectric.

Jacket: A final layer of insulation.

It is a popular cable for the connective of the computer terminals. It consist of the two conductor surrounded by two insulating layers. The first layer of insulation encloses a central copper conductor wire. This layer has an outer shielding conductor braided over the top of it.

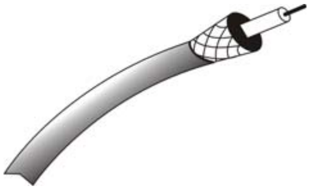


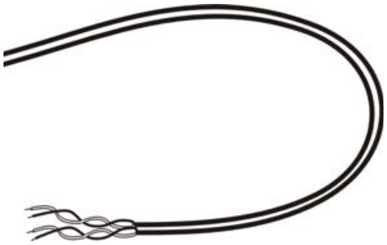
Figure: Coaxial Cable

Twisted Pair Cable:

Twisted pair cable is common type of network cable, because of low cost. Physically, in its simplest form twisted pair cable consists of a pair of insulated copper wires twisted around each other.

On this category include various type of twisted pair, these are: Unshielded twisted pair (UTP), Shielded twisted pair (STP) 10BaseT, 100BaseT. All of them UTP cable prefer Hub based network solution.

- **Unshielded Twisted-Pair:**



The unshielded twisted pair cables are highly sensitive electromagnetic interference. It is commonly used for telephone connections. Now a day they are also used for LAN purpose. The twisted pair compress of two wires twisted together six turns per inch to provide shielding from electrical interference plus consisting impedance; or in other word we can say it is a cabling system that we can use for Ethernet or Token ring networks and many other types of data communications. UTP, unlike coaxial or IBM type 1 cable, in not inherently good at carrying high-speed data. However, it does provide satisfactory results over short distances. Its attraction is that it is thin, cheap, and already in place in many buildings. Standard telephone wiring uses UTP.

- **Shield Twisted Pair**

These wires are generally thicker than UTP and are shielded from any electrical interference by protective coat of insulated material.

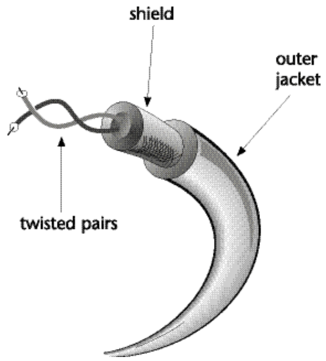
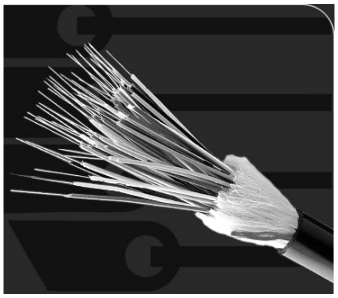


Figure: Shielded Twisted-Pair Cable

Fiber Optics:

The major Network system new support fiber-optic cabling because fiber-optic cables transmit data as light pulses through glass cables & the significant advantage of this type of cabling over others, is that it provide the fastest transmission speed and more reliable. Fiber-optic is thin on flexible.



Fiber optic also called Optical Fiber is usually found where long cable lengths are required, where extremely high speed is desire. It is much less weak to these environmental difficulties because it uses light impulses along a glass or plastic wear or fiber, rather than electrical signals through on electrically conductive medium light signal protection from environmental interface. The light produce from the end of a fiber optic cable is a high density, laser quality light.

Radio or Microwave

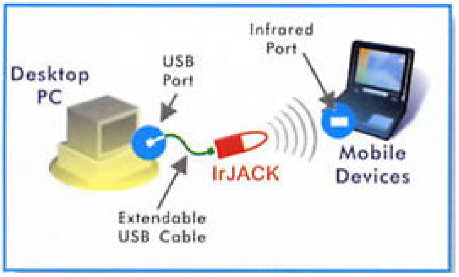
Microwaves are just a small part of the radio spectrum, but because they are so widely used, they tend to be called by their own name. Data is sent out through aerials mounted on tall towers. The 'cable' is effectively the microwave link between towers. Some large companies use microwave towers spread along hilltops to allow one office to communicate with others in the same country.

They do this because it is cheaper than renting telephone lines for carrying the same amount of data. On a much smaller scale, laptops can communicate with the local area network with radio links:

Infra-Red / Bluetooth

This is a very familiar method of transferring data if you are at all aware of your remote control! The television remote control makes use of an infra-red link.

PDA and personal organizers often make use of an infra-red link to synchronies calendars and 'to-do' lists.



Open System Interconnection Reference Model (OSI Reference Model or simply OSI Model)

OSI model defines a networking framework for implementing protocols in 7 (SEVEN) layers (Application to Physical). The International Organization for Standardization (ISO) develops the OSI (Open System Interconnection) model in 1977. The OSI model defines the rules that apply to the following issues:

1. How Network devices contact each other and how they understand the language of each other and how they communicate with each other.
2. Methods by which a device in which a network knows when to transmit data and when not to.
3. Methods to insure that network transmissions are received correctly and by the right recipient.
4. How the physical transmission media are arranged and connected.
5. How to ensure that network devices maintain a proper rate of data flow.
6. How bits are represented on the network media.

The OSI model is nothing tangible; it is simply a conceptual framework. The OSI model does not perform functions in the communication process. The actual work is done by the appropriate software and hardware. The OSI model protocols will handle those tasks. The OSI model consists of seven layers.

UPPER Layers (Application Set)	Layer 7	Application	**High Level Protocols**
	Layer 6	Presentation	
	Layer 5	Session	
LOWER Layers (Transport Set)	Layer 4	Transport	**Medium Level Protocols**
	Layer 3	Network	
	Layer 2	Data Link	**Low Level Protocols**
	Layer 1	Physical	

The OSI model defines internetworking in terms of a vertical stack of seven layers. The **upper layers** of the OSI model represent software that implements network services like encryption and connection management. The **lower layers** of the OSI model implement more primitive, hardware-oriented functions like routing, addressing, and flow control.

In the OSI model, data communication starts with the top layer at the sending side, travels down the OSI model stack to the bottom layer, then traverses the network connection to the bottom layer on the receiving side, and up its OSI model stack.

High Level Protocols

How the data is presented, displayed and summarized for the user – and in the reverse direction, how the user prepared data is assembled into meaningful data structures (high-level protocols).

Medium Level Protocols

How the data is assembled into packets and frames and how error checking and flow control is implemented – and in reverse direction, how the received packets and frames are assembled into structures such as files and databases (medium-level protocols).

Low Level Protocols

How the data is converted into electrical pulses of 1's and 0's (bits) and sent across cables or the physical medium – and in the reverse direction, how the electrical pulses are taken off the cable and converted into 1's and 0's.

1. Application Layer (Layer 7)

The application layer is the topmost layer of the OSI model and it provides services that directly support user application such as database access, e-mail and file transfer. It also allows application to communicate with application on other computers as though they were on the same computer. This application layer includes the basic service from any network including dealing with files, sending messages to other network.

This layer supports application and end-user processes. Communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. Everything at this layer is application-specific. This layer provides application services for file transfers, e-mail, and other network software services. Telnet and FTP are applications that exist entirely in the application level. Tiered application architectures are part of this layer.

Purpose of Application Layer:

- Talks to application software
- Interface between application and computer network
- Interacts with Operating System or Applications
- Transfer files, read messages, perform network related activities
- Defines interface to user processes for communication and data transfer in network.
- Provides standardized services such as virtual terminal, file and job transfer and operations.
- Open files from network using specific software.
  Example: Fast Ethernet, RS232, ATM

2. Presentation Layer (Layer 6)

The presentation layer translates the data access from the application layer in the language understandable by network or computer. The presentation layer does protocol conversion, data translation, compression and encryption, character set conversion and the interpretation of graphics commands. The network redirector operates at this level. The network redirector is what makes the files on a file visible to the client's computer.

The network redirector also makes remote printers act as though they are attached to the local computer. This layer is responsible for ensuring that data is in a form everyone can understand and work with takes the data from the session layer and passes it along to the application layer.

This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa. The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. It is sometimes called the syntax layer.

Purpose of Presentation Layer:

- Reformat, encrypt/decode, compress/decompress
- Presentation layer receives requests for files from the Application layer and presents to the session layer
- In order for data to be sent faster and more secure, the presentation layer encrypts/decodes or compresses/decompresses the data so that the application and session layers can communicate.
- Takes data from Application layer and converts it into a standard format.
- Masks the differences of data formats between dissimilar systems
- Specifies architecture-independent data transfer format
- Encodes and decodes data; encrypts and decrypts data; compresses and decompresses data

3. Session Layer (Layer 5)

This layer establishes a session in which the communication has done between two computers. This layer provides services such as name look up and security to allow two programs to find each other and established the communication link the session layer also provides for data synchronization and check pointing so that in the event of network failure, only the data sent after the point of failure need by resend this layer also controls the dialogue between two processes after mining who can transmit and who can receive at what point during the communication. Session Layer protocol establishes and manages session using a data's taken to determine which can talk and when talk to communicate the Computer one to others all data packet's information knows as token.

This layer establishes, manages and terminates connections between applications. The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. It deals with session and connection coordination.

Purpose of Session Layer:

- Makes connection at both ends.
- Establishes and maintains a session, sometimes known as socket, between the two network nodes.
- An attempt is made to create the socket – both nodes acknowledge the session and the session is assigned an identifying number. Either node can close the socket when communications in both directions is completed.
- Establishes, maintain and ends communication with receiving device.
- Manages user sessions and dialogues
- Controls establishment and termination of logic links between users
- Reports upper layer errors

  Example: TCP, SPX (Sequenced Packet Exchange)

4. Transport Layer (Layer 4)

The transport layer ensures that packets are delivered error free, in sequence, and with no loses or duplication it provides error free transmission of data from one computer to another. The transport layer message from the session layer into packet to be sent to the destination computer and reassembles packets into message to be presented to the session layer the transport layer typically sends and acknowledgement to the originator for message receive. The Transport layer is home to a number of protocols: TP0, TP1, TP2 and so on. These layers handle the packet of message and reassembly and error recovery.

This layer provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer.

Purpose of Transport Layer:

- Error correction
- The transport layer guarantees successful delivery of data by checking for errors and requesting retransmission of data if errors are detected.
- Transport protocol includes:
  i. TCP
  ii. IPX (Internet Packet Exchange)
  iii. NetBEUI

- Maintain flow control of data, provides for error checking and recovery of data between the devices.
- Manages end-to-end message delivery in network
- Provides reliable and sequential packet delivery through error recovery and flow control mechanisms
- Provides connectionless oriented packet delivery

5. Network Layer (Layer 3)

The network layer decides the best route for data transfer, which are adopted from transport layer and forward packets for devices that are further away then a single link. The network layer translates logical network addresses into physical machine addresses. This layer also determine the quality of service such as the priority of the message and the route message will take if there are several ways a message can get to it's destination.

The network layer also break large packets into small chunks if the packet is larger than the largest data frame the data link layer will accept the network resembles the hunks into packets at the receiving in the protocols at this layer may choose a specific route through an interact work to avoid the access traffic caused by sending data over networks.

Network Layer defines how the network moves information from one device to another. This layer corresponds to the hardware interface function BIOS of an individual PC, because it provides a common software interface.

This layer provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing.

Purpose of Network Layer:

- Finds the best possible route for sending frames over an Internet.
- The way that the data will be sent to the recipient device is determined.
- Logical protocols, routing and addressing are handled here.
- Determines how data are transferred between network devices
- Routes packets according to unique network device addresses
- Provides flow and congestion control to prevent network resource depletion
  Example: IP, IPX

6. Data Link Layer (Layer 2)

The data link layer provides for the flow of data over a single link from one device to another. It accepts packets from the network layer and packages the information into data unit called frames to be presented to the physical layer for transmission. The data link layer adds control information such as frame types routing to the data being sent. Actually this layer provides for the error free transfer of frames from one computer to another. A cycle redundancy check added to the data frame can detect damaged frames. The data link layer can also detect when frames are lost and request that those frames be sent again. This layer further divided into two sub-layers.

At this layer, data packets are encoded and decoded into bits. It furnishes transmission protocol knowledge and management and handles errors in the physical layer, flow control and frame synchronization. The data link layer is divided into two sub layers: The Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. The MAC sub layer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronization, flow control and error checking.

i. **Logical link control**, which establish and maintains links between the communicating devices.

ii. **Media access control** (MAC), which controls the way multiple devices share the same media channel. MAC addresses are written as a sequence of 12 hexadecimal digits.

It defines how information gains access to the wiring system. The data link layer defines the basic protocol used in the local network. It decide and send a message over the cable at any given item, the form of messages and the transmission method of those message.

Purpose of Data Link Layer:

- The job of data-link layer is to disassemble and reassemble segmented data.
- Defines procedures for operating the communication links
- Frames packets
- Detects and corrects packets transmit errors

  Example: NIC – Ethernet, Token Ring, FDDI (Fiber Distributed Data Interface) etc.
- Those devices segments and packages the stream of data bytes into packets before presenting it to the physical layer to be transmitted over the media.

7. Physical Layer (Layer 1)

The first layer of the OSI Reference Model is the physical layer, which defines the basic hardware of network, which is the cable that conducts the flow of information between the devices linked by the network. This layer defines the type of wire such as coaxial, twisted pair cable, length and connection and the interface of the cabling system.

The physical layer is simply responsible for sending bits (0,1) from one computer to another. This layer deals with the physical connection to the network and with transmission and reception of signals.

This layer conveys the bit stream - electrical impulse, light or radio signal -- through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards and physical aspects. Fast Ethernet, RS232, and ATM are protocols with physical layer components.

The following items are addressed at the physical layer.

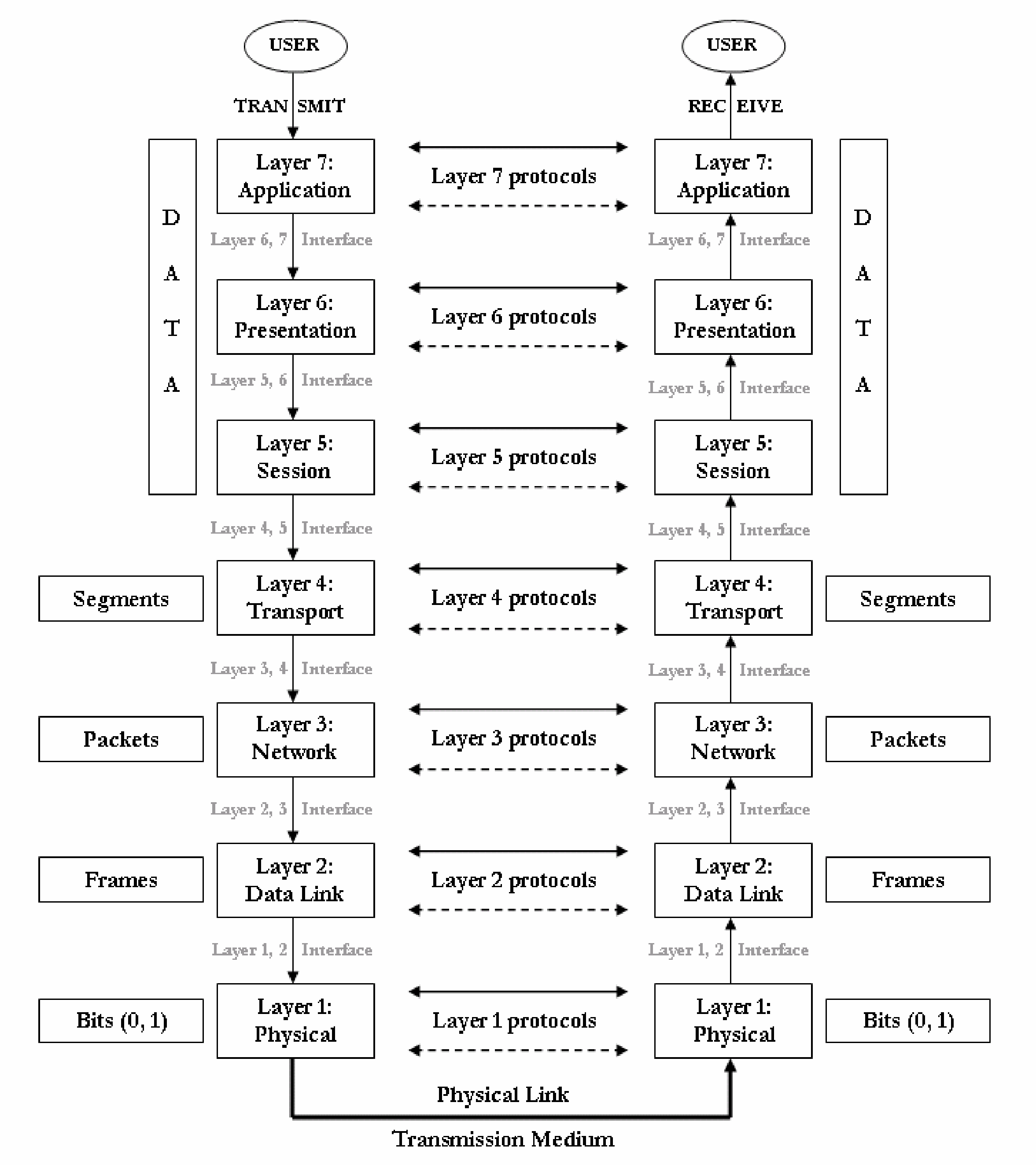
a. Network connection type
b. Physical topologies
c. Analog and Digital signaling
d. Base band and Broad band transmission
e. Termination

Purpose of Physical Layer:

- Defines physical means of sending data over network devices
- Interfaces between network medium and devices
- Defines optical, electrical and mechanical characteristics
- Passes data onto media
- Transport bits between machines
  - How do we send 0's and 1's across a medium?
  - Vary physical property like voltage or current
- Representing the property as a function of time
  - Analyze it mathematically
- Does the receiver see the same signal generated by the sender?
  - Why or why not?

Example: NIC Firmware, NIC driver

Function of OSI Model



RESEARCH METHODOLOGY

This section includes

RESEARCH METHODOLOGY

Deductive Approach

Inductive Approach

AASA (Analysis, Assess, Security & Awareness)

1. Analysis
2. Assess
3. Security
4. Awareness

CASE-STUDY

1. ANALYSIS

Penetration Testing

2. ASSESS

Use of network security tools

3. SECURITY

Developing a Security Policy

Security of Physical threats

Data Security

Application Security

Network Security

Protect yourself from

How to protect your system from crimeware?

How to protect your system from hackers?

How to protect from a phishing attack?

How to protect from Spam?

How to protect from Identity Theft?

To protect against malicious code attacks

4. AWARENESS

How to choose secure passwords?

How to keep your passwords safe?

Top Security vulnerabilities

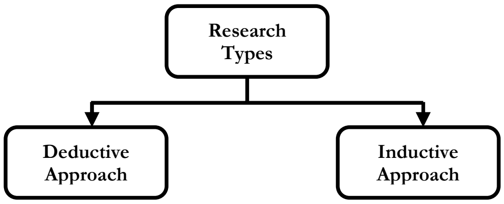
Common security lapses

Network Administration Tips

Things to know about network administration

In research, we often refer to two broad methods of analysis:

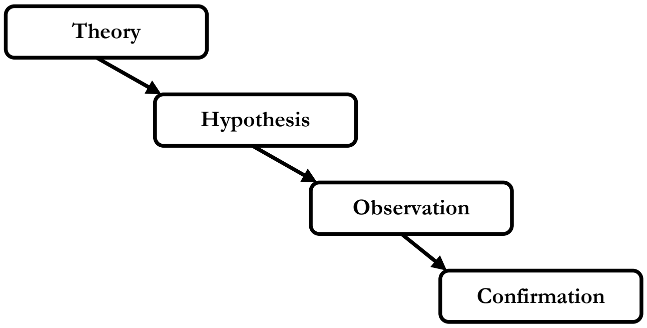
1. Deductive and;
2. Inductive approach



Deductive Approach

Deductive approach begins with general ideas (such as theory, laws, and principles) and based on them, you form specific hypotheses which can be tested in order to support the general ideas. If the hypothesis is supported, you may want to say that the initial (general) idea was indeed correct.

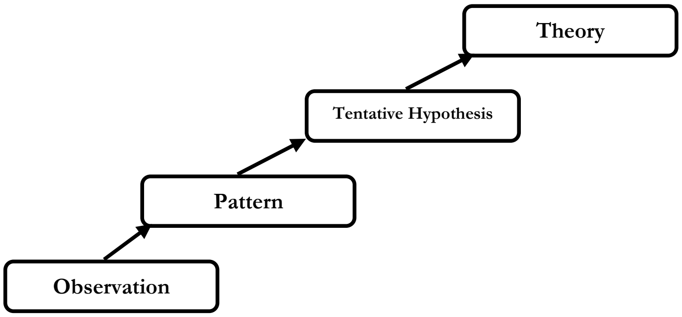
- Deductive reasoning works from the more general to the more specific.
- Sometimes this is informally called a "top-down" approach.
- Conclusion follows logically from premises (available facts)



Inductive Approach

On the other hand, inductive approach begins with specific things -- observations of individual cases, for example. Based on the accumulation of such observation, you may want to build a general idea on that observation. Inductive approach is often compared to what detectives are doing. They gather small evidence and information around the specific things and pin down a theory.

- Inductive reasoning works the other way, moving from specific observations to broader generalizations and theories.
- Informally, we sometimes call this a "bottom up" approach.
- Conclusion is likely based on premises.
- Involves a degree of uncertainty.



In this research, the Deductive approach would be used in testing the theory upon which the model AASA was built.

The model AASA would be implemented in the live scenario (CASE-STUDY: Stratford College London) with the help of no-cost network security supplementary tools– whois.sc, network-tools.com, ping, ipconfig, traceroute, nslookup, nmap etc...

The research will be carried out according to the stages of AASA model and the outcomes would be discussed in the CASE-STUDY section.

AASA (Analysis, Assess, Security & Awareness)

1. Analysis

A. Identifying assets and security perimeters
B. Identifying the area of threats (risks) and creating a list
C. Identifying vulnerabilities
D. Prioritizing assets and vulnerabilities

A. Identifying assets and a security perimeter

1. Computers and laptops
2. Routers and networking equipment
3. Printers
4. Data - sales, customer information, employee information
5. Email
6. Log of employees daily schedule and activities
7. Web pages, especially those that ask for customer details and those that are backed by web scripts that query a database
8. Web server computer
9. Security cameras
10. Employee access cards.
11. Access points (i.e., any scanners that control room entry) etc…

B. Identifying the area of threats and creating a list

1. Computer and network passwords
2. Physical assets
3. Records of physical assets
4. Data backups
5. Logging of data access
6. Access to sensitive data
7. Access to client lists
8. Long-distance calling
9. Emails etc…

Once the general list of threats has been compiled, review it with those most knowledgeable about the system, organization or industry to gain a list of threats that applies to the system.

It is valuable to compile a list of threats that are present across the organization and use this list as the basis for all risk management activities. As a major consideration of risk management is to ensure consistency and repeatability.

C. Identifying Vulnerabilities

Vulnerabilities can be identified by numerous means. Different risk management schemes offer different methodologies for identifying vulnerabilities. In general, start with commonly available vulnerability lists or control areas. Then, working with the system owners or other individuals with knowledge of the system or organization, start to identify the vulnerabilities that apply to the system.

Additionally, while the following tools and techniques are typically used to evaluate the effectiveness of controls, they can also be used to identify vulnerabilities:

- **Penetration Testing** – An attempt by human security analysts to exercise threats against the system. This includes operational vulnerabilities, such as social engineering.
- **Vulnerability Scanners** – Software that can examine an operating system, network application or code for known flaws by comparing the system (or system responses to known stimuli) to a database of flaw signatures.
- **Audit of Operational and Management Controls** – A thorough review of operational and management controls by comparing the current documentation to best practices (such as ISO 17799) and by comparing actual practices against current documented processes.

It is invaluable to have a base list of vulnerabilities that are always considered during every risk assessment in the organization. This practice ensures at least a minimum level of consistency between risk assessments. Moreover, vulnerabilities discovered during past assessments of the system should be included in all future assessments. Doing this allows management to understand that past risk management activities have been effective.

Past due Diligence & Predicting the Future

- Examining Threat History
- Checking threats from Competitors

D. Prioritizing Assets & Vulnerabilities

- **Risk Calculation/ Probability Calculation**
  Risk = Probability x Harm
  - **Calculating Probability**
  - **Calculating Harm**
- **Developing Security Threat Response Plan**

2. Assess

Vulnerabilities

- Vulnerability Scanners
- Audit of Operational and Management controls

Threats

- Intrusion Detection Systems (physical & logical)
- Security Systems

Attacks

- Physical and Logical controls

An outcome of this step is discussed in the CASE-STUDY section.

Vulnerability Assessment Methodology:

Step 1: Study & scope the network architecture & components for assessment

Step 2: Determine the boundary of analysis

Step 3: Identify asset owners & schedule tasks

Step 4: Impact analysis for Active scans, which includes assessment of Service(s) or Server(s) scans in online production.

Step 5: Plan for Downtime & Contingency, if applicable

Step 6: Estimate the scan process, based on the complexity of the target network(s) and host(s)

Step 7: Define the scan Policy for each target. Scan Policy to define the level of scan - Information gathering, Policy checking, Port scanning, Password analysis, Attack stimulation etc.

Step 8: Scan the targeted network(s) and host(s), based on the defined scan policy

Step 9: Collect the scan results and analyze for security loopholes, configuration errors, default installation settings, overlooked setups, password quality, firmware/software revisions, patch fixes, security policy violations etc.

Step 10: Submission of Assessment Reports with suggestions and recommendations to fix the vulnerabilities

Using a combination of various freeware and commercial tools and techniques to evaluate your network offers a clear picture of the dangers the company faces. At the minimum, an effective network assessment testing methodology should address the following areas:

- External network topology for improper firewall configuration
- Router filtering rules and configuration
- Weak authentication mechanisms (which could lead to a dictionary-based authentication attack)
- Improperly configured or vulnerable e-mail and DNS servers
- Potential network-layer Web server exploits
- Improperly configured database servers
- SNMP checks
- Vulnerable FTP servers

Assessing the Network Risk

Network risk assessment includes four phases: discovery, device profiling, scanning, and validation.

a. Discovery

Discovery involves establishing a fingerprint of the target network segment. This should include all active device addresses and their associated TCP, UDP, and other network services accessible from the internal network.

During this phase, use both active and passive sniffers to collect network traffic for parsing and analysis. Information obtained through this method should include identification of active hosts, authentication credentials (such as username and password combinations), indication of potential computer worm and/or Trojan presence, and other vulnerabilities.

Here's a list of some of the most popular tools used for network discovery:

Tools: Nmap, Ethereal, Firewalk, hping etc…

b. Device profiling

Using the information gathered during the discovery phase, you can analyze the list of accessible network services, Internet Protocol (IP) stack fingerprints, and known network architectures to identify potential roles and trust relationships each device plays in your network infrastructure.

c. Scanning

Test each network service identified during the discovery and device profiling phases for known vulnerabilities. Vulnerabilities can fall into one or more categories. These include:

- System compromise
- Unauthorized data access
- Information disclosure
- Command execution
- Denial of service (DoS)

In some instances, it's possible to detect and exploit security risks associated with a particular network service using the following software applications (tools):

Tools: Nessus, onesixtyone, nikto etc…

d. Validation

After you've completed the first three phases of your network risk assessment, your final step is to attempt to exploit or validate all results from the vulnerability scanning phase. Tests and techniques applied during this stage of the assessment are often very specific to the potential vulnerabilities detected. This final phase of the assessment will generate the bulk of your results.

3. Security

- Different preventive and mitigation techniques
- Strong Password techniques, Anti-malware software etc.

Security systems are discussed in the Security Chapter.

4. Awareness

- Providing guidelines for network security precautions, awareness and risk management tips about the security system to the network administrators and security engineers.

Details about the awareness are discussed in the Awareness Chapter.

NO-COST Network Security Tools:

When combined with automated assessment and configuration tools, AASA becomes a powerful, fundamental vulnerability assessment protocol. The below table enumerates many of the freeware or trialware products, that when used effectively together and in connection with AASA, provide a potent and functional toolkit for executing vulnerability assessment.

Tool Names	Functional comment	Tools type
http://www.whois.net/ http://whois.domaintools.com/ nslookup	Network enumeration (Determining IP Addresses)	Free/Command line
Ping (fping, gping)	Network enumeration (Identifying active addresses)	Command line
Nmap (www.nmap.org) Superscan (www.foundstone.com)	Port Scanner, URL Scanner (Host discovery, Port scanning, version detection, OS detection)	Free/Command line
Fport (www.foundstone.com)	Identifying open TCP/IP, UDP ports	Free/Command line
Sam Spade (www.samspade.org)	Multi network query	Freeware
GFI LANGuard (www.gfi.com) Nessus (www.nesus.org) – Linux Wireshark (www.wireshark.org)	- Network Security Scanner and Vulnerability Management Tool - Port scanner and penetration testing TCP, UDP, SNMP, URL - Network protocol analyzer	- Trialware - Full featured & Free - Freeware

Tool Names	**Functional comment**	**Tools type**
Cain and Abel (www.oxid.it) John the Ripper (www.openwall.com/john) L0phtcrack (www.l0phtcrack.com)	- Password recovery tool for Microsoft OS - Password recovery tools for Windows, Linux, Mac, UNIX - Password Auditing & Recovery	- Freeware - Free and open source - 15 days freeware
Snort (www.snort.org)	IDS, Packet Sniffer, Packet Logging	Full featured & Free
Metasploit framework (www.metasploit.com)	Vulnerability exploitation, penetratation testing for Windows, Linux, UNIX	Freeware
Tcptraceroute (UNIX) Tracepath (Linux) Tracert (windows)	Determining the route taken by packets across an IP network	Command line
Netstat (www.netstat.net) - Linux	Finding problems in the network and to determine the amount of traffic on the network as a performance measurement	Command line
Netcat (http://netcat.sourceforge.net)	Reads and writes data across network connections, using the TCP/IP protocol	Opensource

EMPIRICAL OBSERVATION

CASE-STUDY

In this case-study, the proposed protocol for network security assessment methodology **AASA (Analysis, Assess, Security and Awareness)** would be implemented and tested using some freely available network security tools to prove its effectiveness.

The research will be carried out according to the AASA model.

The selected organization for the dissertation, empirical study, is **Stratford College London** whereby the model would be tried and tested in the college IT network system in order to test a theory.

The business is in the domain of education sector, delivering higher education courses for Business and Computer Studies. In education sector, the needs of security are important due to the sensitive data and information of students and staffs' record, students' work, internet access, intranet system and access to the resources/systems.

Stratford College London was chosen because it would provide the requirement environment to conduct the research. Also, it would represent the medium-scale business organizations. The choice of this college was also the result of the researchers familiarity with the institution and its IT and network system. Access would not be a problem with the permission from college, this research will be carried out with the support of the administrative and IT staffs.

In this college, there are approximately 100 computer systems, two routers, eight switches, two different network domains, database system and other relevant equipments exists. Security policies, anti-virus software, IDS, Firewalls are used to secure the system.

Implementation of AASA protocol (Stratford College London)

1. ANALYSIS

A. Identifying assets and a security perimeter

1. Personal Computers - 95 and laptops - 8
2. Routers – 2 and networking equipments: switches – 6, hubs - 2
3. Printers - 12
4. Data – students' record, students' project, employee information, exam materials, teaching materials, learning materials, library records
5. Email – xxxxx@sclondon.co.uk (25 email accounts)
6. Log of employees daily schedule and activities – YES, Domains – 2 (sclondon.co.uk, admin.co.uk)
7. Web pages – Online application, online feedback within www.sclondon.co.uk
8. Web server computer - 1
9. Security cameras - 5
10. Employee access cards - YES
11. Access points – Code lock system

B. Identifying the area of threats

1. Computer and network passwords
2. Physical assets and its record system
3. Data backups
4. Logging of data access
5. Access to sensitive data
6. Access to students' and employees' records
7. Emails
8. Online forms
9. Access privilege
10. Access to learning materials

C. Identifying Vulnerabilities

Penetration Testing

Usually for a penetration test you will be given the name of the organization or a person name.

Example: **Stratford College London** and **Hemanta Baral**

Domain name: www.sclondon.co.uk

Tool Used: Google Search
Tool Syntax: Stratford College London

IP Address: The IP address of www.sclondon.co.uk is **94.76.229.197**
Tool Used: http://www.selfseo.com/find_ip_address_of_a_website.php
Tool Syntax: www.sclondon.co.uk

Registrant: Shahzadi Services Ltd.
Tool Used: http://whois.domaintools.com or, www.whois.sc
Tool Syntax: www.sclondon.co.uk

Administrative Contact, Technical Contact:

```
Master, Host (HM6761)
  One.com
  Kalvebod Brygge 45

  Copenhagen V, 1560
  DK
```

hostmaster@one.com

```
  +45.46907100 Fax: +45.70205872
```

Tool Used: http://whois.domaintools.com
Tool Syntax: www.hemantabaral.com

Billing Contact:

```
Registrant:
  Raj Baral, Hemanta (509968)
  Flat 12, IBIS Court
  Edward Place, Deptford
  London, SE8 5PY
  GB
```

Tool Used: http://whois.domaintools.com or www.whois.sc
Tool Syntax: www.hemantabaral.com

Domain servers in listed order:

```
NS1.ONE.COM (NSONECOM416)
  NS2.ONE.COM (NSONECOM828)
  NS3.ONE.COM (NSONECOM746)
```

Tool Used: http://whois.domaintools.com or www.whois.sc
Tool Syntax: www.hemantabaral.com

SOA (Start of Authority record)

Tool Used: http://network-tools.com
Tool Syntax: www.sclondon.co.uk

serial:	2009100801
refresh:300	
retry:	300
expire:	86400
minimum ttl:	300

List Mail Server IP Addresses:

First we have to find out mail server name using above mentioned method.

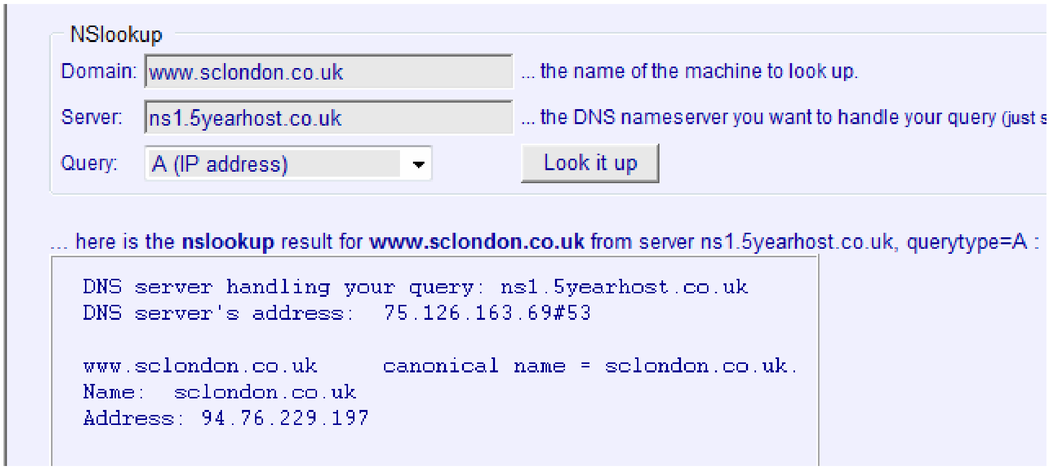
Tool Used: www.network-tools.com
Tool Syntax:: mail server name i.e. ns1.one.com

IP address: **195.47.247.15**
Host name: ns1.one.com

List DNS NS IP Addresses:

```
DNS server handling your query: ns1.5yearhost.co.uk
DNS server's address:  75.126.163.69#53
```

Tool Used: http://www.kloth.net/services/nslookup.php
Tool Syntax:



Domain: www.sclondon.co.uk ... the name of the machine to look up.
Server: ns1.5yearhost.co.uk ... the DNS nameserver you want to handle your query (just s
Query: A (IP address)

... here is the **nslookup** result for **www.sclondon.co.uk** from server ns1.5yearhost.co.uk, querytype=A :

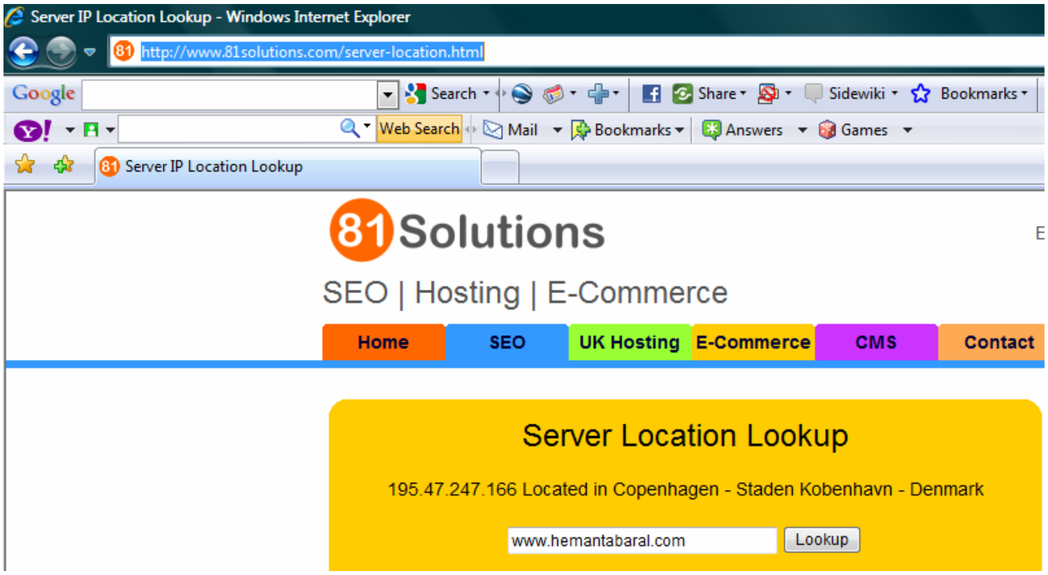
```
DNS server handling your query: ns1.5yearhost.co.uk
DNS server's address:  75.126.163.69#53

www.sclondon.co.uk      canonical name = sclondon.co.uk.
Name:  sclondon.co.uk
Address: 94.76.229.197
```

Note: DNS servers can be found using http://network-tools.com

List Web Server IP Address:

195.47.247.166 located in Copenhagen – Staden Kobenhavn – Denmark

Tool Used: http://www.81solutions.com/server-location.html
Tool Syntax: www.hemantabaral.com



http://www.81solutions.com/server-location.html

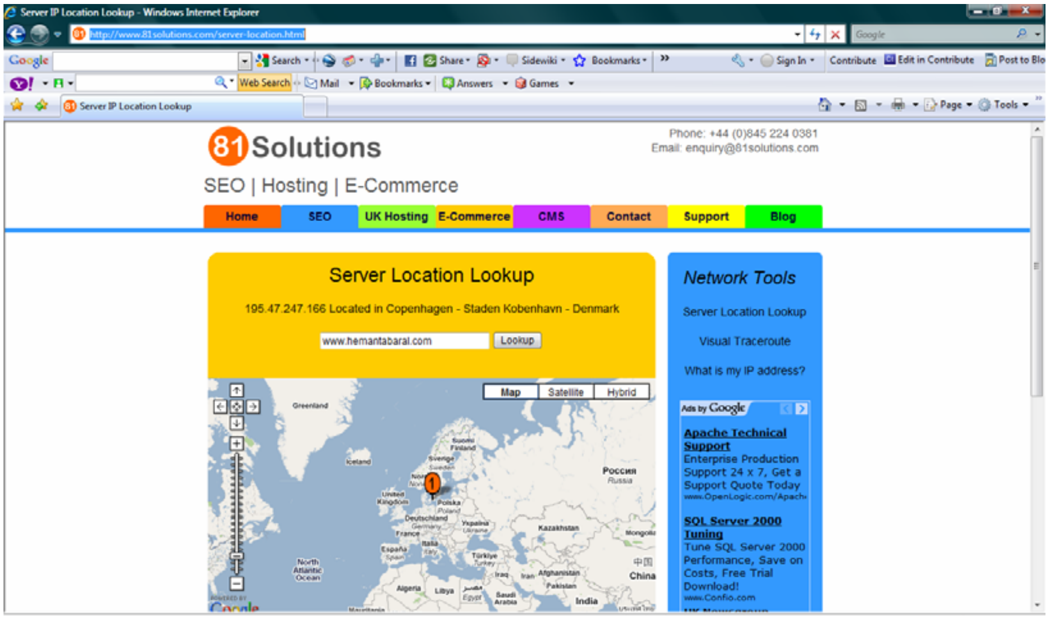
Server Location Lookup

195.47.247.166 Located in Copenhagen - Staden Kobenhavn - Denmark

www.hemantabaral.com

Where is the Web Server located?

Tool Used: http://www.81solutions.com/server-location.html
Tool Syntax: www.hemantabaral.com



http://www.81solutions.com/server-location.html

Phone: +44 (0)845 224 0381
Email: enquiry@81solutions.com

Server Location Lookup

195.47.247.166 Located in Copenhagen - Staden Kobenhavn - Denmark

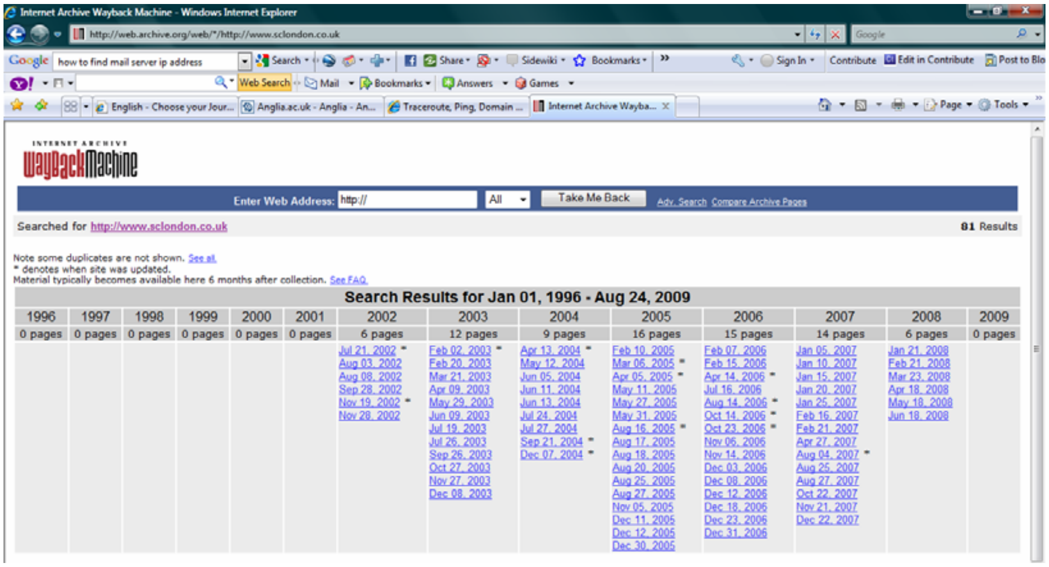
www.hemantabaral.com

Apache Technical Support
Enterprise Production Support 24 x 7, Get a Support Quote Today
www.OpenLogic.com/Apach

SQL Server 2000 Tuning
Tune SQL Server 2000 Performance, Save on Costs, Free Trial Download!
www.Confio.com

When was the first web page put up …………… and what did it look like?

First web page was put up: **July 21, 2002**



Internet Archive Wayback Machine - Windows Internet Explorer

http://web.archive.org/web/*/http://www.sclondon.co.uk

Enter Web Address: http:// All Take Me Back Adv. Search Compare Archive Pages

Searched for http://www.sclondon.co.uk 81 Results

Note some duplicates are not shown. See all.
* denotes when site was updated.
Material typically becomes available here 6 months after collection. See FAQ.

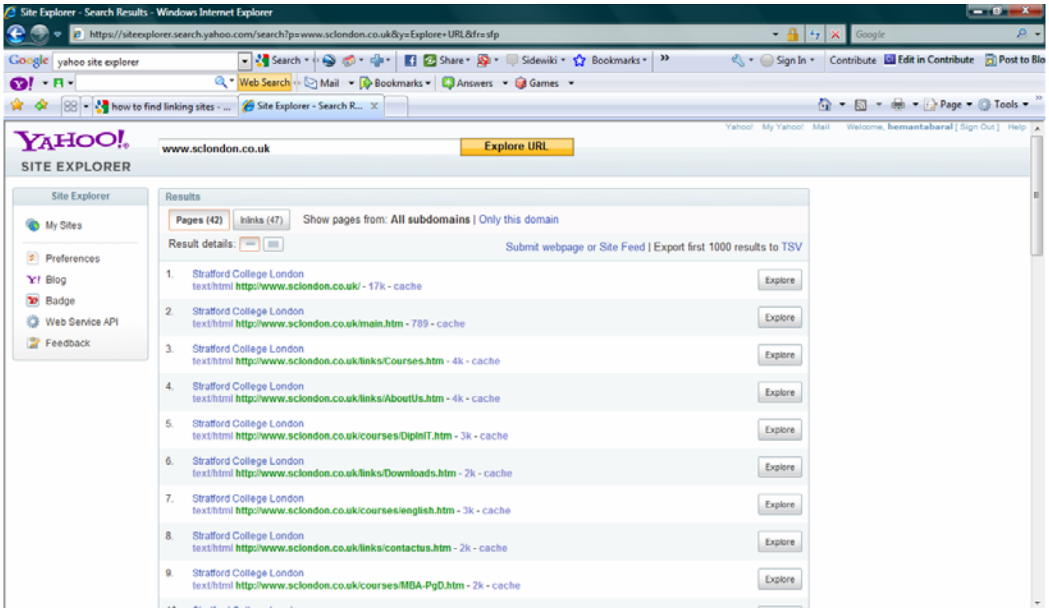
Search Results for Jan 01, 1996 - Aug 24, 2009

1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009
0 pages	0 pages	0 pages	0 pages	0 pages	0 pages	6 pages	12 pages	9 pages	16 pages	15 pages	14 pages	6 pages	0 pages
						Jul 21, 2002 *	Feb 02, 2003 *	Apr 13, 2004 *	Feb 10, 2005	Feb 07, 2006	Jan 05, 2007	Jan 21, 2008	
						Aug 03, 2002	Feb 20, 2003	May 12, 2004	Mar 06, 2005 *	Feb 15, 2006	Jan 10, 2007	Feb 21, 2008	
						Aug 08, 2002	Mar 21, 2003	Jun 05, 2004	Apr 05, 2005 *	Apr 14, 2006 *	Jan 15, 2007	Mar 23, 2008	
						Sep 28, 2002	Apr 09, 2003	Jun 11, 2004	May 11, 2005	Jul 16, 2006	Jan 20, 2007	Apr 18, 2008	
						Nov 19, 2002 *	May 29, 2003	Jun 13, 2004	May 27, 2005	Aug 14, 2006 *	Jan 25, 2007	May 18, 2008	
						Nov 28, 2002	Jun 09, 2003	Jul 24, 2004	May 31, 2005	Oct 14, 2006 *	Feb 16, 2007	Jun 18, 2008	
							Jul 19, 2003	Jul 27, 2004	Aug 16, 2005 *	Oct 23, 2006 *	Feb 21, 2007		
							Jul 26, 2003	Sep 21, 2004 *	Aug 17, 2005	Nov 06, 2006	Apr 27, 2007		
							Sep 26, 2003	Dec 07, 2004 *	Aug 18, 2005	Nov 14, 2006	Aug 04, 2007 *		
							Oct 27, 2003		Aug 20, 2005	Dec 03, 2006	Aug 25, 2007		
							Nov 27, 2003		Aug 25, 2005	Dec 08, 2006	Aug 27, 2007		
							Dec 08, 2003		Aug 27, 2005	Dec 12, 2006	Oct 22, 2007		
									Nov 05, 2005	Dec 18, 2006	Nov 21, 2007		
									Dec 11, 2005	Dec 23, 2006	Dec 22, 2007		
									Dec 12, 2005	Dec 31, 2006			
									Dec 30, 2005				

Tool Used: www.archive.org
Tool Syntax: Web – www.sclondon.co.uk

Who is linking to this site?

For this purpose, you must have yahoo ID and password.
Tool Used: https://siteexplorer.search.yahoo.com/
Tool Syntax: www.sclondon.co.uk – Explore URL



Site Explorer - Search Results - Windows Internet Explorer

https://siteexplorer.search.yahoo.com/search?p=www.sclondon.co.uk&y=Explore+URL&fr=sfp

Welcome, hemantabaral [Sign Out]

YAHOO! SITE EXPLORER

www.sclondon.co.uk Explore URL

Results

Pages (42) Inlinks (47) Show pages from: All subdomains | Only this domain

Result details:

Submit webpage or Site Feed | Export first 1000 results to TSV

1. Stratford College London
text/html http://www.sclondon.co.uk/ - 17k - cache

2. Stratford College London
text/html http://www.sclondon.co.uk/main.htm - 789 - cache

3. Stratford College London
text/html http://www.sclondon.co.uk/links/Courses.htm - 4k - cache

4. Stratford College London
text/html http://www.sclondon.co.uk/links/AboutUs.htm - 4k - cache

5. Stratford College London
text/html http://www.sclondon.co.uk/courses/DiplnIT.htm - 3k - cache

6. Stratford College London
text/html http://www.sclondon.co.uk/links/Downloads.htm - 2k - cache

7. Stratford College London
text/html http://www.sclondon.co.uk/courses/english.htm - 3k - cache

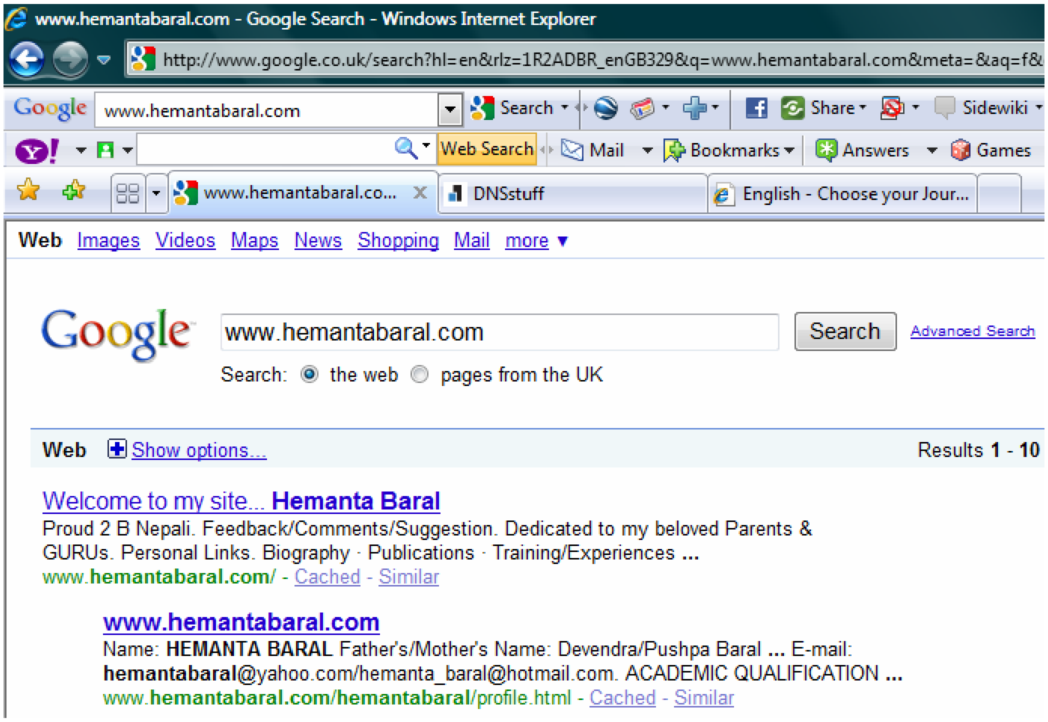
8. Stratford College London
text/html http://www.sclondon.co.uk/links/contactus.htm - 2k - cache

9. Stratford College London
text/html http://www.sclondon.co.uk/courses/MBA-PgD.htm - 2k - cache

---

Gather all other relevant publicly available network information (Google ?)

Tool Used: www.google.com
Tool Syntax: www.hemantabaral.com



www.hemantabaral.com

Search: ● the web ○ pages from the UK

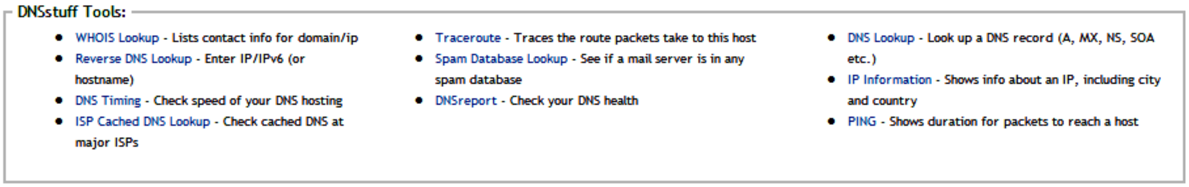
Web Results **1** - **10**

Welcome to my site... **Hemanta Baral**
Proud 2 B Nepali. Feedback/Comments/Suggestion. Dedicated to my beloved Parents & GURUs. Personal Links. Biography · Publications · Training/Experiences **...**
www.**hemantabaral.com**/ - Cached - Similar

www.hemantabaral.com
Name: **HEMANTA BARAL** Father's/Mother's Name: Devendra/Pushpa Baral **...** E-mail: **hemantabaral**@yahoo.com/hemanta_baral@hotmail.com. ACADEMIC QUALIFICATION **...**
www.**hemantabaral.com**/**hemantabaral**/profile.html - Cached - Similar

Find all information in one place

www.dnsstuff.com



DNSstuff Tools:

- WHOIS Lookup - Lists contact info for domain/ip
- Reverse DNS Lookup - Enter IP/IPv6 (or hostname)
- DNS Timing - Check speed of your DNS hosting
- ISP Cached DNS Lookup - Check cached DNS at major ISPs
- Traceroute - Traces the route packets take to this host
- Spam Database Lookup - See if a mail server is in any spam database
- DNSreport - Check your DNS health
- DNS Lookup - Look up a DNS record (A, MX, NS, SOA etc.)
- IP Information - Shows info about an IP, including city and country
- PING - Shows duration for packets to reach a host

2. ASSESS

Experiments:

1. Use **ping** to confirm local network connectivity.

   From the command line, type '**ipconfig'** to identify your own IP address.

   Ping your own IP address and other hosts with similar IP addresses.
2. Use **traceroute** to test access to the Internet using a target IP address.
3. Use **nslookup** to query about the DNS information
4. Use **netstat** to check whether the network is functioning or not
5. Use **nmap** to run a ping sweep of the local network.
6. Use **nmap and zenmap** to try different scan types.

PING

Pinging is a command which tells you if the connection between your computer and a particular domain is working correctly. If you are having connectivity problems, you can use the **ping** command to check the destination IP address you want to reach and record the results. The **ping** command displays whether the destination responded and how long it took to receive a reply. If there is an error in the delivery to the destination, the **ping** command displays an error message.

You can use the **ping** command to:

- Ping your computer (by address, not host name) to determine that TCP/IP is functioning. (Pinging your computer does not verify that your network adapter is functioning.)
- Ping the local router to determine whether the router is running.
- Ping beyond your local router.

You can run the ping command on a Windows computer by opening an MSDOS window and then typing "ping" followed by the domain name or IP address of the computer you wish to ping. You can list the available options for the Windows ping command with "ping -?".

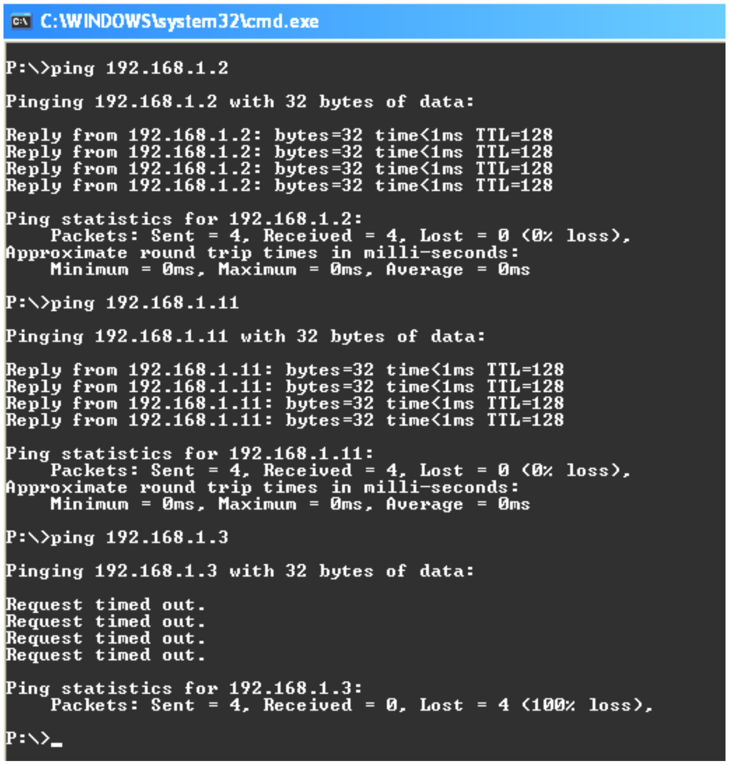
Use of PING command

In Windows, select Start > Programs > Accessories > Command Prompt

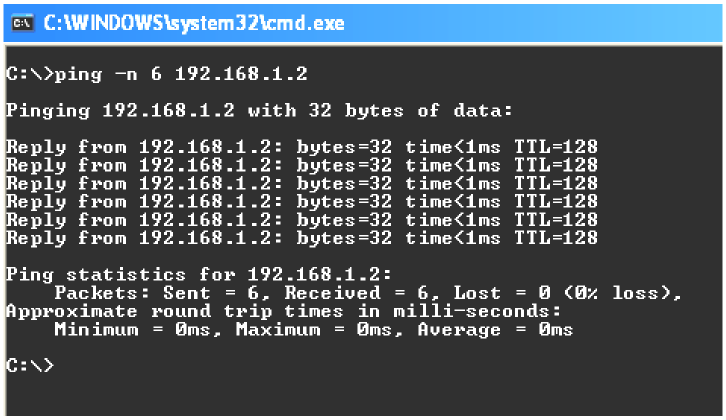
OR,

Start – Run (or start search) – type **cmd** then press Enter key.

To check connectivity by using the **ping** command, at the command prompt, type **ping** and the IP address you want to reach.



```
P:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

P:\>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:

Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

P:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

P:\>_
```



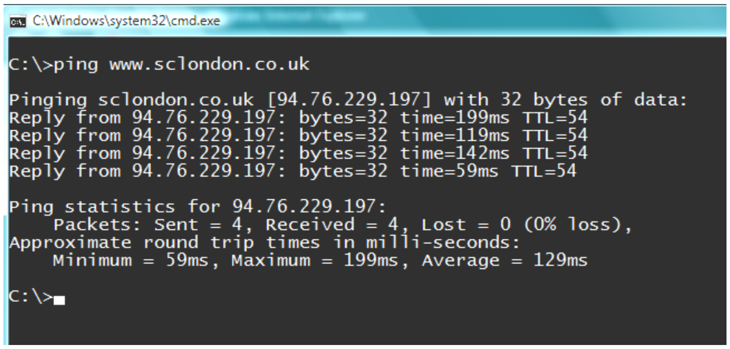
```
C:\>ping -n 6 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 6, Received = 6, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

A response of "Request timed out" means that there was no response to the ping in the default time period (1 second). You can check for the following:

- A router is down.
  To check the routers in the path between the source and the destination, use the **tracert** command.
- The destination host is down.
- There is no route back to your computer.
- The latency of the response is more than one second.
  Use the **-w** option on the **ping** command to increase the time-out. For example, to allow responses within 5 seconds, use **ping -w 5000**.

Pinging domain name

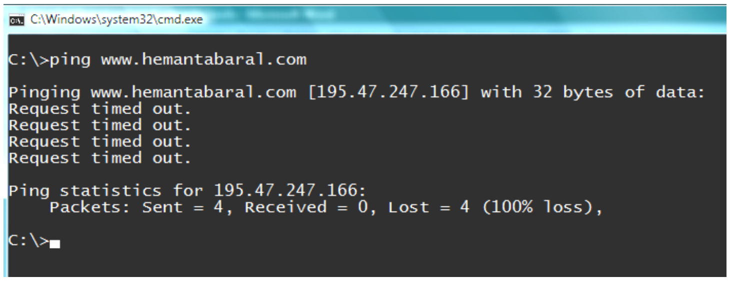
Enter the word ping, followed by a space, then the domain name.



C:\Windows\system32\cmd.exe

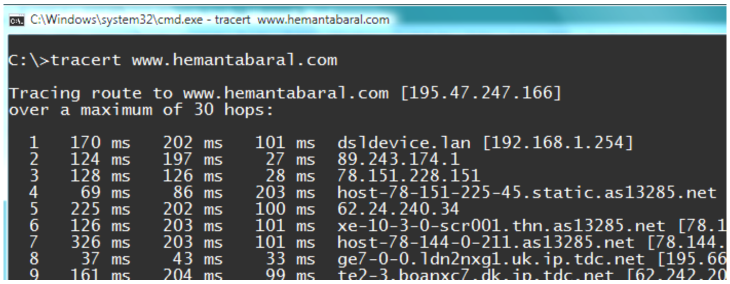
```
C:\>ping www.sclondon.co.uk

Pinging sclondon.co.uk [94.76.229.197] with 32 bytes of data:
Reply from 94.76.229.197: bytes=32 time=199ms TTL=54
Reply from 94.76.229.197: bytes=32 time=119ms TTL=54
Reply from 94.76.229.197: bytes=32 time=142ms TTL=54
Reply from 94.76.229.197: bytes=32 time=59ms TTL=54

Ping statistics for 94.76.229.197:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 59ms, Maximum = 199ms, Average = 129ms

C:\>
```

If the results show a series of replies, the connection is working. The time shows you how fast the connection is. If you see a "timed out" error instead of a reply, there is a breakdown somewhere between your computer and the domain. In this case the next step is to perform a traceroute.



C:\Windows\system32\cmd.exe

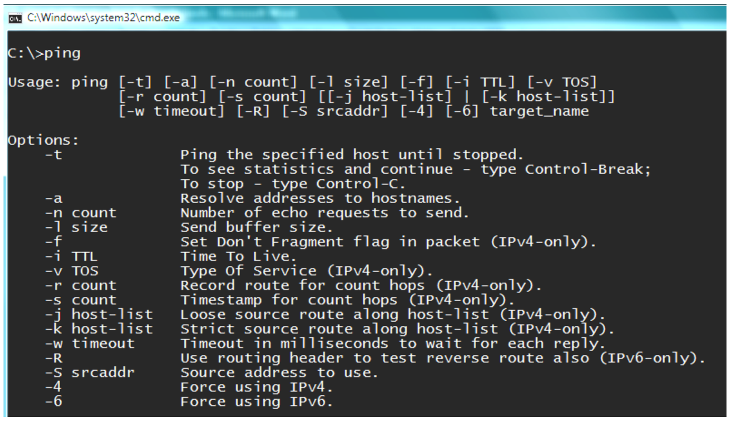
```
C:\>ping www.hemantabaral.com

Pinging www.hemantabaral.com [195.47.247.166] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 195.47.247.166:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```



C:\Windows\system32\cmd.exe - tracert www.hemantabaral.com

```
C:\>tracert www.hemantabaral.com

Tracing route to www.hemantabaral.com [195.47.247.166]
over a maximum of 30 hops:

  1   170 ms   202 ms   101 ms  dsldevice.lan [192.168.1.254]
  2   124 ms   197 ms    27 ms  89.243.174.1
  3   128 ms   126 ms    28 ms  78.151.228.151
  4    69 ms    86 ms   203 ms  host-78-151-225-45.static.as13285.net
  5   225 ms   202 ms   100 ms  62.24.240.34
  6   126 ms   203 ms   101 ms  xe-10-3-0-scr001.thn.as13285.net [78.1
  7   326 ms   203 ms   101 ms  host-78-144-0-211.as13285.net [78.144.
  8    37 ms    43 ms    33 ms  ge7-0-0.ldn2nxg1.uk.ip.tdc.net [195.66
  9   161 ms   204 ms    99 ms  te2-3.boanxc7.dk.ip.tdc.net [62.242.20
```

Ping options:



C:\Windows\system32\cmd.exe

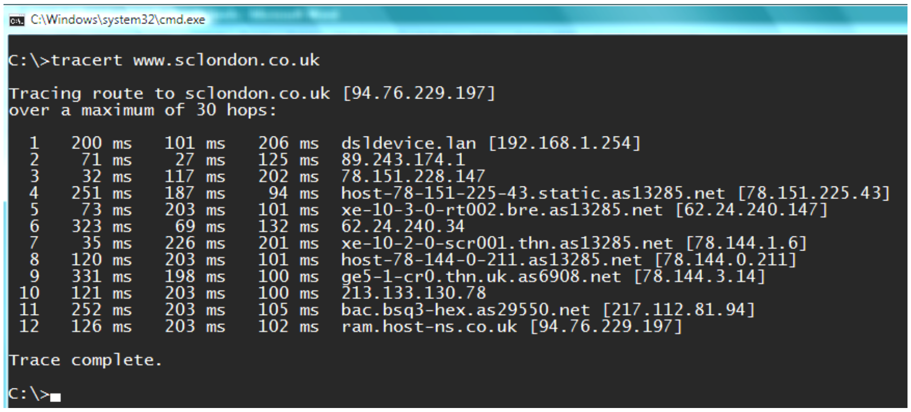
```
C:\>ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
    -S srcaddr     Source address to use.
    -4             Force using IPv4.
    -6             Force using IPv6.
```

TRACEROUTE (TRACERT)

Traceroute is a command which can show you the path a packet of information takes from your computer to one you specify. It will list all the routers it passes through until it reaches its destination, or fails to and is discarded. In addition to this, it will tell you how long each 'hop' from router to router takes.

In Windows, select Start > Programs > Accessories > Command Prompt.
OR,
Start – Run (or start search) – type **cmd** then press Enter key.

Enter the word **tracert**, followed by a space, then the domain name.

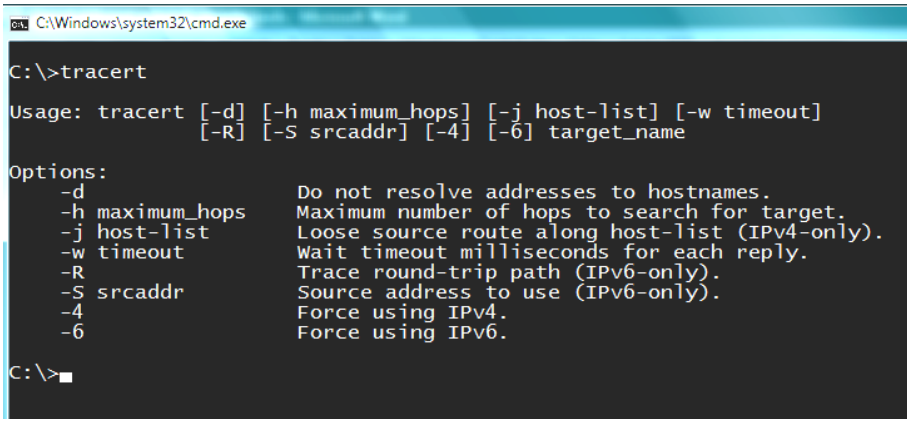


```
C:\>tracert www.sclondon.co.uk

Tracing route to sclondon.co.uk [94.76.229.197]
over a maximum of 30 hops:

  1   200 ms   101 ms   206 ms  dsldevice.lan [192.168.1.254]
  2    71 ms    27 ms   125 ms  89.243.174.1
  3    32 ms   117 ms   202 ms  78.151.228.147
  4   251 ms   187 ms    94 ms  host-78-151-225-43.static.as13285.net [78.151.225.43]
  5    73 ms   203 ms   101 ms  xe-10-3-0-rt002.bre.as13285.net [62.24.240.147]
  6   323 ms    69 ms   132 ms  62.24.240.34
  7    35 ms   226 ms   201 ms  xe-10-2-0-scr001.thn.as13285.net [78.144.1.6]
  8   120 ms   203 ms   101 ms  host-78-144-0-211.as13285.net [78.144.0.211]
  9   331 ms   198 ms   100 ms  ge5-1-cr0.thn.uk.as6908.net [78.144.3.14]
 10   121 ms   203 ms   100 ms  213.133.130.78
 11   252 ms   203 ms   105 ms  bac.bsq3-hex.as29550.net [217.112.81.94]
 12   126 ms   203 ms   102 ms  ram.host-ns.co.uk [94.76.229.197]

Trace complete.

C:\>
```

This is extremely useful when trying to find out why a website is unreachable, as you will be able to see where the connection fails. If you have a website hosted somewhere, it would be a good idea to do a traceroute to it when it is working, so that when it fails, you can do another traceroute to it (which will probably time out if the website is unreachable) and compare them.

It is generally recommended that if you have a website that is unreachable, you should use both the traceroute and ping commands before you contact your ISP to complain. More often that not, there will be nothing to your ISP or hosting company can do about it.

Tracert options



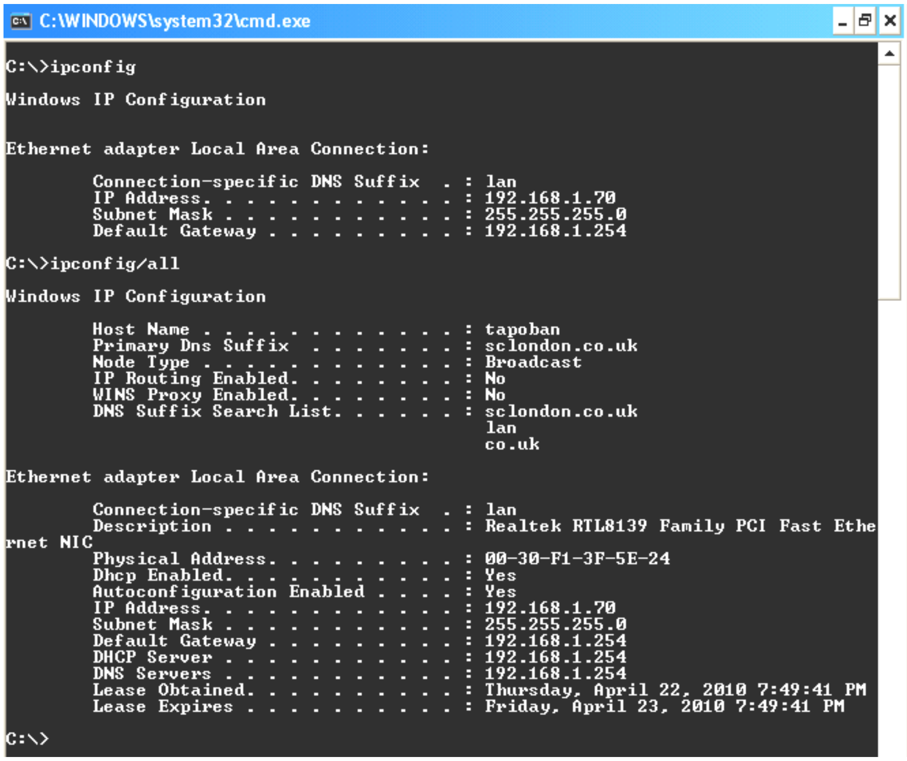
```
C:\>tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.

C:\>
```

IPCONFIG

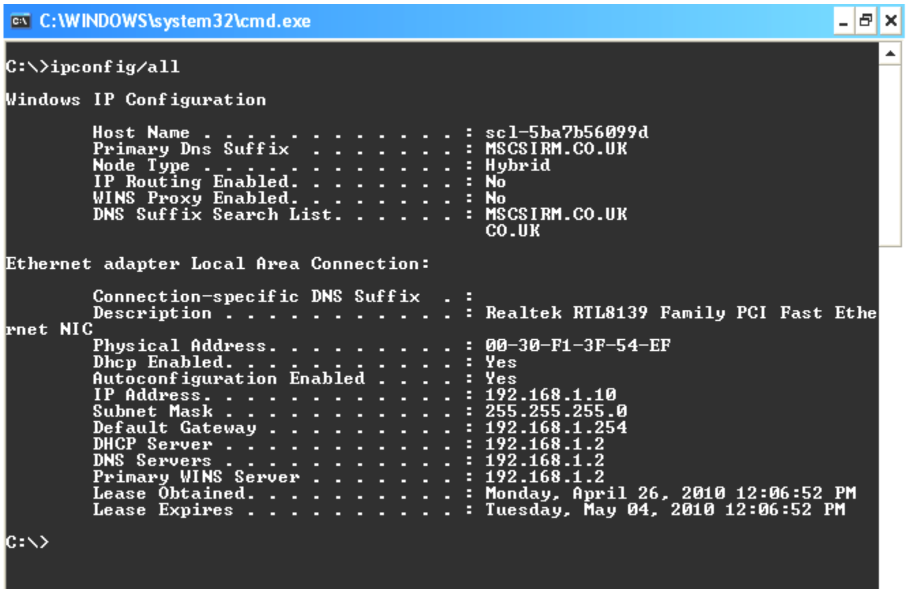
This command is useful in determining what could be wrong with a network.

This utility allows you to get the IP address information of a Windows computer. It also allows some control over active TCP/IP connections.

This command when used with the /all switch, reveal enormous amounts of troubleshooting information within the system. This option displays the same IP addressing information for each adapter as the default option. Additionally, it displays DNS and WINS settings for each adapter.



```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : lan
        IP Address. . . . . . . . . . . . : 192.168.1.70
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.254

C:\>ipconfig/all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : tapoban
        Primary Dns Suffix  . . . . . . . : sclondon.co.uk
        Node Type . . . . . . . . . . . . : Broadcast
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : sclondon.co.uk
                                            lan
                                            co.uk

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : lan
        Description . . . . . . . . . . . : Realtek RTL8139 Family PCI Fast Ethe
rnet NIC
        Physical Address. . . . . . . . . : 00-30-F1-3F-5E-24
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.1.70
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.254
        DHCP Server . . . . . . . . . . . : 192.168.1.254
        DNS Servers . . . . . . . . . . . : 192.168.1.254
        Lease Obtained. . . . . . . . . . : Thursday, April 22, 2010 7:49:41 PM
        Lease Expires . . . . . . . . . . : Friday, April 23, 2010 7:49:41 PM

C:\>
```



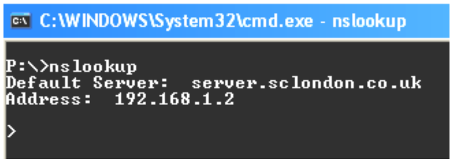
```
C:\>ipconfig/all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : scl-5ba7b56099d
        Primary Dns Suffix  . . . . . . . : MSCSIRM.CO.UK
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : MSCSIRM.CO.UK
                                            CO.UK

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Realtek RTL8139 Family PCI Fast Ethe
rnet NIC
        Physical Address. . . . . . . . . : 00-30-F1-3F-54-EF
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.1.10
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.254
        DHCP Server . . . . . . . . . . . : 192.168.1.2
        DNS Servers . . . . . . . . . . . : 192.168.1.2
        Primary WINS Server . . . . . . . : 192.168.1.2
        Lease Obtained. . . . . . . . . . : Monday, April 26, 2010 12:06:52 PM
        Lease Expires . . . . . . . . . . : Tuesday, May 04, 2010 12:06:52 PM

C:\>
```

NSLOOKUP

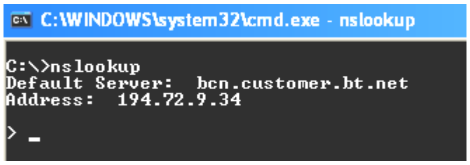
You can use the Name Server Lookup (NSLOOKUP) command to query the Domain Name Service for information about domain names and IP addresses. If you enter a domain name, you get back the IP address to which it corresponds, and if you enter an IP number, then you get back the domain name to which it corresponds. In practice, NSLOOKUP reaches out over the *Internet* to do a DNS lookup from an authorized name server, and then formats the information returned for convenient display.

If you first set the type to mx with the command "set type=mx", then NSLOOKUP also returns all sorts of interesting information about the name server that manages the domain that you look up. For additional fun, you can lookup the IP addresses and domain names returned by your first NSLOOKUP query and follow the chain of server administration backward. You end the NSLOOKUP program by typing "exit". Resources are provided below for running NSLOOKUP on operating systems and websites, and references provided for a similar system called Dig.

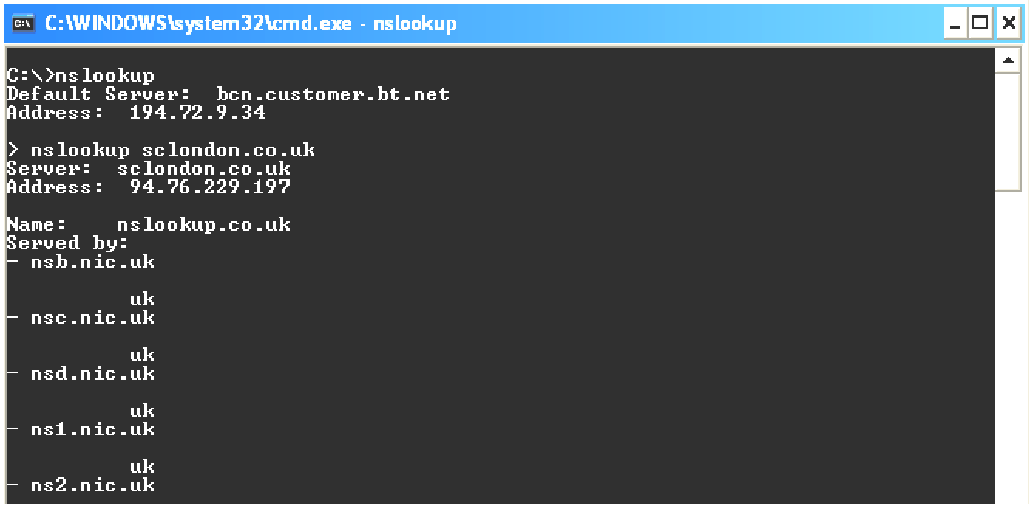
Example:



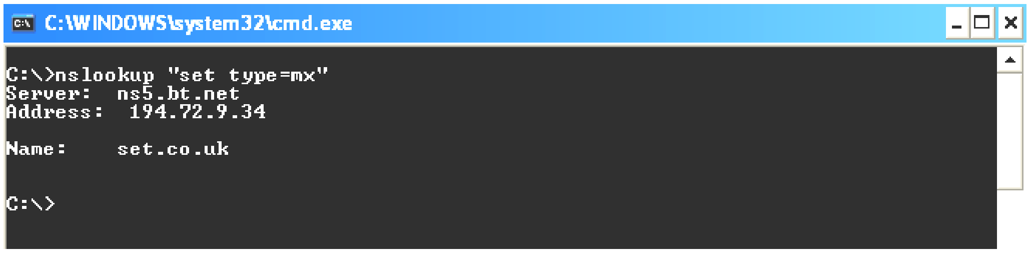
```
P:\>nslookup
Default Server:  server.sclondon.co.uk
Address:  192.168.1.2

>
```



```
C:\>nslookup
Default Server:  bcn.customer.bt.net
Address:  194.72.9.34

> _
```



```
C:\>nslookup
Default Server:  bcn.customer.bt.net
Address:  194.72.9.34

> nslookup sclondon.co.uk
Server:  sclondon.co.uk
Address:  94.76.229.197

Name:    nslookup.co.uk
Served by:
- nsb.nic.uk

          uk
- nsc.nic.uk

          uk
- nsd.nic.uk

          uk
- ns1.nic.uk

          uk
- ns2.nic.uk
```

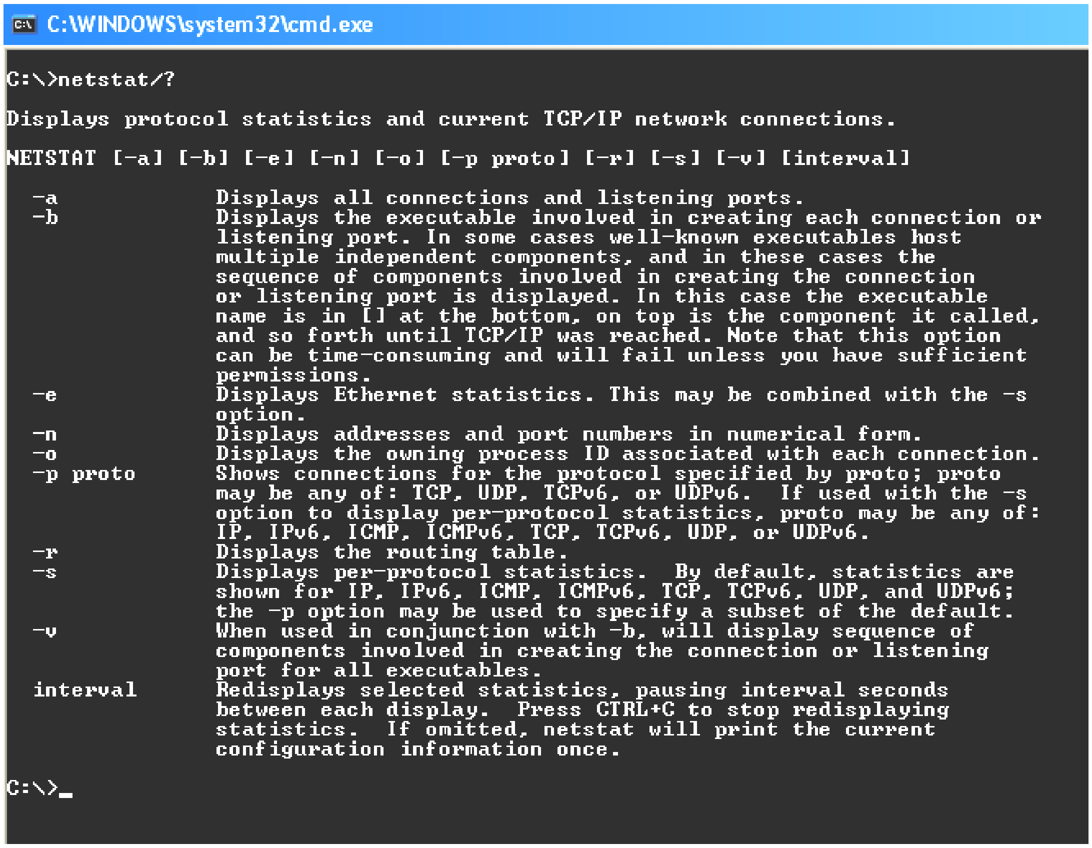


```
C:\>nslookup "set type=mx"
Server:  ns5.bt.net
Address:  194.72.9.34

Name:    set.co.uk


C:\>
```

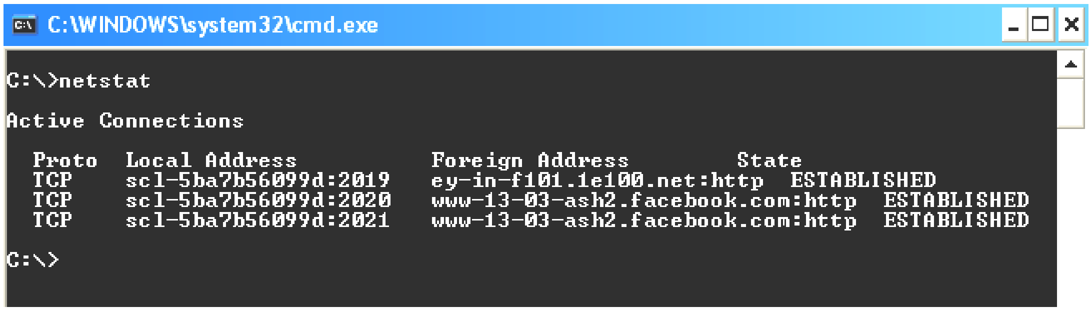
NETSTAT

NETSTAT is a useful tool available to check the functioning of a network. It provides a way to check if various aspects of TCP/IP are working and what connections are present.

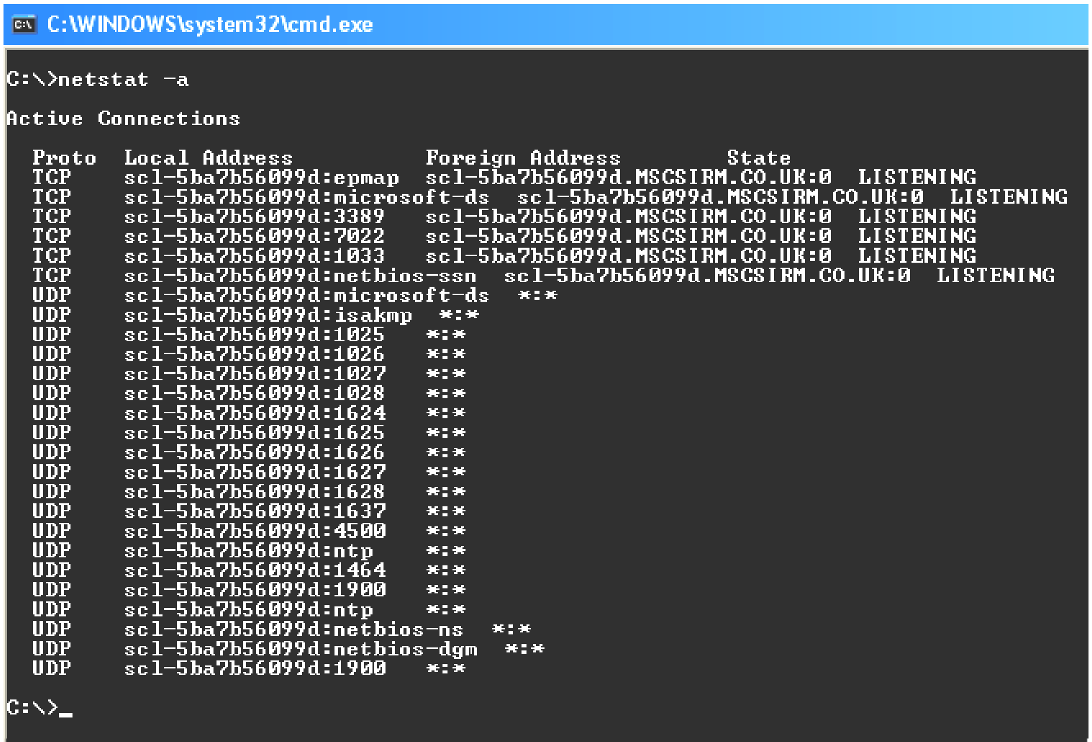
NETSTAT is used to look up the various active connections within a computer. It is helpful to understand what computers or networks you are connected to. This allows you to further investigate problems. One host may be responding well but another may be less responsive.



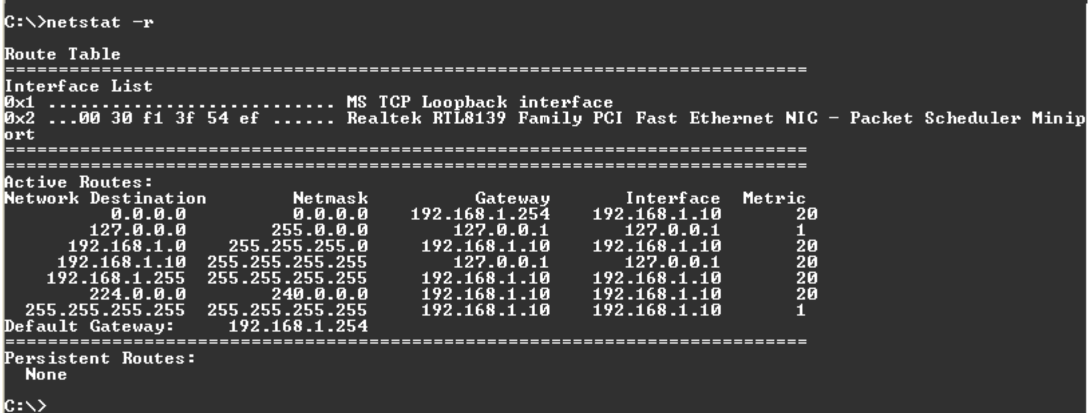
```
C:\>netstat/?

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-n] [-o] [-p proto] [-r] [-s] [-v] [interval]

  -a            Displays all connections and listening ports.
  -b            Displays the executable involved in creating each connection or
                listening port. In some cases well-known executables host
                multiple independent components, and in these cases the
                sequence of components involved in creating the connection
                or listening port is displayed. In this case the executable
                name is in [] at the bottom, on top is the component it called,
                and so forth until TCP/IP was reached. Note that this option
                can be time-consuming and will fail unless you have sufficient
                permissions.
  -e            Displays Ethernet statistics. This may be combined with the -s
                option.
  -n            Displays addresses and port numbers in numerical form.
  -o            Displays the owning process ID associated with each connection.
  -p proto      Shows connections for the protocol specified by proto; proto
                may be any of: TCP, UDP, TCPv6, or UDPv6.  If used with the -s
                option to display per-protocol statistics, proto may be any of:
                IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
  -r            Displays the routing table.
  -s            Displays per-protocol statistics.  By default, statistics are
                shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6;
                the -p option may be used to specify a subset of the default.
  -v            When used in conjunction with -b, will display sequence of
                components involved in creating the connection or listening
                port for all executables.
  interval      Redisplays selected statistics, pausing interval seconds
                between each display.  Press CTRL+C to stop redisplaying
                statistics.  If omitted, netstat will print the current
                configuration information once.

C:\>_
```



```
C:\>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    scl-5ba7b56099d:2019   ey-in-f101.1e100.net:http  ESTABLISHED
  TCP    scl-5ba7b56099d:2020   www-13-03-ash2.facebook.com:http  ESTABLISHED
  TCP    scl-5ba7b56099d:2021   www-13-03-ash2.facebook.com:http  ESTABLISHED

C:\>
```



```
C:\>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    scl-5ba7b56099d:epmap  scl-5ba7b56099d.MSCSIRM.CO.UK:0  LISTENING
  TCP    scl-5ba7b56099d:microsoft-ds  scl-5ba7b56099d.MSCSIRM.CO.UK:0  LISTENING
  TCP    scl-5ba7b56099d:3389   scl-5ba7b56099d.MSCSIRM.CO.UK:0  LISTENING
  TCP    scl-5ba7b56099d:7022   scl-5ba7b56099d.MSCSIRM.CO.UK:0  LISTENING
  TCP    scl-5ba7b56099d:1033   scl-5ba7b56099d.MSCSIRM.CO.UK:0  LISTENING
  TCP    scl-5ba7b56099d:netbios-ssn  scl-5ba7b56099d.MSCSIRM.CO.UK:0  LISTENING
  UDP    scl-5ba7b56099d:microsoft-ds  *:*
  UDP    scl-5ba7b56099d:isakmp  *:*
  UDP    scl-5ba7b56099d:1025   *:*
  UDP    scl-5ba7b56099d:1026   *:*
  UDP    scl-5ba7b56099d:1027   *:*
  UDP    scl-5ba7b56099d:1028   *:*
  UDP    scl-5ba7b56099d:1624   *:*
  UDP    scl-5ba7b56099d:1625   *:*
  UDP    scl-5ba7b56099d:1626   *:*
  UDP    scl-5ba7b56099d:1627   *:*
  UDP    scl-5ba7b56099d:1628   *:*
  UDP    scl-5ba7b56099d:1637   *:*
  UDP    scl-5ba7b56099d:4500   *:*
  UDP    scl-5ba7b56099d:ntp    *:*
  UDP    scl-5ba7b56099d:1464   *:*
  UDP    scl-5ba7b56099d:1900   *:*
  UDP    scl-5ba7b56099d:ntp    *:*
  UDP    scl-5ba7b56099d:netbios-ns  *:*
  UDP    scl-5ba7b56099d:netbios-dgm  *:*
  UDP    scl-5ba7b56099d:1900   *:*

C:\>_
```



```
C:\>netstat -r

Route Table
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 30 f1 3f 54 ef ...... Realtek RTL8139 Family PCI Fast Ethernet NIC - Packet Scheduler Minip
ort
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.1.254    192.168.1.10       20
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
      192.168.1.0    255.255.255.0     192.168.1.10    192.168.1.10       20
     192.168.1.10  255.255.255.255        127.0.0.1       127.0.0.1       20
    192.168.1.255  255.255.255.255     192.168.1.10    192.168.1.10       20
        224.0.0.0        240.0.0.0     192.168.1.10    192.168.1.10       20
  255.255.255.255  255.255.255.255     192.168.1.10    192.168.1.10       1
Default Gateway:     192.168.1.254
===========================================================================
Persistent Routes:
  None

C:\>
```

Nmap

Nmap is a port scanner. A port scanner scans for open ports, such as 80 (http) or 25 (SMTP). It is an extremely powerful tool for identifying remote hosts. It is capable of identifying active hosts (e.g., an ICMP ping scan) and transport layer ports (TCP and UDP). In addition, it contains fingerprinting capabilities.

Nmap not only identifies available TCP network services on a remote host, but it can attempt to identify the type of services (Web, email, etc.) and identify remote operating systems.

Nmap has got the following features:

- Portscanner
- Service identification
- OS identification

- Traceroute
- Limited vulnerability scanning

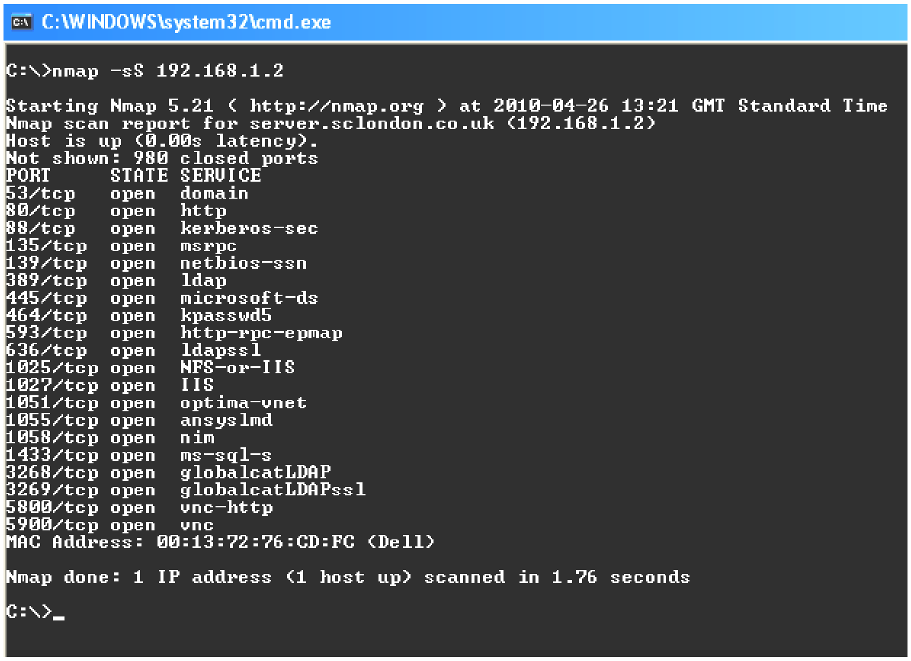
The following are the most useful uses of nmap.

-sT TCP connect() port scan (default)

This option is the most simple and straightforward. It performs a simple connect() system call on any interesting port on the target machine. This type of scan is easily detected by intrusion detection software.

-sS TCP SYN stealth port scan (best all-around TCP scan)

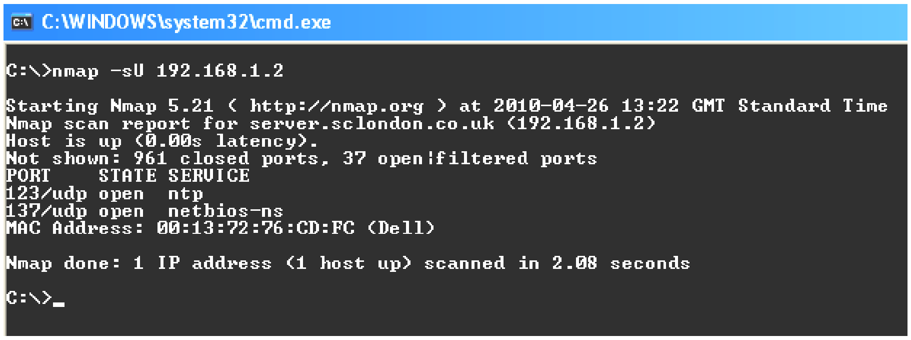
This technique is often referred to as "half-open" scanning, because you don't open a full TCP connection. You send a SYN packet, as if you are going to open a real connection and you wait for a response. A SYN|ACK indicates the port is listening. A RST is indicative of a non-listener. If a SYN|ACK is received, a RST is immediately sent to tear down the connection. The primary advantage to this scanning technique is that fewer sites will log it. Unfortunately you need root privileges to build these custom SYN packets.



```
C:\>nmap -sS 192.168.1.2

Starting Nmap 5.21 ( http://nmap.org ) at 2010-04-26 13:21 GMT Standard Time
Nmap scan report for server.sclondon.co.uk (192.168.1.2)
Host is up (0.00s latency).
Not shown: 980 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
1025/tcp open  NFS-or-IIS
1027/tcp open  IIS
1051/tcp open  optima-vnet
1055/tcp open  ansyslmd
1058/tcp open  nim
1433/tcp open  ms-sql-s
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
5800/tcp open  vnc-http
5900/tcp open  vnc
MAC Address: 00:13:72:76:CD:FC (Dell)

Nmap done: 1 IP address (1 host up) scanned in 1.76 seconds

C:\>_
```

-sU UDP port scan

UDP scans: This method is used to determine which UDP (User Datagram Protocol, RFC 768) ports are open on a host. The technique is to send 0 byte udp packets to each port on the target machine. If we receive an ICMP port unreachable message, then the port is closed. Otherwise we assume it is open.



```
C:\>nmap -sU 192.168.1.2

Starting Nmap 5.21 ( http://nmap.org ) at 2010-04-26 13:22 GMT Standard Time
Nmap scan report for server.sclondon.co.uk (192.168.1.2)
Host is up (0.00s latency).
Not shown: 961 closed ports, 37 open|filtered ports
PORT    STATE SERVICE
123/udp open  ntp
137/udp open  netbios-ns
MAC Address: 00:13:72:76:CD:FC (Dell)

Nmap done: 1 IP address (1 host up) scanned in 2.08 seconds

C:\>_
```

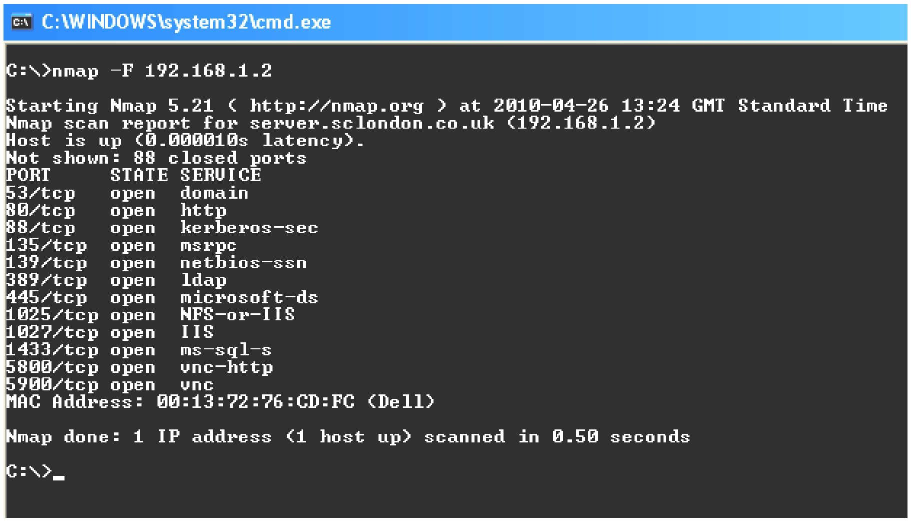
-sP ping scan (Find any reachable machines)

This option will simply attempt to ping any machine or range of machines listed.

-p ports to scan

Specify a range of ports to scan

-F Only scans ports listed in nmap-services



```
C:\>nmap -F 192.168.1.2

Starting Nmap 5.21 ( http://nmap.org ) at 2010-04-26 13:24 GMT Standard Time
Nmap scan report for server.sclondon.co.uk (192.168.1.2)
Host is up (0.000010s latency).
Not shown: 88 closed ports
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1027/tcp open  IIS
1433/tcp open  ms-sql-s
5800/tcp open  vnc-http
5900/tcp open  vnc
MAC Address: 00:13:72:76:CD:FC (Dell)

Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds

C:\>_
```

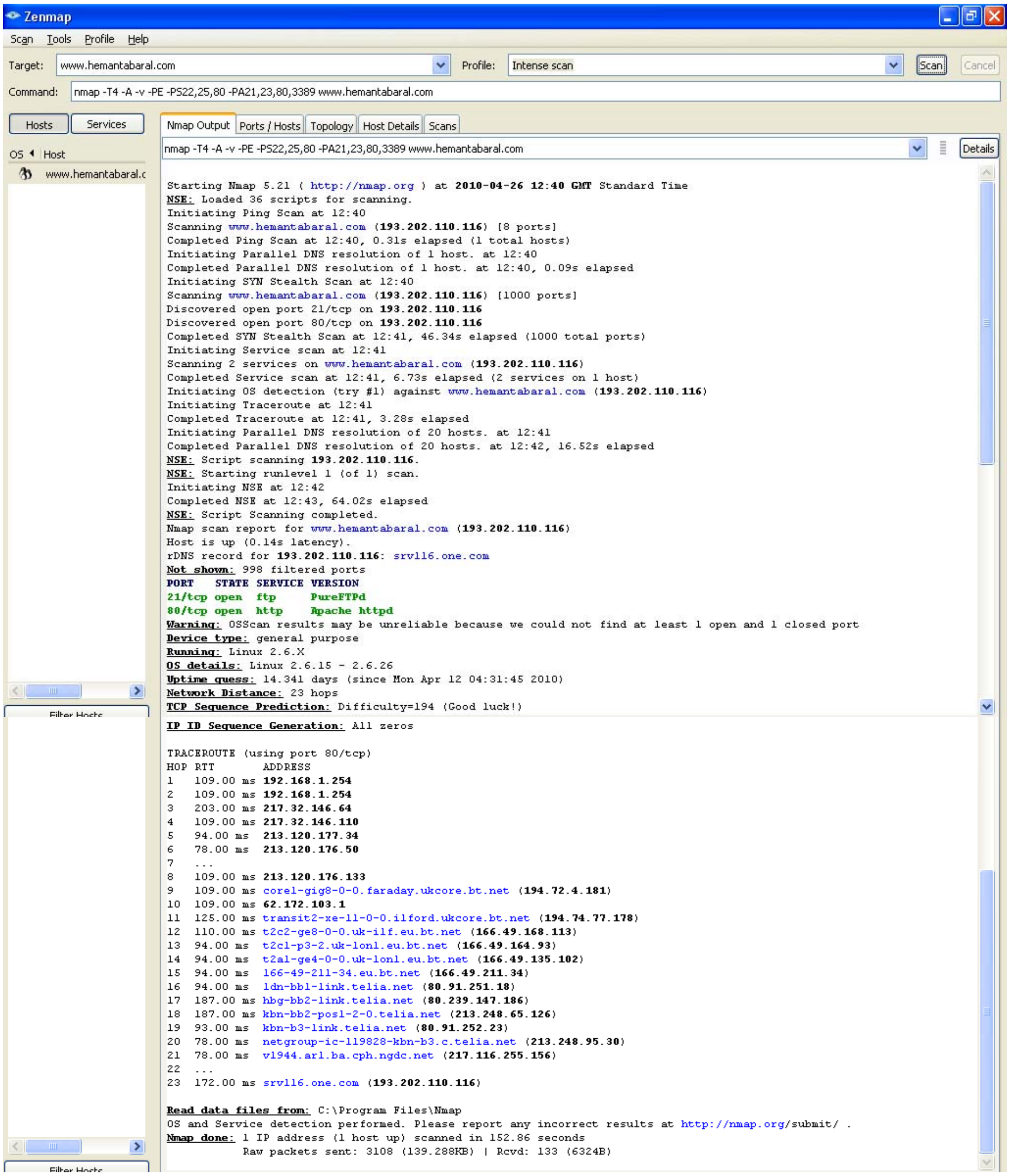
-T General timing policy

General timing policy is basically the rate at which packets are sent out. Main question here, is do you care if the network administrator for the IP or block you are scanning knows you are scanning it?

Zenmap

Zenmap is the official Nmap Security Scanner GUI. It is a multi-platform (Linux, Windows, Mac OS X, BSD, etc.) free and open source application which aims to make Nmap easy for beginners to use while providing advanced features for experienced Nmap users. Frequently used scans can be saved as profiles to make them easy to run repeatedly. A command creator allows interactive creation of Nmap command lines. Scan results can be saved and viewed later. Saved scan results can be compared with one another to see how they differ. The results of recent scans are stored in a searchable database.

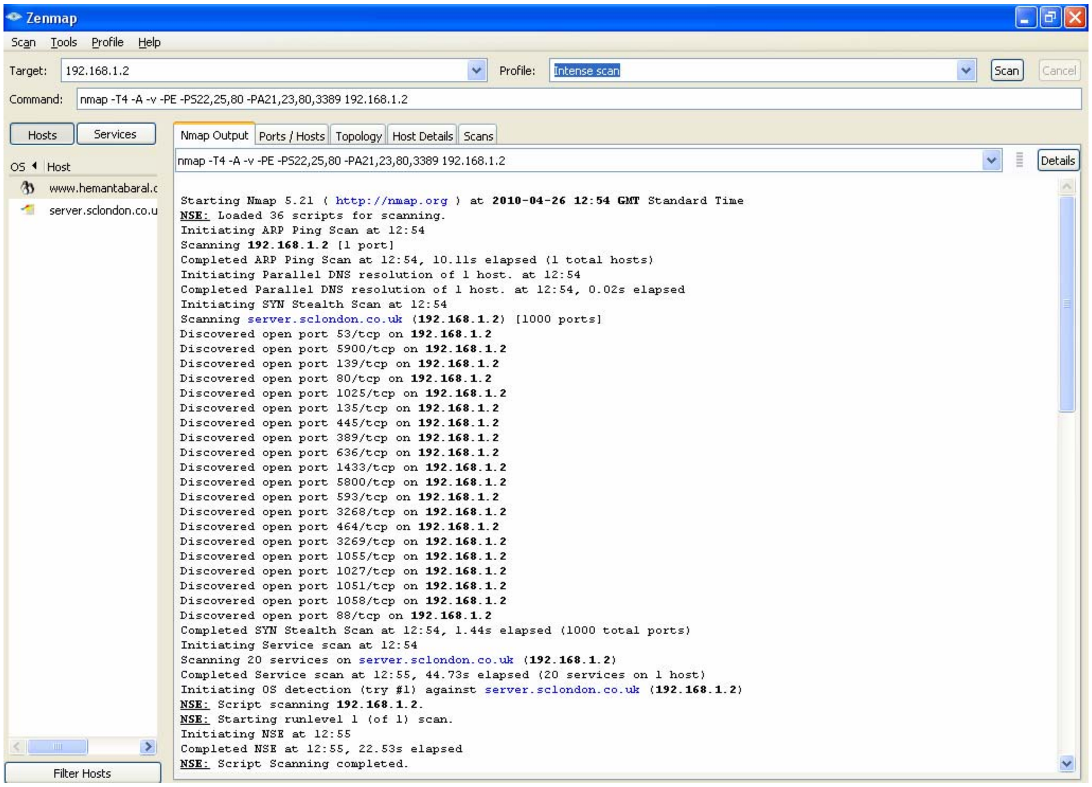
Example: www.hemantabaral.com



Target: www.hemantabaral.com
Profile: Intense scan
Command: nmap -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 www.hemantabaral.com

```
Starting Nmap 5.21 ( http://nmap.org ) at 2010-04-26 12:40 GMT Standard Time
NSE: Loaded 36 scripts for scanning.
Initiating Ping Scan at 12:40
Scanning www.hemantabaral.com (193.202.110.116) [8 ports]
Completed Ping Scan at 12:40, 0.31s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:40
Completed Parallel DNS resolution of 1 host. at 12:40, 0.09s elapsed
Initiating SYN Stealth Scan at 12:40
Scanning www.hemantabaral.com (193.202.110.116) [1000 ports]
Discovered open port 21/tcp on 193.202.110.116
Discovered open port 80/tcp on 193.202.110.116
Completed SYN Stealth Scan at 12:41, 46.34s elapsed (1000 total ports)
Initiating Service scan at 12:41
Scanning 2 services on www.hemantabaral.com (193.202.110.116)
Completed Service scan at 12:41, 6.73s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against www.hemantabaral.com (193.202.110.116)
Initiating Traceroute at 12:41
Completed Traceroute at 12:41, 3.28s elapsed
Initiating Parallel DNS resolution of 20 hosts. at 12:41
Completed Parallel DNS resolution of 20 hosts. at 12:42, 16.52s elapsed
NSE: Script scanning 193.202.110.116.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 12:42
Completed NSE at 12:43, 64.02s elapsed
NSE: Script Scanning completed.
Nmap scan report for www.hemantabaral.com (193.202.110.116)
Host is up (0.14s latency).
rDNS record for 193.202.110.116: srv116.one.com
Not shown: 998 filtered ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     PureFTPd
80/tcp open  http    Apache httpd
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.15 - 2.6.26
Uptime guess: 14.341 days (since Mon Apr 12 04:31:45 2010)
Network Distance: 23 hops
TCP Sequence Prediction: Difficulty=194 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   109.00 ms 192.168.1.254
2   109.00 ms 192.168.1.254
3   203.00 ms 217.32.146.64
4   109.00 ms 217.32.146.110
5   94.00 ms  213.120.177.34
6   78.00 ms  213.120.176.50
7   ...
8   109.00 ms 213.120.176.133
9   109.00 ms corel-gig8-0-0.faraday.ukcore.bt.net (194.72.4.181)
10  109.00 ms 62.172.103.1
11  125.00 ms transit2-xe-11-0-0.ilford.ukcore.bt.net (194.74.77.178)
12  110.00 ms t2c2-ge8-0-0.uk-ilf.eu.bt.net (166.49.168.113)
13  94.00 ms  t2cl-p3-2.uk-lonl.eu.bt.net (166.49.164.93)
14  94.00 ms  t2al-ge4-0-0.uk-lonl.eu.bt.net (166.49.135.102)
15  94.00 ms  166-49-211-34.eu.bt.net (166.49.211.34)
16  94.00 ms  ldn-bbl-link.telia.net (80.91.251.18)
17  187.00 ms hbg-bb2-link.telia.net (80.239.147.186)
18  187.00 ms kbn-bb2-posl-2-0.telia.net (213.248.65.126)
19  93.00 ms  kbn-b3-link.telia.net (80.91.252.23)
20  78.00 ms  netgroup-ic-119828-kbn-b3.c.telia.net (213.248.95.30)
21  78.00 ms  vl944.arl.ba.cph.ngdc.net (217.116.255.156)
22  ...
23  172.00 ms srv116.one.com (193.202.110.116)

Read data files from: C:\Program Files\Nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 152.86 seconds
           Raw packets sent: 3108 (139.288KB) | Rcvd: 133 (6324B)
```

Example: 192.168.1.2

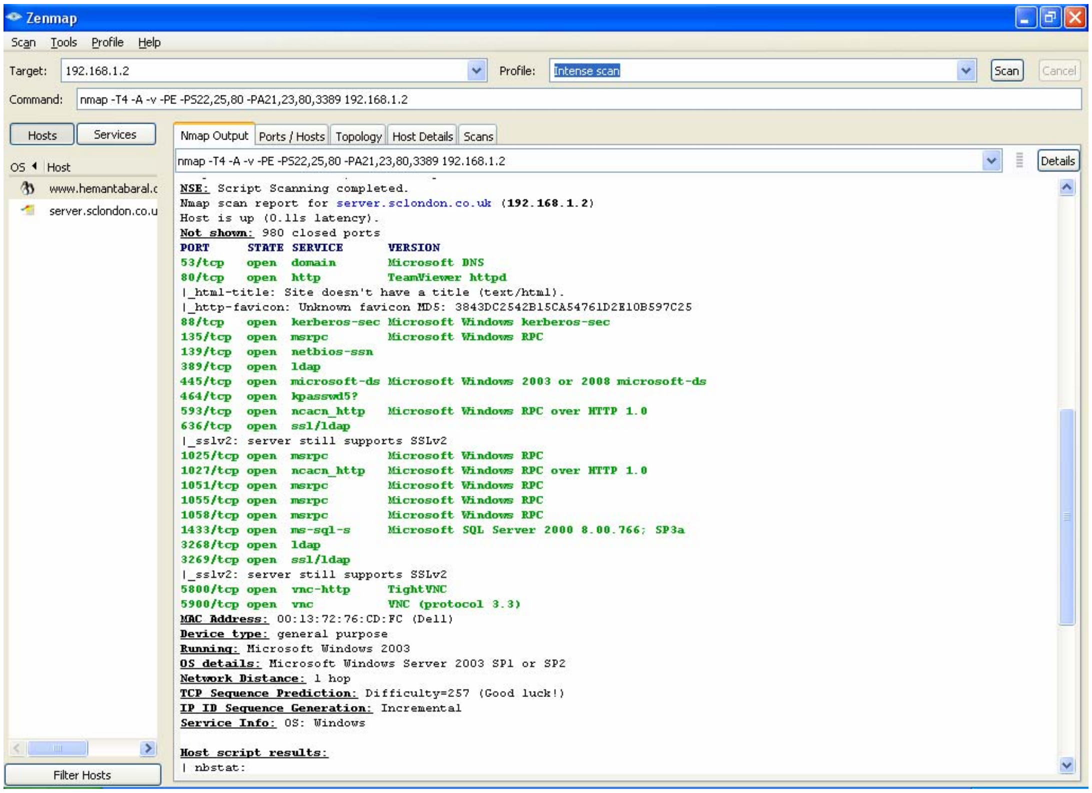


Target: 192.168.1.2

Profile: Intense scan

Command: nmap -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 192.168.1.2

```
Starting Nmap 5.21 ( http://nmap.org ) at 2010-04-26 12:54 GMT Standard Time
NSE: Loaded 36 scripts for scanning.
Initiating ARP Ping Scan at 12:54
Scanning 192.168.1.2 [1 port]
Completed ARP Ping Scan at 12:54, 10.11s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:54
Completed Parallel DNS resolution of 1 host. at 12:54, 0.02s elapsed
Initiating SYN Stealth Scan at 12:54
Scanning server.sclondon.co.uk (192.168.1.2) [1000 ports]
Discovered open port 53/tcp on 192.168.1.2
Discovered open port 5900/tcp on 192.168.1.2
Discovered open port 139/tcp on 192.168.1.2
Discovered open port 80/tcp on 192.168.1.2
Discovered open port 1025/tcp on 192.168.1.2
Discovered open port 135/tcp on 192.168.1.2
Discovered open port 445/tcp on 192.168.1.2
Discovered open port 389/tcp on 192.168.1.2
Discovered open port 636/tcp on 192.168.1.2
Discovered open port 1433/tcp on 192.168.1.2
Discovered open port 5800/tcp on 192.168.1.2
Discovered open port 593/tcp on 192.168.1.2
Discovered open port 3268/tcp on 192.168.1.2
Discovered open port 464/tcp on 192.168.1.2
Discovered open port 3269/tcp on 192.168.1.2
Discovered open port 1055/tcp on 192.168.1.2
Discovered open port 1027/tcp on 192.168.1.2
Discovered open port 1051/tcp on 192.168.1.2
Discovered open port 1058/tcp on 192.168.1.2
Discovered open port 88/tcp on 192.168.1.2
Completed SYN Stealth Scan at 12:54, 1.44s elapsed (1000 total ports)
Initiating Service scan at 12:54
Scanning 20 services on server.sclondon.co.uk (192.168.1.2)
Completed Service scan at 12:55, 44.73s elapsed (20 services on 1 host)
Initiating OS detection (try #1) against server.sclondon.co.uk (192.168.1.2)
NSE: Script scanning 192.168.1.2.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 12:55
Completed NSE at 12:55, 22.53s elapsed
NSE: Script Scanning completed.
```

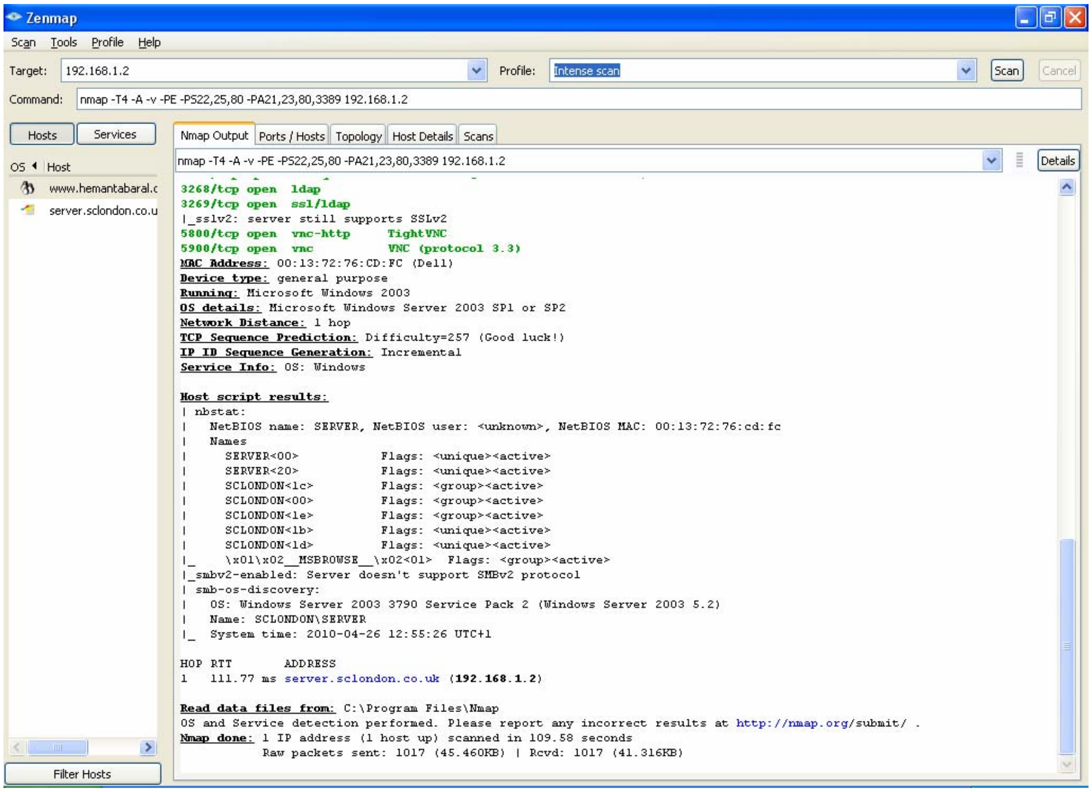


Target: 192.168.1.2

Profile: Intense scan

Command: nmap -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 192.168.1.2

```
NSE: Script Scanning completed.
Nmap scan report for server.sclondon.co.uk (192.168.1.2)
Host is up (0.11s latency).
Not shown: 980 closed ports
PORT     STATE SERVICE     VERSION
53/tcp   open  domain      Microsoft DNS
80/tcp   open  http        TeamViewer httpd
|_html-title: Site doesn't have a title (text/html).
|_http-favicon: Unknown favicon MD5: 3843DC2542B15CA54761D2E10B597C25
88/tcp   open  kerberos-sec Microsoft Windows kerberos-sec
135/tcp  open  msrpc       Microsoft Windows RPC
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds Microsoft Windows 2003 or 2008 microsoft-ds
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http  Microsoft Windows RPC over HTTP 1.0
636/tcp  open  ssl/ldap
|_sslv2: server still supports SSLv2
1025/tcp open  msrpc       Microsoft Windows RPC
1027/tcp open  ncacn_http  Microsoft Windows RPC over HTTP 1.0
1051/tcp open  msrpc       Microsoft Windows RPC
1055/tcp open  msrpc       Microsoft Windows RPC
1058/tcp open  msrpc       Microsoft Windows RPC
1433/tcp open  ms-sql-s    Microsoft SQL Server 2000 8.00.766; SP3a
3268/tcp open  ldap
3269/tcp open  ssl/ldap
|_sslv2: server still supports SSLv2
5800/tcp open  vnc-http    TightVNC
5900/tcp open  vnc         VNC (protocol 3.3)
MAC Address: 00:13:72:76:CD:FC (Dell)
Device type: general purpose
Running: Microsoft Windows 2003
OS details: Microsoft Windows Server 2003 SP1 or SP2
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows

Host script results:
| nbstat:
```



Target: 192.168.1.2

Profile: Intense scan

Command: nmap -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 192.168.1.2

```
nmap -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 192.168.1.2
3268/tcp open  ldap
3269/tcp open  ssl/ldap
|_sslv2: server still supports SSLv2
5800/tcp open  vnc-http     TightVNC
5900/tcp open  vnc          VNC (protocol 3.3)
MAC Address: 00:13:72:76:CD:FC (Dell)
Device type: general purpose
Running: Microsoft Windows 2003
OS details: Microsoft Windows Server 2003 SP1 or SP2
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows

Host script results:
| nbstat:
|   NetBIOS name: SERVER, NetBIOS user: <unknown>, NetBIOS MAC: 00:13:72:76:cd:fc
|   Names
|     SERVER<00>          Flags: <unique><active>
|     SERVER<20>          Flags: <unique><active>
|     SCLONDON<1c>        Flags: <group><active>
|     SCLONDON<00>        Flags: <group><active>
|     SCLONDON<1e>        Flags: <group><active>
|     SCLONDON<1b>        Flags: <unique><active>
|     SCLONDON<1d>        Flags: <unique><active>
|_    \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|_smbv2-enabled: Server doesn't support SMBv2 protocol
| smb-os-discovery:
|   OS: Windows Server 2003 3790 Service Pack 2 (Windows Server 2003 5.2)
|   Name: SCLONDON\SERVER
|_  System time: 2010-04-26 12:55:26 UTC+1

HOP RTT       ADDRESS
1   111.77 ms server.sclondon.co.uk (192.168.1.2)

Read data files from: C:\Program Files\Nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 109.58 seconds
           Raw packets sent: 1017 (45.460KB) | Rcvd: 1017 (41.316KB)
```

3. SECURITY

1. Developing a Security Policy

The first step any organization should take to protect its data and itself from a liability challenge is to develop a security policy. A policy is a set of principles that guide decision-making processes and enable leaders in an organization to distribute authority confidently. RFC2196 states that a "security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide." A security policy can be as simple as a brief Acceptable Use Policy for network resources, or it can be several hundred pages long and detail every element of connectivity and associated policies.

A security policy meets these goals:

- Informs users, staff, and managers of their obligatory requirements for protecting technology and information assets
- Specifies the mechanisms through which these requirements can be met
- Provides a baseline from which to acquire, configure, and audit computer systems and networks for compliance with the policy

Assembling a security policy can be daunting if it is undertaken without guidance. For this reason, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) have published a security standard document called ISO/IEC 27002. This document refers specifically to information technology and outlines a code of practice for information security management.

ISO/IEC 27002 is intended to be a common basis and practical guideline for developing organizational security standards and effective security management practices. The document consists of 12 sections:

- Risk assessment
- Security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development, and maintenance
- Information security incident management
- Business continuity management
- Compliance

2. Security of Physical threats

Place your systems (servers, routers, switches, appliances, management stations, etc.) in a controlled environment whenever feasible. Mission-critical equipment must be confined to computer rooms, server rooms, or wiring closets. Here are some recommendations for equipment security:

a. Physical threat mitigation

- Offer limited and locked (physical or electronic) access to authorized personnel only.
- The area should not be accessible through dropped ceilings, raised floors, windows, or ductwork, or point of entry other than the secured access point.
- An official, secured access point must be the only point of entry.
- Electronic access control should be implemented, if feasible, with all attempts to access logged by security systems and monitored by security personnel.
- Trained security personnel should monitor security cameras with automatic log recording if possible.
- Always follow ESD procedures when replacing or working inside hardware devices.

b. Environmental threat mitigation

- Create a proper operating environment through temperature control, humidity control, positive air flow, remote environmental alarming, and recording and monitoring.

c. Electrical threat mitigation

In addition to the electrical threats, electrical supply problems should be limited with the following measures:

- Install UPS (uninterruptible power supply) systems for mission-critical hardware.
- Deploy backup generator systems for mission-critical disaster recovery if feasible.
- Test and maintain UPS and/or generators based on the manufacturers' suggested preventative maintenance schedule.
- Monitor and alarm power-related parameters at the supply and device level.
- Use filtered power and install redundant power supplies on mission-critical devices.
- Perform remote alarming and monitoring system.

d. Maintenance threat mitigation

- Maintain critical spare parts and modules in case of emergencies.
- Don't leave a console, workstation, or management station logged on with administrative access when you leave the area for any significant amount of time. Be sure these systems are locked down with cables and locks as well.
- Maintain a regularly updated database of all hardware documentation and technical support information in case of emergencies.
- Label and secure cabling to equipment racks to protect against accidental disconnection or damage. This also helps prevent hardware from walking away with the assistance of thieves.
- Use cable runs and/or raceways to traverse rack-to-ceiling or rack-to-rack links.
- Use electrostatic discharge procedures
- Stock critical spares, and control access to console ports.

One of the most significant reasons for placing physical security as the top security layer is that it can often be implemented with low cost, diligence, and common sense. Remember that an entire fleet of expensive security software tools can quickly be rendered impotent if a malicious user can gain physical access to your corporate servers, networking devices, and management workstations.

3. Data Security

The second layer of security is data security, which involves a variety of complex mechanisms. This area consists of components to guard against unauthorized access to data in storage as well as data that is transmitted over communications networks, both private and public. This layer involves components such as integrity controls, and authentication, plus additional access controls and/or encryption mechanisms.

Integrity controls are mechanisms that ensure that the data being electronically stored or transmitted is valid. One of the best open standards for implementing data security is IPSec (Internet Protocol Security). This can include additional support for message and user authentication. Message authentication is the process of ensuring that the sent message exactly matches the received message. User authentication makes sure that the sender of the message is genuinely who they are supposed to be. Businesses can also use these technologies to guarantee accountability and reliability when exchanging electronic documents, such as contracts and agreements.

System access controls involve controlling access to corporate information, system and documentation files, electronic records and assets, and even data about customers or clients. User access management prevents unauthorized access to business information systems and computers as well. These access controls can also involve monitoring and auditing. Network operating systems from a number of vendors provide secure directories and file systems with access security measures and hardening techniques -- Microsoft Windows 2003 with Active Directory is a prominent example.

Encryption is any process or technology that uses cryptography to translate plaintext into cipher text. This is used to keep someone other than the intended recipient from reading the data. Encryption is often provided by third-party components or integrated code on the actual system boards. Digital signatures, certificates, and PKI (Public Key Infrastructure) tools can be used to provide this service.

4. Application Security

Application security mechanisms include the usage of secure program code, regular updates, patching, and fixing, and security policy software solutions to guarantee secure business application processes. Some programs introduced into the environment can be Trojan horse programs that are actually snippets of nefarious code in disguise. You should use antivirus software and software firewalls in concert with your corporate collaboration and productivity applications to protect against attacks.

5. Network Security

You absolutely must protect your internal corporate network and perimeter networks from intruders and malware using network firewalls (software and/or appliances), VPNs (virtual private networks), IDSs (intrusion detection systems), as well as web and content filtering for your enterprise. Network security is a constantly continuing and dynamic process.

Network security includes the following four steps:

1. **Secure:** Lock your networks with a combination of authentication, encryption, firewalls, and continuous patching of system vulnerabilities.

2. **Examine:** To maintain a secure network, you have to regularly monitor the state of security mechanisms, readiness, and incident handling procedures. Network vulnerability scanners from a number of reputable vendors will proactively locate areas of weakness, and IDSs can alert and respond to security events when they occur. Your organization can get high visibility of the network data stream and the security condition of the network using emerging security solutions.

3. **Test:** Equally as vital as network examination and assessment is testing. Without adequate testing of the security solutions, it's tough to know about new threats and attacks. The hacker community is an ever-changing continuum

with menacing designs on your systems and data. You can perform this testing yourself or you can outsource it to a third party.

4. **Enhance:** Use the information gathered from the Examine and Test phases to constantly enhance and improve the corporate security implementation and modify the security policy as new vulnerabilities and risks are identified and the business model changes.

Checklist for network security

Task 1 - Install and Use Anti-Virus Programs

Task 2 - Keep Your System Patched

Task 3 - Use Care When Reading Email with Attachments

Task 4 - Install and Use a Firewall Program

Task 5 - Make Backups of Important Files and Folders

Task 6 - Use Strong Passwords

Task 7 - Use Care When Downloading and Installing Programs

Task 8 - Install and Use a Hardware Firewall

Task 9 - Install and Use a File Encryption Program and Access Controls

Protect yourself from

1. Crimeware
2. Hacking
3. Phishing
4. Spam
5. Identity Theft
6. Malicious Codes

1. How to protect your system from crimeware?

There are several steps you can take to protect your system from today's cyber threats. Following guidelines will help to minimize the risk of attacks.

1. Protect your computer by installing Internet security software.
2. Install security patches for your operating system and applications.
3. If you receive an email with an attached file (Word documents, Excel spreadsheets, .EXE files, etc.) don't open it unless you know who sent it and only then if you're expecting it. NEVER open an attachment sent in an unsolicited (spam) email. The same is true for email messages or IM (Instant Messaging) messages that contain links.
4. Update your security software regularly (i.e. at least once a day).
5. Keep your other applications updated.
6. Only use your computer's Administrator account if you need to install software or make system changes. For everyday use, create a separate account with only limited access rights (this can be done through 'User Accounts' in 'Control Panel'). By doing this, you limit a malicious program's access to valuable system data.
7. Backup your data regularly to a CD, DVD, or external USB drive. If your files become damaged or encrypted by a malicious program you can then copy them back from your backup.

2. How to protect your system from hackers?

Hackers are like electronic burglars, who use loopholes in your programs - vulnerabilities - to break into your computer system. You can protect your system from hackers by using a **firewall**. A firewall program, which often comes as part of an anti-virus software package, protects a PC by detecting potential intruders and making the PC invisible to hackers.

Firewalls

Personal computers connected to the Internet through a dialup connection, DSL, or cable modems are as vulnerable as corporate networks. Personal firewalls reside on the PC of the user and attempt to prevent attacks. Personal firewalls are not designed for LAN implementations, such as appliance-based or server-based firewalls, and they may prevent network access if installed with other networking clients, services, protocols, or adapters.

Some personal firewall software vendors include McAfee, Norton, Symantec, and Zone Labs.

Intrusion detection systems

"Intrusion-prevention systems have a learning capability, and these engines are more intelligent and better able to identify and stop attacks,"

Intrusion detection systems (IDS) detect attacks against a network and send logs to a management console. Intrusion prevention systems (IPS) prevent attacks against the network and should provide the following active defense mechanisms in addition to detection:

Prevention - Stops the detected attack from executing.

Reaction - Immunizes the system from future attacks from a malicious source.

Either technology can be implemented at a network level or host level, or both for maximum protection.

Security is a top consideration whenever planning a network. In the past, the one device that would come to mind for network security was the firewall. A firewall by itself is no longer adequate for securing a network. An integrated approach involving firewall, intrusion prevention, and VPN is necessary.

3. How to protect from a phishing attack?

Phishing attacks can be prevented by educating users and implementing reporting guidelines when they receive suspicious e-mail. Administrators can also block access to certain web sites and configure filters that block suspicious e-mail.

1. Be very wary of any email messages asking for personal information. It's highly unlikely that your bank will request such information by email. If in doubt, call them to check!
2. Don't complete a form in an email message asking for personal information. Only enter such information using a secure website. Check that the URL starts with 'https://', rather than just 'http://'. Look for the lock symbol on the lower right-hand corner of the web browser and double-click it to check the validity of the digital certificate. Or, alternatively, use the telephone to conduct your banking.
3. Report anything suspicious to your bank immediately.
4. Don't use links in an email message to load a web page. Instead, type the URL into your web browser.

5. Check if your anti-virus program blocks phishing sites, or consider installing a web browser tool bar that alerts you to known phishing attacks.
6. Check your bank accounts regularly (including debit and credit cards, bank statements, etc.), to make sure that listed transactions are legitimate.
7. Make sure that you use the latest version of your web browser and that any security patches have been applied.

4. How to protect from Spam?

1. Maintain at least two email addresses. Use your private address only for personal correspondence, and another address for registering on public forums, in chat rooms, to subscribe to mailing lists etc.
2. Your private address should be difficult to guess. Spammers use combinations of obvious names, words and numbers to build lists of possible addresses. Your private address should not simply be your first and last name. Be creative and personalize your email address.
3. Treat your public address as a temporary one. The chances are high that spammers will get hold of your public address fairly quickly if it is frequently being used on the internet. Don't be afraid to change it often.
4. Never respond to spam. Most spammers verify receipt and log responses. The more you respond, the more spam you will receive.
5. Do not click on 'unsubscribe' links in emails from questionable sources. Spammers send fake unsubscribe letters in an attempt to collect active email addresses. If you click 'unsubscribe' in one of these letters, it will simply increase the amount of spam you receive.
6. Never publish your private address on publicly accessible resources.
7. If you must publish your private address electronically, mask it to avoid having it picked up by spammers. ‘hemanta.baral@yahoo.com’ is easy to find, as is ‘H.Baral@yahoo.com.’ Try writing ‘hemanta-dot-baral-at-yahoo.com’ instead. If you need to publish your private address on a website, do this as a graphics file rather than as a link.
8. Consider using a number of public addresses in order to trace which services are selling your address to spammers.
9. Make sure that you use the latest version of your web browser and that any security patches have been applied.
10. Use an anti-spam solution and only open email accounts with providers who provide spam filtering.
11. If your private address is discovered by spammers - change it. This can be inconvenient, but changing your email address does help you avoid spam - at least for a while!

5. How to protect from Identity Theft?

Choosing a good password is vital to being secure online. Just follow a few rules, which a surprising amount of people ignore. Three of the most common internet passwords are 'password', 'monkey' and '123456'.

Why are passwords important?

We now use the Internet for a wide range of activities, including online banking, online shopping and online research. Increasingly, we're also using the Internet to socialise. In the last few years there's been a massive growth in the number of social networking sites such as Hi5, Facebook, MySpace, etc. We share all kinds of personal details as well as music, pictures, and videos.

Unfortunately, the more personal details we make available, the more exposed we are to online identify theft. Identity theft is when a criminal steals confidential personal data that lets them fraudulently obtain goods and services in your name. A cybercriminal could, for example, open a bank account, obtain a credit card or apply for a driving licence or passport. Or they could simply steal money directly from your bank account.

Given that passwords protect such valuable data, they're clearly very important. You should protect all your online accounts with passwords - but you must be careful when choosing them.

Passwords help safeguard you against identity theft. They make it harder for cybercriminals to profile you, access your bank account (or other online accounts) and steal your money.

Choosing a good password is an important part of lowering the risk of becoming a victim of cybercrime. The following guidelines should help you when choosing passwords for your online accounts.

When choosing passwords:

1. Make them memorable;
2. Keep them secret;
3. Don't be fooled into disclosing them to seemingly legitimate organisations;
4. Mix uppercase and lowercase letters, numbers and non-alphanumeric characters;
5. Don't use the same password for multiple accounts;
6. Don't recycle passwords ('password1', 'password2', etc.).

6. To protect against malicious code attacks:

1. Install Internet security software.
2. Install security patches.
3. Be wary of unsolicited email or IM messages.
4. Be careful about logging in with Administrator rights.
5. Backup your data.

Antivirus Software

Install host antivirus software to protect against known viruses. Antivirus software can detect most viruses and many Trojan horse applications, and prevent them from spreading in the network.

Antivirus software does this in two ways:

- It scans files, comparing their contents to known viruses in a virus dictionary. Matches are flagged in a manner defined by the end user.
- It monitors suspicious processes running on a host that might indicate infection. This monitoring may include data captures, port monitoring, and other methods.

Most commercial antivirus software uses both of these approaches.

Securing wireless network

If your wireless network is not secure, a hacker can easily intercept the data you send and receive, or access files saved on your computer – all from the comfort of their own sofa.

These days, most computers are wireless-enabled: they let you connect to the Internet without a physical network cable. The major benefit, of course, is that you can use your computer anywhere in the house or office (as long as it's within range of your wireless router). However, there are potential risks involved in wireless networking - unless you make your network secure:

- A hacker could intercept any data you send and receive;
- A hacker could get access to your wireless network;
- Another person could hijack your Internet access.

Therefore, if your wireless network is not protected, a hacker could intercept any data you send; access your network, and therefore your shared files; use your connection to connect to the Internet - especially significant if you have a download limit on your internet package and your bandwidth is being swallowed up by a hijacker.

How do I secure my wireless network?

There are some simple steps you can take to secure your wireless network and router in order to minimise the risks:

1. Change the administrator password for your wireless router. It's easy for a hacker to find out the manufacturer's default password and use this to access your wireless network. And avoid using a password that can be guessed easily.
2. Switch off SSID (Service Set Identifier) broadcasting, to prevent your wireless device announcing its presence to the world.
3. Enable encryption in your connection settings: WPA encryption is best, if your device supports it (if not, use WEP encryption).
4. Change the default SSID name of your device. Again, it's easy for a hacker to find out the manufacturer's default name and then use this to locate your wireless network. Avoid using a name that can be guessed easily

4. AWARENESS

How to choose secure passwords?

1. Make your passwords memorable, so that you don’t have to write them down or store them in a file on your computer (remember, this file could be stolen by cybercriminals).
2. Don’t use real words that a hacker or cybercriminal can find in a dictionary.
3. Use a mixture of uppercase and lowercase letters, numbers and non-alphanumeric characters such as punctuation marks (although the latter are not always allowed).
4. Don’t recycle passwords, e.g. don’t use 'password1', 'password2', 'password3', etc. for different accounts.
5. If possible, use a passphrase, rather than a single word.
6. Don’t use the same password for multiple accounts. If a cybercriminal finds the password to one account, they can use to access other accounts.

How to keep your passwords safe?

1. Don’t use obvious passwords that can be easily guessed, such as your spouse’s name, your child’s name, pet's name, car registration, postcode etc.
2. Don’t tell anyone your password. If an organisation contacts you and asks for your password, even by phone, don't give them any of your personal details. Remember, you don’t know who’s at the other end of the telephone line.
3. If an online store, or any web site, sends you an email confirmation that contains a new password, login again and change your password immediately.
4. Check that your Internet security software blocks attempts by cybercriminals to intercept or steal passwords.

Top Security vulnerabilities

1. Security threats and risks are not analyzed prior to selection of security technology and design
2. Corporates fail to deal with the awareness and operational aspects of security
3. Lack of robust security policy definition or non-adherence to security policies
4. Absence of non-periodic security audits of IT infrastructure and operations
5. Lackadaisical implementation of physical security - Easy physical access to Data centers & critical IT assets

6. Misconfiguration of servers - Default options in installation procedures of operating systems and applications, which can be hacked easily
7. Password User accounts with No Passwords or Weak Passwords - Leads to password cracks with easy guesses
8. Failure to block unauthorized access to application ports - Unwanted TCP ports are open in Application Servers
9. Lack of availability of data foot prints due to non-existent or incomplete logging and backup of data
10. Improper Virus prevention procedures - Lack of timely update of periodic virus signatures

Common security lapses

Mistakes made by Users

- Opening unsolicited e-mail attachments without verifying their source and checking their content first
- Failing to install security patches—especially for Microsoft Office, Microsoft Internet Explorer, and Netscape
- Installing screen savers or games from unknown sources
- Not making and especially, not testing backups
- Using a modem while connected through a local area network

Mistakes made by Senior Executives

- Assigning untrained people to maintain security and providing neither the training nor the time to make it possible to learn and do the job
- Failing to understand the relationship of information security to the business problem
- Failing to deal with the operational aspects of security: making a few fixes and then not performing the necessary action to ensure the problems stay fixed
- Depending primarily on a firewall alone
- Failing to realize how much money their information and organizational reputation are worth
- Authorizing reactive, short-term fixes leading to problems re-emerging
- Mistakes made by IS Department
- Connecting systems to the Internet before hardening them
- Connecting test systems to the Internet with default accounts/passwords
- Failing to update systems when security holes are found

- Using telnet and other unencrypted protocols for managing systems, routers, firewalls, and PKI
- Giving users passwords over the phone or providing configuration information without authenticating the requester
- Failing to maintain and test backups
- Running unnecessary services, especially ftp, telnet, finger
- Implementing firewalls with rules that don't stop malicious or dangerous traffic-incoming or outgoing
- Failing to implement or update virus detection software
- Failing to educate users on what to look for and what to do when they see a potential security problem
- Providing users with too many usernames & passwords and making things difficult for the user to manage the same

Network Administration Tips

To keep the words in black and white is now old dated. Today's offices are equip with latest computers or laptops that have not only made the work easy but also reduced the bulk of files one has to carry from office to home and vice versa. In offices all computers are usually inter-linked and common share keeps the record of files being exchanged among the officials. Any problem in the network of these computers can not only block the sharing of significant confidential files but also their uploading or/and downloading. It is a time when no one can bear the loss of time so it is suggested that all companies must manage to keep themselves and their equipments up to date to avoid any un-wanted situation.

1. Many people do not bother about using illegal or pirated software. Being cheap and easily available, these software no doubt facilitate the users but their efficiency is obviously not lasting. After some times, the computer starts tomes up things and asking users to change or upgrade the program. It seldom affects the data within the computers. So always make original CDs your first priority in installing the operating system because they will keep the system working for a longer time and thus keeps your client satisfied. Do not forget to install some latest anti virus program because it saves the system from the attacks of intruders. You can select any antivirus program like Norton Antivirus, McAfee, Kaspersky etc…
2. You must have strong grip on sub-netting, bit-masks and gateways. Train yourself to think in terms of binary. You must also be aware of how address, for example network portion, the host portion, etc, are constructed.

3. You must also go through the implementation of hosts on network stack. You must be also well aware of the responsibilities of significant components like device drivers, firmware, the OS, the NIC, etc.). If you just learn all this once by heart than troubleshooting will be no more an issue.

4. You must also know the difference between broadcast and collision domain, and read VLANs. You should also be acquainted with the functions of Spanning Tree Protocol and must understand what is bridging.

5. Knowing about the routing protocol can also be very helpful. There is no need to be an expert of routing but you at least have a general idea. You can start from RIP.

6. You must also have knowledge about the DHCP and DNS and WINS and their substitutes for example static addressing, lmhost and host.

7. There is no need to install unnecessary applications or software. Just keep the applications on your network to the point. A variety of viruses and malicious codes can attack your computer in case you have used some uncertified software or a web based application.

8. After installing the operating system never forget to properly check the speed, security and performance of your system to resolve nay existing problem on the spot.

9. It is advised that you must keep the design of network as simple as possible because keeping it simple avoids many complexities. Moreover, do not forget to manage your network in segments to limit the affects of any out of order section from affecting adjacent systems. A network in segments easily cuts off from the troubling part and can go on as usually.

10. Keeping up a system or network updates is as important as installing it because delayed up-gradation can affect the performance of the system. Keep in mind that you must up date latest anti virus definitions and other measures along with software patches.

11. Do not forget to purchase a well planned hardware and to keep the documented record of hardware and software inventory, basic network configuration, computers and log on script in your network.

12. Keep complete back up of data of your serve. Try to manage the network resources in a manner which the performance of the server does not get affected by the approach of multi-systems to the server simultaneously.

13. Do remember to place resources close to the system user, and to classify IP address, create user material and enclosed user accounts.

14. Many times a sound network gets corrupted by the negligence of some user. It is very crucial that you must describe some basic features to the users so they can sort minor problem on the spot by self help. User awareness will also

relieve you. Warn the IT staff and the network users to refrain from doing any unauthorized activity on the system.

15. It will be also very helpful if your keep monitoring the access to internet. You should also block all unwanted applications based on web and ports. Moreover, you must also maintain strict control over the use of uncertified use of the internet.

16. Must remember that gateways are directly disclosed to the internet and extremely vulnerable to the attacks. Keep your proxy server or your computer gateway as secure as possible

17. Do not forget to mirror your hard disk.

18. Being a good network administrator you must make the structure of your network.

19. Do not limit yourself with the existing knowledge of computers and networks as there is improvement by each day. Keep yourself updated about all new and upcoming trends. Try to use these new trends and technologies on your network from time to time.

20. Keep the basic tips of troubleshooting on your fingertips to save time.

21. If you have to set up a network for an organization do not forget to make a well researched plan before installing the network.

22. Being a responsible administrator it is your duty to keep back up utility, recovery software, up to date program of anti virus, cable connectors, cable cutters, cable testers and other troubleshooting and network security apparatus in your resource kit.

23. You must be aware of latest networking certificates and networking knowledge, for example CCNP, CCNA, MCSE, Server+ and Network+. Sharing your knowledge with other network administrators will help you in improving your ideas and strengthening your knowledge. You can also correct yourself by giving answers to online questions about networking problems.

24. You should also set as complex the password of your network as possible. Try to keep and train an assistant network administrator. Network security tool must be kept up to dated so any external or internal attack on the security of your network can be tackled in the mean time.

25. Server room must be a restricted area where only certified staff can enter. Do not forget to take back your critical data on other hard disks and regularly backing up your data on CDs. Always keep some attendant in the server room to keep an eye on the entering officers.

Things to know about network administration

1. **The OSI model:** Memorize it. It's almost a formula, but understanding it is critical.
2. **TCP/IP concepts:** Learn to think in binary and get a firm grasp on bitmasks, subnetting, gateways (like the "default gateway") and how addresses are constructed (the network portion, the host portion, etc).
3. **Stacks:** Read about how the network stack is implemented on hosts. Get a good feel for what each component (the NIC, firmware, device drivers, the OS, etc) is responsible for. Once you understand this, troubleshooting is easy.
4. **Layer 2:** Learn how switches operate and how they're different from hubs and routers. Understand bridging, and get a general idea of what Spanning Tree Protocol does. Learn the difference between a collision domain and a broadcast domain, and then study VLANs.
5. **Routing:** Learn a routing protocol. Start with RIP, because it's easy. You don't need to be a guru, just get a general idea about how routers can exchange information about the network.
6. **Services:** Understand the role of DNS and DHCP and WINS and know their alternatives, like the host and lmhost files and static addressing.
7. Find yourself some good networking **reference material**. Whatis.com is a great for deciphering arcane acronyms.
8. **Security:** Read a little about how firewalls operate and other security technologies like VPNs. Understand the difference between authentication, authorization and accounting.
9. **Output:** Learn how to get status and information out of your networking devices. A good place to start is with the "show" commands (which will be featured in next week's tip).

FINDINGS AND CONCLUSION

With the increased use of Information Systems in society, security is becoming more and more important for strategic and operational concerns. Particularly network security is of more immediate consideration for protecting the system externally and internally.

This dissertation discusses the network security assessment methodology and its supportive tools applications.

At a core of discussion the proposed protocol AASA (Analysis, Assess, Security and Awareness) is briefed to achieve the security objectives in a network system.

AASA is a proposed protocol for network security assessment methodology that analyzes, assess, securitize and spread awareness for network security issues.

The selective methodology for the dissertation is more on the track of **positivism**.

The theoretical development is **deductive** whereby the AASA framework is tested in terms of hypothesis for a selected network (Stratford College London).

The selection of the organization as a base case links the dissertation with **empiricism**.

"The term 'empiricism' is used in a number of ways, but two stand out. First, it is used to denote a general approach to the study of reality that suggests that only knowledge gained through experience and the sense is acceptable. In other words, this position means that ideas must be subjected to the rigours of testing before they can be considered knowledge." **(Alan Bryman, 2003)**

AASA is useful methodology for incorporating network security. For the testing of the AASA framework; penetration testing was used to analyze the network security vulnerabilities and the following freely available tools were used to test the hypothesis: PING, IPCONFIG, TRACEROUTE, NSLOOKUP, NETSTAT, NMAP.

- Penetration Testing helps:
    - To identify assets and security perimeters
    - To identify threats (risks) and creating a list.
    - Identifying network security vulnerabilities and;
    - Prioritizing assets and vulnerabilities

- The PING command checks the connectivity between the user's computer and a particular domain. It also helps to determine whether TCP/IP is functioning or not.

- IPCONFIG provides the information about IP address, subnet mask, default gateway, hostname and information about local area connection.

- The application of the tool TRACEROUTE in the research shows the complete path or route of the information transmission. It provides the detailed routes including disturbance on the way until the information reaches its destination point.

- NSLOOKUP command gives the information about the domain names and IP addresses.

- NETSTAT is used to check the functionality of a network. It provides the details about all the connected computers and networks.

- The use of NMAP in the dissertation helps to detect the network vulnerabilities and the open ports. It identifies the active hosts and TCP, UDP (transport layer) ports; also it contains fingerprinting capabilities for service identification, operation system including remote operating system.

As a part of AASA protocol, some of the network security techniques are discussed which include:

- Securing computer networks
- Protection from crimeware, hackers, phishing attack, spam, identity theft and malicious code attacks
- Wireless network

Finally, awareness required for the network security professionals and precautions to be taken during the process are discussed in the research. It covers:

- How to choose secure password?
- Common security lapses
- Network Administrator duties
- System Administration Tips

On an aggregate level the application of various tools concludes that AASA framework is an approach for analyzing the network, assessing the vulnerabilities and securitizing the possible threats and creating the awareness.

RECOMMENDATION

This dissertation is in partial fulfilment of the requirements for the degree of MSc whereby a protocol for network security assessment methodology called **AASA (Analysis, Assess, Security and Awareness)** is developed and tested using certain freely available supporting tools to conclude the authenticity and reliability of this protocol.

Due to the limitation of finances, time and inclusion of other universities, the AASA model is not applied on the longer extents. There also exist certain other credible tools and options to further validate this protocol. These tools include:

- Nessus
- Metasploit Framework
- L0phtcrack 6 Administrator
- Snort
- Netstat
- Wireshark
- Netcat
- Cain and Abel etc…

Some of the above mentioned tools are free and some are commercial such as Nessus-$1200 (ProfessionalFeed for 1 year), L0phtcrack 6 Administrator - $595.00 etc.. as per the price of 10 May 2010.

The University Alliance Community (UAC) provides connection between university leaders, students, partners and internal experts. This platform is working on SAP.

(http://www.sdn.sap.com/irj/uac 19 May 2010 17:00PM)

It is recommended at initial level of development to further test to validate AASA at a longer industrial level.

The focus of this AASA protocol is an analytical side to uncover the potential threats for a network. The initial identification further leads to the detail assessment and mitigation process.

Strength of this model: Analytical side

Weaknesses: It can be further extended on more technical and probabilistic approach for artificial neural networks.

REFERENCES / BIBLIOGRAPHY

1. Campbell, Paul, Calvert, Ben, Boswell Steven, 2003. *Security + Guide to NETWORK SECURITY Fundamentals*. Cisco Learning Institute: THOMSON
2. Shinder, Debra Littlejohn, 2001. *Computer Networking Essentials*. Cisco Press
3. Bhaiji, Fahim Hussain Yusuf, 2008. *Network security technologies and solutions*. Cisco; London: Pearson Education (distributor)
4. Wang, Jie, 2009. *Computer Network Security: Theory and Practice*. Jointly published with Higher Education Press
5. Panko, Raymond R, 2004. *Corporate Computer and Network Security*. International Edition. Pearson Education Inc.
6. Cretaro, Paul, 2003. *Lab manual for Security + Guide to Network Security Fundamentals*. Thomson Learning Inc.
7. Panko, Raymond J, 2010. *Corporate Computer and Network Security*. Second Edition. Pearson Education Inc.
8. McNab, Chris, 2008. *Network Security Assessment*. Second Edition. O'Reilly Media Inc.
9. Poole, Owen, 2003. *Network Security: A practical guide*. Butterworth-Heinemann
10. Meyers, Michael, 2002. *Network + Certification All in one Exam Guide*, Second Edition. Osborne/McGraw-Hill
11. Onwubiko, C, Lenaghan, A.P., 2005. *Vulnerability Assessment: Towards an Integrated Security Infrastructure,* International Conference on Computer Science & Information Systems, ATINER, Athens, Greece, PP. 157-172
12. Braunton, Gregory, 2004. *A Security Assessment Methodology*. SANS Institute InfoSec Reading Room. Available at: www.sans.org/reading_room/whitepapers/auditing/b_a_s_e_–_a_security_assessment_methodology_1587 [Accessed 25 January 2010]
13. *Network Security Wheel* Available at: http://netlab.anglia.ac.uk/uc/en_EWAN_v40_Linux/theme/cheetah.html?cid=140000000&l1=en&l12=none&chapter=1 [Assessed 05 January 2010]
14. Baral, Hemanta, 2000. *Advanced Diploma in Hardware and Networking*. 4th Edition. Kathmandu, NEPAL: Vidyarthi Prakashan
15. Wisker, Gina 2008. *The postgraduate Research Handbook*. Second Edition. Palgrave Macmillan.

16. Fisher, Colin, 2007. *Researching and writing a Dissertation*. Second Edition. Prentice Hall

17. Bryman, Alan, Bell, Ema, 2003. *business research methods*. Second Edition. Oxford University Press

18. *Top 100 Network Security Tools*. Available at: http://sectools.org/ [Accessed 02 February 2010]

19. *Use of PING*. Available at: http://www.livinginternet.com/i/ia_tools_ping.htm#use [Accessed 05 February 2010]

20. www.Kaspersky.co.uk [Accessed 13 February 2010]

21. *WLAN*. Available at: http://compnetworking.about.com/cs/wirelessproducts/g/bldef_wlan.htm [Accessed 27 February 2010]

22. *Introduction to Intranet*. Available at: http://www.cs.nott.ac.uk/~tar/DBC/dbc-lecture8.pdf [Accessed 28 February 2010]

23. *Benefits of intranets and extranets*. Available at: http://businesslink.gov.uk/bdotg/action/detail?type=RESOURCES&itemId=1075386483 [Accessed 01 March 2010]

24. *What is VPN*. Available at: http://searchenterprisewan.techtarget.com/sDefinition/0,,sid200_gci213324,00.html [Accessed 02 March 2010]

25. http://www.teach-ict.com/as_a2/topics/networks/network%20components/network_components/cables.htm [Accessed 28 February 2010]

26. http://www.conec.com/section23/fiber.optic.connector.html [Accessed 6 March 2010]

27. *The 7 Layers of the OSI Model*. Last updated: March 03, 2008 http://www.webopedia.com/quick_ref/OSI_Layers.asp [Accessed 10 March 2010]

28. *The OSI (Open System Interconnection) Model*. http://www.infocellar.com/networks/osi-model.htm [Accessed 16 March 2010]

29. http://etutorials.org/Networking/Router+firewall+security/Part+I+Security+Overview+and+Firewalls/Chapter+1.+Security+Threats/Types+of+Security+Threats/[Accessed 26 March 2010]

30. *Network reconnaissance* http://en.citizendium.org/wiki/Network_reconnaissance. [Accessed March 28 2010]

31. *What is a Packet Sniffer?* http://www.wisegeek.com/what-is-a-packet-sniffer.htm [Accessed March 28, 2010]

32. *http://www.cisco.com/web/learning/netacad/index.html*
33. *TCP/IP Suite Weaknesses* http://mudji.net/press/?p=152 [Accessed April 5, 2010]
34. *NSLOOKUP Coomand* http://www.livinginternet.com [Accessed 22 April 2010]
35. *Ping command* http://www.livinginternet.com/i/ia_tools_ping.htm#use [Accessed 23 April 2010]
36. *Network Administrator duties* http://www.wifinotes.com/computer-networks/system-network-administration-guidelines.html [Accessed 23 April 2010]
37. *Network Security:Security and ThreatsSecurity Threats* http://research.microsoft.com/en-us/um/people/tuomaura/teaching/network-security-threats.pdf [Assessed 26 April 2010]
38. *Deductive Vs Inductive* http://www.greenspun.com/bboard/q-and-a-fetch-msg.tcl?msg_id=002ZrE [Assessed 18 May 2010]