Introduction to Network Security

Overview

- Almost every other day there is a story about a computer network being compromised by hackers.
- It is in record that the Department of Defense (DOD) was a victim of a successful hacker raid;
  - hackers were able to penetrate DOD computers during a two-week period before they were detected.
  - Fortunately, the computers contained only non-classified personnel and payroll information, so national security was not threatened.
- More recently, Yahoo, Amazon.com, eBay, and some other popular World Wide Web (WWW) sites were targets of what appears to have been a coordinated "denial-of-service" attack.
  - During a three- or four-day period, the sites were overwhelmed with massive bombardments of false traffic from multiple sites.
  - As a result, the sites were shut down for hours at a time.
- In 1999, a survey conducted jointly by the American Society for Industrial Security and Pricewaterhouse-Coopers (ASIS/PWC) reported that Fortune 1000 companies lost more than $45 billion from theft of "proprietary information."
- The ASIS/PWC survey of Fortune 1000 companies received 97 responses. Also of interest, the survey reported the following: •
  - Forty-five percent of the respondents said that they had suffered a financial loss as a result of information loss, theft, or misappropriation.
  - On average, the responding companies reported 2.45 incidents with an estimated cost of $500,000 per incident.
  - The number of reported incidents per month had increased over the last 17 months.
- Another survey conducted jointly by the FBI and the Computer Security Institute (CSI) also yielded some interesting numbers. The FBI/CSI survey received 521 responses from individuals in the computer security field. The findings were as follows.
  - Thirty percent of the respondents reported an intrusion from an outside source.
  - Fifty-five percent of the respondents reported an unauthorized intrusion by a source inside the organization.
  - The average loss from the theft of proprietary information increased from $1,677,000 in 1998 to $1,847,652 in 1999.
  - The average loss from financial fraud rose from $388,000 in 1998 to over $1,400,000 in 1999.

- The total financial losses due to computer-related crime for the 521 respondents amounted to more than $120 million.

These attacks and survey results illustrate how pervasive the threats to information systems has become.

Objectively , every organization that uses computers faces the threat of hacking from :

- Individuals within the organization. Employees or former employees with malicious intent or who want to obtain information such as employee salaries or view other employee's files are also a threat to an organization's computers and networks

Computerworld (US Magazine) ran a story about a programmer employee of a company who allegedly launched a denial-of-service attack against his own company, a provider of on-line stock trading services.

This programmer wanted more compensation. He became frustrated with the progress of the negotiations and decided to demonstrate to the company its vulnerability by launching an attack on its systems from the Internet.

He was familiar with the company's systems and software, and his inside knowledge enabled him to hit the firm in a manner that shut it down.

In fact, the attack disrupted stock trading services at the company for three days. The U.S. Secret Service was eventually employed, and the attack was traced to the employee, who was subsequently arrested.

- Every organization should monitor its systems for possible unauthorized intrusion and other attacks.
- This should be part of the daily routine of every organization's IT unit, as it is essential to safeguarding a company's information assets.

Importance of Computer and Network Security

Computer and network security is important for the following reasons.

1. **To protect company assets:**
    - One of the primary goals of computer and network security is the protection of company assets.
    - By "assets," I do not mean the hardware and software that constitute the company's computers and networks.
    - The assets are comprised of the "information" that is housed on a company's computers and networks. Information is a vital organizational asset.
    - Network and computer security is concerned, above all else, with the protection, integrity, and availability of information.

2. **To gain & maintain a competitive advantage:**
    - Developing and maintaining effective security measures can provide an organization with a competitive advantage over its competition.
    - Network security is particularly important in the arena of Internet financial services and e-commerce.
    - It can mean the difference between wide acceptance of a service and a mediocre customer response. For example, how many people do you know who would use a bank's Internet banking system if they knew that the system had been successfully hacked in the past? Not many. They would go to the competition for their Internet banking services.

3. To comply with regulatory requirements and fiduciary responsibilities:
    - Corporate officers of every company have a responsibility to ensure the safety and soundness of the organization.
    - Part of that responsibility includes:
        - Ensuring the continuing operation of the organization.
        - Accordingly, organizations that rely on computers for their continuing operation must develop policies and procedures that address organizational security requirements. Such policies and procedures are necessary not only to protect company assets but also to protect the organization from liability.
        - Profit based organizations must also protect shareholders' investments and maximize return.
        - Also organizations are subject to governmental regulation, which often stipulates requirements for the safety and security of an organization.
        - For example, most financial institutions are subject to federal/county regulation.

-

1. To keep your job:
    1. Finally, to secure one's position within an organization and to ensure future career prospects,

Historical and Technological Factors fueling insecurity

- Prior to the 1980s most computers were not networked due to lack of enabling technology.
  - Most systems were mainframes or midrange systems that were centrally controlled and administered.
  - Users interfaced with the mainframe through "dumb" terminals.
  - The terminals had limited capabilities.
  - Terminals actually required a physical connection on a dedicated port.
  - The ports were often serial connections that utilized the RS-232 protocol.
  - It usually required one port for one terminal.
- In the 1980s, the combination of the development of the personal computer (PC),
  - the development of network protocol standards,
  - the decrease in the cost of hardware, and the
  - development of new applications made networking a much more accepted practice.
  - As a result, LANs, WANs, and distributed computing experienced tremendous growth during
- Interconnected WANs and LANs
  - Intially LANs were relatively secure-mainly because they were physically isolated.
  - They were not usually connected to WANs, so their standalone nature protected the network resources.
  - WANs preceded LANs and had been around for some time, but they were usually centrally controlled and accessible by only a few individuals in most organizations.
  - WANs utilizing direct or dedicated privately owned or leased circuits were relatively secure because access to circuits was limited. To connect two locations (points A and B) usually required a point-to-point (A-B) circuit.
- Development of packet-switched protocols
  - Protocols such as X.25 and Transmission Control Protocol/Internet Protocol (TCP/IP) reduced the cost to deploy WANs, thus making them more attractive to implement.
  - These protocols allowed many systems to share circuits. Many people or organizations could be interconnected over the shared network. It was no longer necessary to connect systems in a point-to-point configuration.
  - Vulnerabilities were introduced with the deployment of this distributed environment utilizing shared, packet- switched networks employing protocols such as TCP/IP and the concept of trusted systems.

- Systems on the network "trusted" each other. This situation was frequently made worse by connecting relatively secure LANs to an unsecured WAN. Figure 1.2 illustrates the concept behind the packet-switched network.
- Technically an organization's network connections would enter into the cloud of the packet-switched network.
- In this distributed environment the emphasis was on providing ease of access and connectivity.
- Security was an afterthought, if it was considered at all.
- As a result, many systems were wide open and vulnerable to threats that previously had not existed.
- The Internet is the largest and best known of this type of network.
- The Internet utilizes TCP/IP and was primarily designed to connect computers regardless of their operating systems in an easy and efficient manner.
- Security was not part of the early design of TCP/IP, and there have been a number of widely publicized attacks that have exploited inherent weaknesses in its design.
- One well-known event was the Internet Worm that brought the Internet to its knees back in 1986.
- Today, security has to be more important than ease of access.

Towards a more secure Network

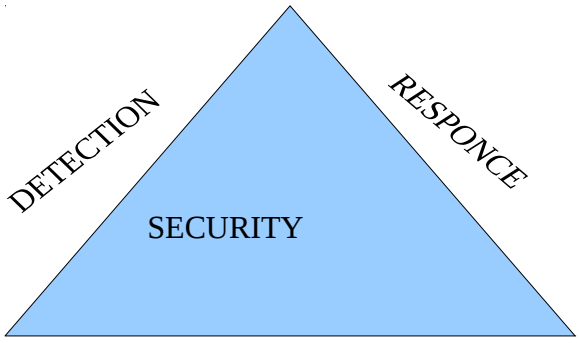
One of the most important steps in any task is to identify why you are doing it. Rather than just saying we need to make a system secure you need to:

1. Consider what is meant by secure,
2. Identify what risks are associated with any data that's available,
3. Evaluate what impact your security measures will have on your users.

These preliminary steps will help you know if you've met your goal of making a system secure.

The Security Trinity

- The basis of for network security. comprise of the three legs of the "security trinity," prevention, detection, and response.
- The security trinity should be the foundation for all security policies and measures that an organization develops and deploys.



PREVENTION

Prevention

- The foundation of the security trinity is prevention. To provide some level of security, it is necessary to implement measures to prevent the exploitation of vulnerabilities.
- In developing network security schemes, organizations should emphasize preventative measures over detection and response:
- It is easier, more efficient, and much more cost-effective to prevent a security breach than to detect or respond to one.
- Companies should ensure that their preventative measures are strong enough to discourage potential criminals-so they go to an easier target.

Detection

- Once preventative measures are implemented, procedures need to be put in place to detect potential problems or security breaches, in the event preventative measures fail.
- It is very important that problems be detected immediately. The sooner a problem is detected the easier it is to correct and cleanup.

Response

- Organizations need to develop a plan that identifies the appropriate response to a security breach.
- The plan should be in writing and should identify who is responsible for what actions and the varying responses and levels of escalation.

NOTE

1. Network security is not a technical problem; it is a business and people problem. The technology is the easy part. The difficult part is developing a security plan that fits the organization's business operation and getting people to comply with the plan.
2. Network security is not absolute. All security is relative.
    - Network security should be thought of as a spectrum that runs from very unsecure to very secure.
    - The level of security for a system or network is dependent on where it lands along that spectrum relative to other systems. It is either more secure or less secure than other systems relative to that point.
    - There is no such thing as an absolutely secure network or system.
3. Network security is a balancing act that requires the deployment of "proportionate defenses."
    - The defenses that are deployed or implemented should be proportionate to the threat.
    - Organizations determine what is appropriate in several ways, described as follows.
        - Balancing the cost of security against the value of the assets they are protecting;
        - Balancing business needs against security needs.
        - Balance possible threats against probable threats .
4. Organizations also need to balance the cost of security against the cost of a security breech.
    - Generally, as the investment in security increases, the expected losses should decrease.
    - Companies should invest no more in security than the value of the assets they are protecting.
    - This is where cost benefit analysis comes into play.
5. Balancing possible threats against probable threats is important:
    - As it is impossible to defend against every possible type of attack, it is necessary to

determine what types of threats or attacks have the greatest probability of occurring and then protect against them.

6. It is also important to balance business needs with the need for security and assessing the operational impact of implementing security measures.
    - Security measures and procedures that interfere with the operation of an organization are of little value.
    - Those types of measures are usually ignored or circumvented by company personnel, so they tend to create, rather than plug, security holes.
    - Whenever possible, security measures should complement the operational and business needs of an organization.

Security requirements

After establishing why security is to be implemented you should consider the aspects of security that are required. The main security requirements are:

1. **Authorisation** - Only allow those that need access to the data
2. **Authenticity** - Verifying they are who they say they are.
3. **Privacy / Confidentiality** - Ensure personal information is not being compromised
4. **Integrity** - Ensuring that the data has not been tampered with
5. **Non-repudiation** - Confirmation that data is received. The ability to prove it in court
6. **Availability** - Ensure that the system can perform it's required function

Requirements	Brief Explanation
1. **Privacy or confidentiality**	1. Keeping information secret from all but those who are authorized to see it.
2. **Data integrity**	2. Ensuring information has not been altered by unauthorized or unknown means.
3. **Entity authentication or identification**	3. Corroboration of the identity of an entity (e.g. A person, a computer terminal, a credit card, etc.).
4. **Message authentication**	4. Corroborating the source of information; also known as data origin authentication.
5. **Signature**	5. A means to bind information to an entity.
6. **Authorization**	6. Conveyance/Permission, to another entity, of official sanction to do or be something.
7. **Validation**	7. A means to provide timeliness of authorization to use or ma manipulate information or resources.
8. **Access Control**	8. Restricting access to resources to privileged entities.
9. **Certification**	9. Endorsement of information by a trusted entity.
10. **Time Stamping**	

11. witnessing **12. Receipt** **13. Confirmation** **14. Ownership** **15. Anonymity** **16. Non-repudiation** **17. Revocation**	10. recording the time of creation or existence of information. 11. verifying the creation or existence of information by an entity other than the creator. 12. acknowledgment that information has been received. 13. acknowledgment that services have been provided. 14. a means to provide an entity with the legal right to use or transfer a resource to others. 15. concealing the identity of an entity involved in some process. 16. preventing the denial of previous commitments or actions. 17. retraction of certification or authorization.

Imposed Requirements

Some security requirements are not ones that are directly under your control but are instead imposed upon you. These include:

- These may be legal requirements (e.g. Data Protection Act 1998),
- Compliance with standards (e.g. ISO 7984-2 International Standards Organisation Security Standard), or corporate policy. If you handle credit card transactions then you may be required to comply with minimum security standards as described by the Payment Card Industry (PCI).
- Some of these standards are very vague (e.g. the Data Protection Act just specifies that appropriate security should be in place) whereas some may be more specific (e.g. a corporate policy may insist on a minimum length of passwords etc.).

Knowing the enemy

Before being able to effectively protect a computer system you need to know who it is that is trying to attack your systems and what they are trying to do. Some questions may provide a guidelines.

1. Who want to attack?
2. What is the motivation?
3. How do they do it?
4. What do they use?
5. Where do they want to attack?

NOTE

- "Attackers look for the easiest means of compromise. That's why attacks are moving from more security-mature organizations down to less mature, typically smaller, partners.

- Attackers can exploit the trust relationships between companies to infiltrate well-protected targets through supply chain partners with less security experience.

- Advanced cyber attacks have been known to attack their primary targets by exploiting business partners with weaker defenses.

- Rather than combat the well-protected computer networks of a target company, cyber attackers try instead to infiltrate the organization through its connections to trusted partners with less-developed security practices.

- In recent incidents, cyber attackers have sought to cover their tracks by routing data stolen from a company through the computer networks of a business partner.

- Identifying appropriate levels of security can prove challenging, because it's an exercise based on risk and relativity.

Appropriate security for any organizations is determined by four factors:

1. The organization's risks and requirements, which change over time and are unique for each organization
2. The value of information assets being protected, with high-value assets monitored more closely and subject to more controls .
3. The security risks and threats the organization can reasonably expect to face, considering that attack techniques are constantly changing and rising in sophistication .
4. Prevailing security practices for the organization's peers, with the organization aiming to be at

or above the group “average” so as to not make itself an easy target

5. Another way organizations can diagnose security performance on a relative basis is through self-assessment tools. Many consulting firms and security service providers offer proprietary “security maturity” models. Each has merits and deficiencies, but they all aim to provide a progressive framework for measuring security performance.

Attributes and Goals for an Effective Security System

Highly secure

- Allow access to legitimate users only
- Minimize the opportunity of hacker access
- Minimize the possibility for damage in the event of hacker access.

Easy to use

- Security system is easy to use so that there is no motivation to circumvent it
- The interface is intuitive

Appropriate cost of ownership

- Consider the initial purchase cost and the price of upgrades and service
- Consider the cost of successful implementation and maintenance

Flexible and scalable

- The system allows your company to do business the way it wants to
- The system can grow as the company grows

Superior alarming and reporting

- In the event of a security breach, the system notifies the administrator quickly and in sufficient detail
- System notification (alerts by email, computer screens, and pagers) options are efficient

Risk Assessment

To determine exactly how much protection a resource requires, you must also decide how much risk it is exposed to. For example, an internal user workstation is at significantly less risk than a Web server because the latter is directly exposed to the Internet.

The concept of risk assessment is crucial to developing proportionate defenses. To perform a risk analysis, organizations need to understand possible threats and vulnerabilities. Risk is the probability that a vulnerability will be exploited.

To reduce risk, you should take the following steps:

1. Identifying and prioritizing assets;
2. Identifying vulnerabilities;
3. Assign risk factors
4. Identifying threats and their probabilities;
5. Determine security priorities for each system
6. Developing a cost benefit analysis;
7. Define acceptable and unacceptable activities
8. **Developing security policies and procedures.**
9. Determine who will administer your policy

To identify and prioritize information assets and to develop a cost benefit analysis, the following questions can act as a guidance.

- What do you want to safeguard?
- Why do you want to safeguard it?
- What is its value?
- What are the threats?
- What are the risks?
- What are the consequences of its loss?
- What are the various scenarios?
- What will the loss of the information or system cost?

SECURITY ATTACKS

There exist a wide range of security attacks some of which includes:

- **Phreakers** - Also known as Phone Phreakers, this term originates from what could be considered to be the earliest form of attacks against electronic systems. It's earliest for was to bypass the systems used in telephone systems allowing free or reduced price international phone calls. One of the earliest forms of this was when the American pay phone system used a certain frequency signal to indicate that a coin had been placed in the phone. It was discovered that the frequency of the signal was 2600 Hz, which was also the same frequency emitted from a toy whistle distributed with a popular make of cereals. By blowing the whistle into the phone when a request was made for payment the Phreaker could fool the operating into thinking that money had been deposited in the pay phone.
- **Crackers** - These are people that gain unauthorised access to a computer. When people refer to hackers breaking into a computer then they are really referring to crackers.
- **Hackers** - Using the traditional meaning of the word Hacker is not meant to imply any kind of illegal or immoral activities. The true meaning is of a computer enthusiast that understands the inner workings of a system and uses that knowledge to "**hack**" together programs etc. to perform a function.
- Due to incorrect use, including by the press, the word hacker has now come to take on two meanings. One is it’s original meaning and the other is that of anyone who tries to penetrate a computer (crackers) or those who cause intentional disruption or damage (none-physical) to computer systems.
- "Hacker - computer enthusiast, esp. one gaining unauthorised access to files"
  The Oxford Popular Dictionary, Parragon, 1995

Why be a hacker?

There are different reasons that someone would want to attack your system.

- **Just for fun** - Typically someone in further or higher education that uses the college or universities computer facilities to attack another computer over the Internet. Whilst there are indeed a number of attackers that match this description it is important to recognise that these are not the only type of hackers. This person will typically have limited resources and normally does it, just for fun; or to prove their intelligence etc. However they may be part of a larger group united using the Internet. Whilst many do not intend to commit malicious damage they may discredit your company name, they may cause accidental damage, and may open the door for others.
- **Commercial espionage / sabotage** -
  - There is potentially a risk from competitors wanting to gain a competitive edge.
  - For example if you are bidding for a contract and your competitor is able to find out details of your bid, they could easily undercut you and win the contract.
  - Alternatively by putting your web page out of action, customers could be encouraged to try

the competition.

  - This kind of attacker normally has a lot of resources, both financial and in man power, at it's disposal and has very specific targets.

- **Fighting a cause** – For groups that may wish to attack a company for a cause or defending a belief. Whilst there are a number of obvious extremist groups such as terrorists or the extremist animal rights groups this could equally apply to less controversial areas where someone has a different opinion.
- **Disgruntled employees** -
  - It is sometimes the case that the greater risk lies from employees within the organisation.
  - These could already have authorised access to a computer, and already be inside the firewall.
  - They could then use that access against the organisation and exploit other holes in the system.
  - Whilst these people can have different motives one of the most obvious is for someone that has been fired, disciplined or who is not satisfied with their current standing in the organisation.
  - Defending against the internal employee can be more challenging as methods need to be found to limit access without preventing others for performing their job.
  - To tighten up security to the point where employees cannot do their job properly is an indirect Denial of Service.
- **Unintentional user error** – It is possible that users could cause some accidental damage to data. By limiting a users access user errors can be contained to a reasonable extent. This could be in the form of a programming error as well as incorrectly typing instructions into a program.

Types of attacks against systems

There are a number of different types of attacks that take place. These may be different depending upon the services you offer or the type of attacker that is targeting you. These are areas that are looked at later to determine methods of protection. This list is not intended to be a complete list however it does give an idea of what areas to focus your attention on. New methods are still being developed and a security administrator has to ensure that they don't get left behind.

- **Reading data** (Unauthorised access)- Typically associated with espionage or theft, computer systems often contain information that needs to be kept confidential or secure. This could vary from emails discussing the price of a bid for a project to personal information or bank details. The disclosure of this information could severely damage the company or have legal implications. In the UK the storing of personal data is covered by the Data Protection Act (1988). The principle of the act states that personal data shall "Be surrounded by proper security." See http://www.dataprotection.gov.uk/ for more details.
- **Changing data(Data Inetgrity)** -
  - Potentially even more serious is that an attack could gain sufficient access to be able to update data.

- This could be for sabotage, as a means of discrediting the organisation or leaving a calling card.
- One of the biggest risks is that data could be modified and not noticed.
- The cases that tend to get a high profile in this area are:
  - where attackers replace web pages with their own modified versions.
  - Banking systems where avounts data may be modified
  - University student grading system

- **Denial of service** -
  - Denial of Service (DoS) attacks are where the attacker disables, or makes unusable the services provided by the system.
  - An Example DoS attack was the "Ping of Death".
    - By creating a ICMP echo command that was larger than the maximum allowable size a computer could be made to fail. In fact this vulnerability was found to exist on Windows Vista, ten years after the bug was originally fixed in the earlier versions of Windows (http://www.v3.co.uk/v3/news/2249151/ancient-flaw-hits-vista) .
  - Many of the DoS attacks in the past were addressed by fixing bugs there is a more problematic threat known as **Distributed Denial of Service**.
  - The first well known example was the attacks against Altavista and Yahoo in early 2000, but similar attacks have be launched against various sites including Twitter in 2009, and more recently against sites responsible for filtering Pirate Bay and other file sharing sites.
  - The distributed Denial of Service attack works by the attacker, or more likely attackers, planting trojan horses on lots of different machines. When these trojan horses are triggered simultaneously they mount an attack directly against a single system.
  - The combined effect of thousands of simultaneous attacks prevents the system from operating. T
  - his form of attack is getting more and more sophisticated and security administrators are devoting more resources to tackling this kind of problem.

- **Access to computer** -
  - One may allow other users onto your system.
  - Sometimes these user accounts could come under attack.
  - The computer may not contain any confidential material and the user may not be able to write to any data however they could still use your system to cause damage.
  - If someone manages to attack a computer that borders between a secure and insecure network then they could use your machine as a method of traversing between the two networks.
  - Another technique to use your computer to attack another is in the **distributed denial of service.**
  - The attacker could plant a Trojan horse on your computer so that when triggered it attacks

another computer.

- This could be potentially embarrassing if someone found that systems belonging to your organisation were used to commit one of these crimes.
- Indeed it could even look as though it was someone from inside your organisation that perpetrated the crime.

Methods of attacking (Gaining Access to) a system

- The first generation of hackers were typically intelligent people with a great deal of understanding of how computers work.
- They could identify bugs in systems and then use their knowledge of computers to exploit the bug.
- Whilst there are still a lot of hackers that can do this there is also another type of attacker that waits until someone else has found a way into a computer and then uses the same technique.
- They can just take programs and scripts written by hackers and run them against systems hoping to find a way in.
- I have not referred to them as hackers as they do not have the knowledge of computers to back up their curiosity, they are sometimes referred to as "Script Kiddies" (regardless of their actual age).
- Here is a list of some of the techniques used to gain access. This purely gives an idea of some of the methods used and does not list all the available methods.

1. **Password guessing**
    - - Some systems or services may have default passwords when they are installed.
    - Some attackers will just try some standard user names and passwords in the hope they will be lucky and find a easily guessed password.
    - Some people may set the password to be the same as the user name which is one of the standard things the person will try.
    - This method relies on users or administrators not using secure passwords.

3. **Social engineering** -
    - This technique works by working on the failings of people rather than the insecurity of computers.
    - One technique is to phone a help desk pretending to be an employee and trying to get them to give you the password over the phone.
    - It is also possible the other way around pretending to be a system administrator and asking the user for their user name and password.
    - Another technique, known as **shoulder surfing**, is where the attacker would stand behind someone whilst they typed their password into the keyboard, watching what keys are pressed.
    - These are techniques that depend upon the security training (or rather lack of it) that the

employees have.

3. **Trojan horses**
   - Trojan horses are programs planted in a computer which appear to be harmless.
   - These could be left by another user of the system or placed on a previously hacked site that is used to distribute software, they could also be sent as E-mail pretending to be a useful tool or fun game.
   - When a trigger is activated then the hacker can gain access to computer or get the program to run a certain command.
4. **Virus**
   - A virus is a programs designed to self replicate itself. These may have a malicious pay-load that is run to compromise the system in question.
5. **Software bugs**

- - If software has not been written correctly there are sometimes bugs that can lead to a security exposure.
- One example is that a program designed to handle a certain amount of data can be broken by bombarding it with too much data.
- This is sometimes done by overrunning the buffers with data causing data to be stored in memory not allocated for that purpose.
- This could result in the system crashing (e.g. the Ping of Death) or in a trusted program providing access to the system.

6. **Address spoofing** -

- In trusted environments it is sometimes configured that other computers known to be safe are allowed access to that computer without any further authentication.
- Whilst this makes administration easier it does have potential problems in that another computer could masquerade as one of these trusted computers.
- By configuring a computer with the same IP address as a trusted one, which is down or has been forced down, the attacker would have access to other systems the same as if they had been given official access on the trusted server. I
- n a lot of environments it is therefore considered to be bad practice to enable services that rely on these trusted computers.
- This is by no means a comprehensive list of methods however it does give an idea of areas that computers can be vulnerable.

7. Brute-force attacks

- In *brute-force attacks*, a hacker attempts to defeat authentication by obtaining a legitimate user's password.
- A brute-force attack may include a *dictionary file* , a *sniffer*, repeated logon attempts, or an attempt to break a code using combinations of computers and information.

1. ***Dictionary file****:* A file comprised of common passwords used by a hacker in an attempt to gain

entrance to a network.

2. ***Sniffer****:* A program used to intercept passwords.

8. Coding Problems

- Many times, an operating system or program running on the server contains coding problems or *bugs* that create an unintentional opening. Hackers often know about such problems and exploit them.
- Also, program designers sometimes intentionally place a *back door* in an operating system or program so they can support the product quickly.

9. Buffer overflow

- A popular bug-based attack is a *buffer overflow* that works by sending more data than the target system is intended to receive at one time.
- The extra data overflows the program's storage buffer in memory and then overwrites the actual program data, allowing modification of the target system's programs resulting in the creation of a *back door* into the system.

10. Trap Doors

- A trap door or back door is an undocumented way of gaining access to a system that is built into the system by its designer(s).
- It can also be a program that has been altered to allow someone to gain privileged access to a system or process.
- There have been numerous stories of vendors utilizing trap doors in disputes with customers.
- One example is the story of a consultant who was contracted to build a system for a company.
    - The consultant designed a trap door into the delivered system.
    - When the consultant and the company got into a dispute over payment, the consultant used the trap door to gain access to the system and disable the system.
    - The company was forced to pay the consultant to get its system turned back on again.

11. Logic Bombs

- A logic bomb is a program or subsection of a program designed with malevolent intent.
- It is referred to as a logic bomb, because the program is triggered when certain logical conditions are met.
- This type of attack is almost always perpetrated by an insider with privileged access to the network.
- The perpetrator could be a programmer or a vendor that supplies software.
- There is a story about a programmer at a large corporation who engineered this type of attack. Apparently, the programmer had been having some trouble at the company at which he worked and was on probation.
- Fearing that he might be fired and with vengeance in mind, he added a subroutine to another

program.

- The subroutine was added to a program that ran once a month and was designed to scan the company's human resources employee database to determine if a termination date had been loaded for his employee record.
- If the subroutine found that a termination date had been loaded, then it was designed to wipe out the entire system by deleting all files on the disk drives.
- The program ran every month and so long as his employee record did not have a termination date then nothing would happen.
- In other words, if he were not fired the program would do no damage.
- The employee was fired, and the next time the logic bomb that he created ran it found a termination date in his employee record and wiped out the system.
- This is an example of how simple it can be, for one with privileged access to a system, to set up this type of attack.

12. Man in the Middle Attack (MIM)

- In a MIM attack, a hacker inserts himself or herself between a client program and a server on a network.
- By doing so the hacker can intercept information entered by the client, such as credit card numbers, passwords, and account information.
- Under one execution of this scheme, a hacker would place himself or herself between a browser and a Web server.
- There are several ways a hacker can launch a MIM attack.
    - One way is to register a URL that is very similar to an existing URL.
    - When someone who wants to go to the URL web site and types in the URL they would be brought to a Web site set up by the hacker tha look like the the URL wibsite
- To Web surfers everything would look normal. They would interact with the counterfeit Web site just as they would with the real site.
- As the Web surfer enters in choices and information the hacker's Web site can even pass it onto the real site and pass back to the Web surfer the screens that the real site returns.

13. SPAM

- SPAM is unwanted e-mail. Usually it takes the form of a marketing solicitation from some company trying to sell something we don't want or need.
- To a server it can also be used as a denial-of-service attack.
- By sending a targeted system with thousands of e-mail messages, SPAM can eat available network bandwidth, overload CPUs, cause log files to grow very large, and consume all available disk space on a system.
- Ultimately, it can cause a system to crash.
- SPAM can be used as a means to launch an indirect attack on a third party.

- SPAM messages can contain a falsified return address, which may be the legitimate address of some innocent unsuspecting person.
- As a result, an innocent person, whose address was used as the return address, may be spammed by all the individuals targeted in the original SPAM.
- E-mail filtering can prevent much unwanted e-mail from getting through.
- Unfortunately, it frequently filters out legitimate e-mail as well.

How much Security vs. Accessibility

- Increasing the level of security of a system will often involve adding barriers to the legitimate users of the system.
- This can take many forms including limiting how users can access a system, changing how the system responds to forgotten passwords or by reducing the performance of a system.
- It also involves a lot of additional work for the system administrator and security expert.
- *To decide on the appropriate amount of security to apply you first need to identify the risks and the extent of the damage that insufficient security would cost the business.*
- The cost in breach of security may take the form of lost business, additional cost incurred or damage to the company reputation.
- Assessing the risks in this way a picture can be generated as to what level of security is appropriate.
- Part of the security policy should also identify any systems that are more vulnerable and therefore need a higher level of security than others.
- Whilst in the ideal world every system would be completely secure and safe from attack this is not the case in reality.
- The resources required and the effort involved in trying to secure all systems to the same level may leave exposures or cause such an impact as to prevent the system operating correctly.
- The best approach is to classify security items according to functions.

Categorizing systems based on function

An example of how different systems can be categorised is shown below. In this scenario each system is categorised under three headings. These are red for high risk, yellow for medium risk and green for minimum risk. These may be very different depending upon the requirements of your organisation.

Red - High Risk	Yellow - Medium Risk	Green - Low Risk
Internet web server	Intranet web servers	Users personal computers
Firewalls	Internal database servers	Print servers
Database Servers		Non-essential services (e.g. messaging systems)
Payroll / financial systems		

- The red high risk systems are firstly those that customers will see such as the Web Server;
  - Those that protect the internal networks from the external networks such as firewalls.
  - Those carrying sensitive information such as the Database Servers and any systems that hold information that could damage the company if they were released such as:
  - The payroll and financial systems.
  - Students grades database servers
- The yellow medium risk systems are those on which the business relies however are not accessible to the general public.
  - These are usually internal servers that are protected from outside of the company network by firewalls.
  - The systems under this category should still be considered a high risk if a business function is completely reliant upon them.
  - For example a call receipt desk that handles customer orders would be unable to operate if it could not access the order system.
- The green low risk systems are those where an attack would only have limited effect.
  - For example a PC on a single persons desk, a print server; or a service that the organisation does not depend upon to continue to function, e.g.. a peer to peer messaging system that in the event of failure could be bypassed by using the telephone.
  - When systems are put into the low risk category then the overall risks must be considered.
  - For example do users PC’s contain confidential material, in which case that computer may need to be graded a higher risk than one used for less important data. Another factor to be considered is that if someone was able to break into a print server or personal computer could they then use this to inflict more serious damage?
- These categories must also be used in conjunction with the organisations security policy (see later).
- As an example you may decide that because of confidential information stored on a users laptop

computer you really want to upgrade this to a medium risk, however the security policy states that all medium risk systems must be stored in a secure room with no user access except when the system needs repair.

- By putting the laptop in the medium risk category you have just removed it's usefulness as a portable system, indeed the user may not even have access to it.
- Therefore a degree of flexibility needs to be included when the risk analysis is performed, or by including sufficient flexibility within the company policy.
- For example an exception could be made to allow laptops to be taken out of the office as long as they had data encryption.

Identifying the different risks to a system

- After identifying which systems are at risk, it is also important to consider what the risks to that system are.
- This should be achieved by considering the impact of the different types of attacks.
- I have used an example below of some of the high risk systems to determine the impact of different types of attacks.

	Web server	Firewall	Database servers	Payroll / financial
Reading data	Low	Medium	High	High
Changing data	High	High	High	High
Denial of service	High	High	High	Medium
Normal user login	Low	High	High	High

- As you can see from the table certain types of breaches can have a more damaging effect.
- Looking at the Web server someone being able to read data is pretty low as the data stored on the web server is generally available to anyone, however if someone was able to change the data or prevent the service from working (Denial of Service) then the impact, and reputation would be severely hit.
- On the firewall every type of breach can be serious as it could then be used to target a less secure system inside of the internal network.
- The actual impact is also dependant upon the data for which they can read.
- It is obviously much worse if the user is able to read the information that is categorised as confidential (say for example in a secure part of the web server) than say a document giving directions to the location of the next social event.

By identifying the impact a better strategy can be developed on where to invest the available resources.

Data Classification for Access

- In addition to specifying which systems hold which sensitive data the actual data itself should be categorized depending upon it's sensitivity.
- This is particularly useful in deciding which users on a system should be able to access what files.
- If you limit the access of individual users then this limits the damage that the user can do and if the **userid** becomes compromised limits the damage that the attacker can do.
- More useful than categorizing by sensitivity it is useful to group the data into similar access requirements.
- This is likely to be grouped by departments that handle a certain function.
- Then against each of the categories it should be identified who should have what access. Once method of doing this is known as CRUD analysis. This is simply a case of:

  Who can create the data?
  Who can read the data?
  Who can update the data?
  Who can delete the data?

  Who can execute the file?

This analysis can then be used to create groups with the appropriate access. This also has the advantage of making access easier to manage by associating users with groups rather than having to set-up authority on an individual basis.

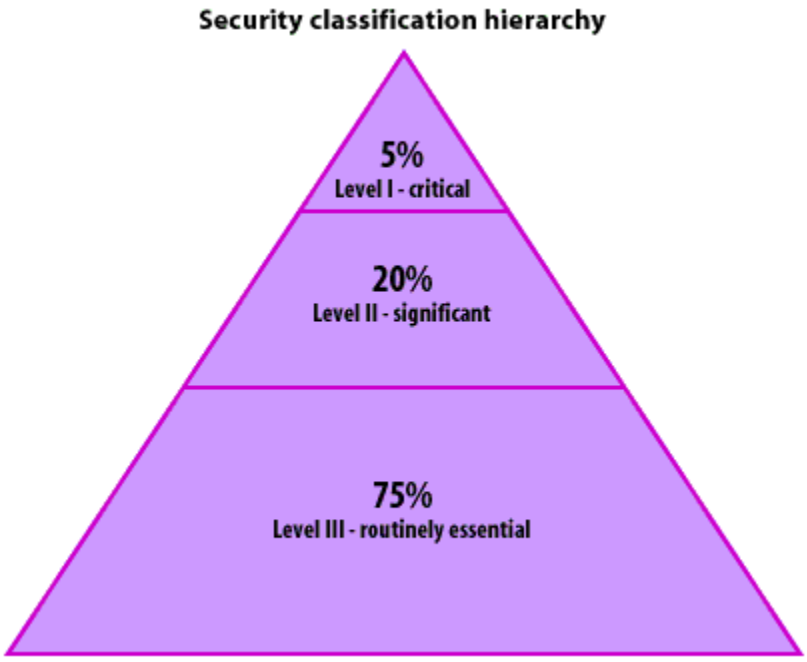
Security policy

Having analyzed the security requirements in the previous section you can now set about work on your own security policy. It may involve writing a security policy from scratch or may be a case of looking to apply a mandated corporate security policy.

- A security policy is a definition of what it means to be secure for a system, organization or other entity.
- A *security policy* is the foundation upon which all security decisions are made.
- A security policy defines each rule to be followed and includes clear explanations of its purpose.
- It should convey the core security values, roles, and responsibilities to the organization.

Develop your security policy by classifying your systems and assigning risk.
Systems classification effectively allocates security resources and develops a sound security infrastructure. Identify and then classify systems and data based on their importance to the organization using the Security Classification diagram below.

- For an organization, it addresses the constraints on behavior of its members as well as constraints imposed on adversaries by mechanisms such as doors, locks, keys and walls.
- For systems, the security policy addresses constraints on functions and flow among them, constraints on access by external systems and adversaries including programs and access to data by people.
- Because the security policy is a high level definition of secure behavior, it is meaningless to claim an entity is "secure" without knowing what "secure" means. It is also foolish to make any significant effort to address security without tracing the effort to a security policy.



1. A Level I system requires significant resources and consideration, whereas a
2. Level III system might need only virus checking. An unrealistic policy will hurt a company's ability to protect itself, and could even damage its ability to communicate efficiently.

Determination of resource risk

- Once all your network's resources have been classified and prioritized, risk factors should be determined for each resource you have defined.
- When determining the risk factors for a resource, use this basic rule:
- The more sensitive the resource, the higher the risk factor.

If you are creating your own security policy there are a number of factors you need to consider.

1. Prior to writing your security policy, create a detailed, written documentation of every system, including hardware types, current configurations, and protocols used.
2. After you have classified all your company's resources, you should include a prioritized threat list and an action list, prioritized by system, in your security implementation plan.
3. You should ensure that you have covered any of the principles Authorisation, Authenticity, Privacy / Confidentiality, Integrity, Non-repudiation and Availability as they apply to your system.
4. Also consider how this is going to be implemented by the users and system administrators.
5. If a security process is hard to implement or restricts someone from doing their job then you may find that the process gets ignored or is not complied with.

Policy requirements

Your security policy should include :

1. Itemized hardware and software and security requirements
2. Physical security
3. Procedures for system failure
4. Procedures for handling system breaches
5. Policies for users and system administrators
6. Requirements for auditing
7. Administrative responsibilities for securing specific systems

Implementing security

Apply your security policy as consistently as possible by :

1. Categorizing and documenting resources
2. Defining and publishing your security policy
3. Secure each resource and service
4. Log, test, and evaluate all systems
5. Keep current and update your policy

When setting up a security policy you should also consider how this can be enforced and audited.

Closing the holes

There are a number of possible security exposures on any computer. Whilst it is practically impossible to fully secure a computer whereby the computer can still fulfil a purpose there are a number of steps that can be carried out to minimise the exposures. These are often referred to as security holes or back doors which need to be closed.

There are also a number of steps that can be taken to try and identify if a machine is under attack or indeed if it has already been penetrated. By regular monitoring of suspicious activities then steps can be taken to limit any damage and to secure against further attack.

Physical security

- Most physical security principles are fairly obvious. If physical access is available to the computer then it's normally trivial to attack a computer by booting into a live CD and then accessing the local disk.
    - Data can be protected from theft by encrypting the disk, but it may still be possible for someone to destroy the information instead.
- All production servers should be kept in a **secure machine room** with restricted access, preferably using an electronic access system or manual key sign-out process to track the physical access.
- To improve system availability one can consider **power on password** when booting the system
- You may also need to consider physical monitoring such as **CCTV** monitoring (a requirement for PCI compliance).
- Use of alarm system with multiple password panels
- Locating a Lab up in the building to limit unauthorized access, break-ins and floods
- Hardening the boot menu by using a password . This will protect the modification of boot start-up to boot into single user mode.
- As well as the obvious areas of physical access to a specific computer or server the physical access to the local area network should also be considered a physical asset to be controlled.
- Many internal networks implement DHCP for the allocation of IP addresses, which makes accessing a network as simple as connecting a portable computer to a network point; even where DHCP isn't available it's usually possible to monitor the network and find the required information that way.

User authorisations

- The normal user authentication is based upon the user being able to provide the correct username and password.
- The username is not something that has to be kept secret as it is readable by anyone on the system however the password is encrypted and should only be known by the user.
- The algorithm used to encrypt the password is a one way password which cannot be reversed. Instead when a user enters their password it is encrypted using the same algorithm and compared against the original.

- Traditionally in UNIX the password was kept in the /etc/passwd file which was readable by all users on the system. Modern Linux distributions use a shadow password file with restricted read permission.
- The following extract shows how this is implemented.
- The /etc/password file still contains password details
- It is important that the password file is kept secure, because although the passwords are encrypted it is possible to perform a dictionary attack against the encrypted passwords.
- These work by taking words from a dictionary and encrypting them as passwords and then comparing them against the password file. If there are any matches then the password is provided.
- These can be more sophisticated by replacing letters with numbers e.g. 1 instead of I etc. and by using different dictionaries the chance of getting the password is better.
- These programs are freely available two examples being “Crack” or “John the Ripper”.
- These can be run by system administrators to ensure that people are using secure passwords.
- It is also possible to have the system check for insecure dictionary passwords when the password is created.

Network security

If you keep a computer off the network then the only security risk exists from people able to physically get access the the computer.

Once you connect to a network it potentially become a target for anyone or any computer around the world. When considering the security for a networked computer then we need to:

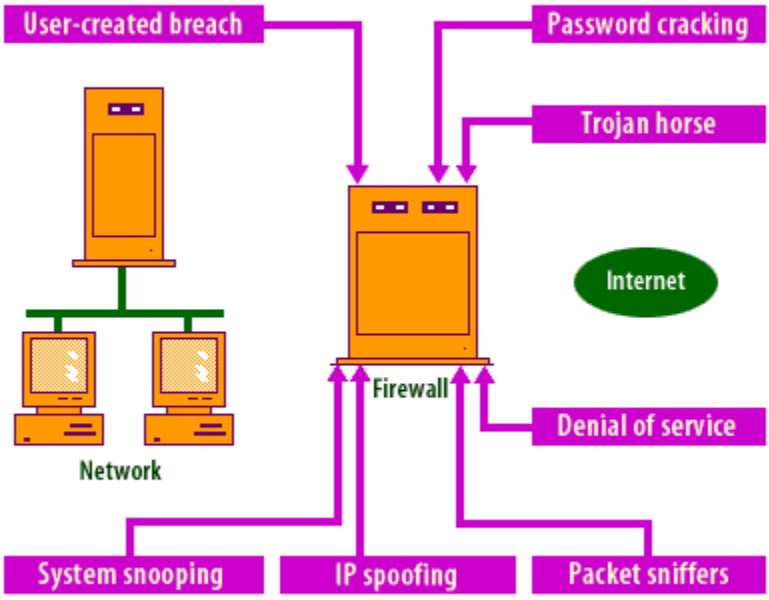
1. Consider the security to prevent someone logging onto the computer, but also
2. The security of data that is transmitted over the network.

Protecting the network using a firewall to restrict access

- One method of providing security is to separate the network that the computer resides on from other networks and in particular the Internet.
- This could be done by ensuring there is no physical routes to any other networks, but usually some form of Internet access is required.
- In this case a dedicated firewall can be used to provide separation from the more secure internal networks to the Internet.
- A firewall uses a set of rules which determines which traffic is allowed to pass and in which direction.
- These are normally used to separate internal networks from external ones (such as the Internet or other business partners), but could also be used to separate different internal networks to prevent someone with access to one network form accessing another part of the company for which they are not authorised.

Firewall: A security system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both.

Protecting wireless networks



- If using an internal wireless network

then not only is there a risk of people accessing the network through a firewall, but the network signal itself could be intercepted or hijacked.

- This would allow someone to either see the traffic being passed over the network or impersonating an internal machine to bypass the firewalls.
- This can be secured by implementing WPA wireless network encryption (note that the older WEP encryption is no longer considered to be secure) or
    - by tunnelling network traffic through a secure connection such as by using VPN tunnelling software.
    - The latter has the advantage that it will also provide protection when using a public network service such as that provided in hotels and wireless hotspots.

Networking protocols

- If using unsecured protocols such as telnet and FTP the passwords are sent unencrypted across the LAN.
- It can be possible for someone with a sniffer or LAN trace tool on the LAN to see these unencrypted passwords.
- If using unsecured network protocols then additional physical security may be required against network ports and restrictions on where that traffic may be routed.
- In some cases the better option is to switch to a protocol with built in security such as ssh, which encrypts any data transmitted.

Protecting the Local Machine From Network Connection

Access control list (ACL)

- An ACL is a list of the entities that can access the resource, such as users, servers, programs, or applets, and their access levels, such as read-only, write-only, read-write, delete, create, access, or other actions.
- If one of these entities attempts to perform an operation beyond its authorized level of access, the operating system will raise an exception or error notification.
- For example, each user or group is assigned an access level in an ACL specifying the operations that each user or group may perform on the database and the documents it contains.
- An authorized user must still pass the ACL test to gain access to a database.

Execution control list (ECL)

- An ECL allows the operating system to limit a program's activity.
- Traditionally, the operations of a program have been predetermined by its creators, and could not be modified or limited in any significant way.
- With an ECL you can determine which of the program's activities are appropriate, and which are not.
- In essence, you can exert operating system-level control over a single application.
- For example, an ECL can minimize the threat of a malicious program, further direct the activity of Java applets, and stop *trojan horses* .

- It can forbid the transmission of certain data and alert you to the unauthorized transmission attempt.
- Eventually, software vendors will begin shipping ECLs, allowing any user to determine the program's parameters.

- Access Control Mechanisms
- Access control mechanisms are essential when securing servers. You must define what users can access on servers, services, and daemons. A hacker can defeat even the most sophisticated operating system with the latest ACL and ECL methods if the administrator uses default settings.

Blocking certain network access

- Another form of protection is to secure the computer by :
  - blocking certain network access based on :
    - limiting running protocols (disabling services),
    - blocking inbound connections (using the personal / in-built firewall,(IPtables in Linux)),
    - by configuring the network protocols to restrict access (eg. By IP address or by blocking certain users from remote logins) or
    - by adding additional restrictions using other software (eg. Tcpwrappers).

Anti-Virus

- Running Windows on a computer and anti-virus software is a must to protect against viruses and spyware software.
- In the Linux world there are currently no active viruses "in the wild".
- This may change in future, but for now there is no significant immediate risk to the local machine from viruses.
- There is however a risk that a Linux machine could harbour a virus that could get inadvertently passed onto others whose choice of operating system is at higher risk of viruses.
- It is therefore recommended to run an anti-virus at least on an occasional basis to provide some level of security for those using other operating systems.
- There are a few different anti-virus packages available either for free or available to purchase.

Unsecured network protocols

- Open protocols such as telnet and FTP the passwords are sent un-encrypted across the LAN.
- It can be possible for someone with a sniffer or LAN trace tool on the LAN to see these unencrypted passwords.
- One can use more secure protocol such as ssh suite of programs (ssh / sftp) can be used to replace telnet and FTP. SSH uses encryption to prevent anyone from sniffing either the password or the data being passed over the connection.

Tunneling Insecure Protocols VPN / SSH Tunneling

- One can encapsulate the information when transmitted over secured network tunnels.
- This can be done using VPN software or hardware, or by using ssh to establish a tunneled connection.

Software updates / patches

- All significant software has bugs. It's a fact of life.
- When a bug is found, especially where security related bugs are concerned, then a fix (or patch) is often provided to fix that bug.
- These can usually be downloaded using the Software Update checker included in most Linux distributions.
- If software is installed form unsupported repositories or outside of the normal software installation process then the system administrator is usually responsible for ensuring patches are up-to-date and may need to follow bug reporting information as well as performing manual updates as required.

Testing for security

- Once the computer has been secured then it should be tested to see if there are any unplanned potential exposures.
- This can taken the form of network port scanning and/or dedicated security software that can fully analyze a system from both local software and networking aspects.
- The practice of testing access is called **penetration testing**.
- Tools for security testing are available as either open-source or closed-source proprietary software.
- A popular open-source network scanner is **Nmap**, which can be used over the network to show network vulnerabilities.
- You should only use penetration testing tools on systems that you are authorized to.
- Running these against other systems could be a considered a criminal act.

Conclusion

We have discussed general security issues which includes :

Types of attacks, Possible solutions, Security policy development factors to consider, Computer based security and Network based security. Having worked through this information it should be possible to work out a plan on which areas to focus resources and provide enough background knowledge as a platform for further research.

We next move to network security encryption schemes digital signatures and hash functions

Appendix A: Terms and Definitions

Key terms and concepts

1. ***Authentication*** proves the identity of an entity during communication or transfer of data.
2. ***Access control*** designates the resources a user or service may access on the system or network.
3. ***Data confidentiality*** protects data from unauthorized disclosure using encryption methods.
4. ***Data integrity*** verifies the consistency of information transferred over the Internet.
5. ***Non-repudiation*** *provides proof of origin and proof of delivery.*
6. ***Back door****:* An intentional hole in a firewall or security apparatus that allows access around security measures.
7. ***Brute-force attack:*** An attempt by a hacker to defeat authentication by obtaining a legitimate user' s password.
8. ***Buffer overflow****:* A popular bug-based attack that works by sending more data than the target system is intended to receive at one time.
9. ***Bug****:* A computer program or hardware error that causes recurring malfunctions.
10. ***Denial-of-service:*** An attempt by attackers to prevent legitimate users of a service from using that service by flooding a network, or by disrupting connections or services.
11. ***Dictionary program:*** A program specifically written to break into a password-protected system. A dictionary program has a relatively large list of common password names that the program repeatedly uses to gain access.
12. ***Front-door attack****:* An attempt by a hacker to access a network by using a valid user name and password.
13. ***Hacke****r:* A user who breaks into sites for malicious purposes.
14. **IP spoofing**: A hacker imitating an Internet Protocol (IP) device that has an IP address allowing the hacker to gain access to the system.
15. ***Open network****:* A group of servers and computers, such as the Internet, which allows free access.
16. ***Password cracking:*** An attempt by a hacker to access a network using possible passwords. A dictionary file is often used to crack passwords.
17. ***Password sniffing:*** Finding a way to intercept the transmission of a password during the authentication process. A sniffer is a program used to intercept passwords.
18. ***Spoofing****:* A form of identity theft in which a hacker attempts to defeat authentication. Specific examples include IP spoofing, ARP spoofing, router spoofing, and DNS spoofing.
19. ***System snooping****:* The action of a hacker who enters a computer network and begins mapping the contents of the system.
20. ***Trojan (trojan horse)****:* A file or program that purports to operate in a legitimate way, but which also has an alternative, secret operation, such as emailing sensitive company information to a hacker. A trojan horse is a specific program that destroys information on a hard drive.
21. ***Virus****:* Self-replicating software used to infect a computer.
22. ***Screening router*** : Examines inbound and outbound packets based upon filter rules. Screening router is another term for a packet filter.
23. ***Firewall:*** A security system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both.
24. ***Firewall token****:* A string of information that identifies a specific user as packets pass through the firewall. A token is usually encrypted.