Learning Management System

Teaching Material Prepared for SYBSc Computer Science and Information Technology Students

Course Title : Network Security (Skill Enhancement Course)

Class : SYBSc (Computer Science and IT)

Prepared By Prof.Dr.B.H.Barhate
Associate Professor, Computer Science Department
Bhusawal Arts,Science and P.O.Nahata commerce College, Bhusawal

Unit-1: Information Security

Prepared By Dr. B. H. Barhate

Information Security

Definition : Information security (IS) is designed to protect the confidentiality, integrity and availability of computer system data from those with malicious intentions. Confidentiality, integrity and availability are sometimes referred to as the CIA Triad of information security. This triad has evolved into what is commonly termed the Parkerian hexad, which includes confidentiality, possession (or control), integrity, authenticity, availability and utility.

Need of Information Security

- **Protecting the functionality of the organisation:** The decision maker in organisations must set policy and operates their organisation in compliance with the complex, shifting legislation, efficient and capable applications.
- **Enabling the safe operation of applications:** The organisation is under immense pressure to acquire and operates integrated, efficient and capable applications. The modern organisation needs to create an environment that safeguards application using the organisations IT systems, particularly those application that serves as important elements of the infrastructure of the organisation.

- **Protecting the data that the organisation collect and use:** Data in the organisation can be in two forms that are either in rest or in motion, the motion of data signifies that data is currently used or processed by the system. The values of the data motivated the attackers to seal or corrupts the data. This is essential for the integrity and the values of the organisation's data. Information security ensures protection of both data in motion as well as data in rest.
- **Safeguarding technology assets in organisations:** The organisation must add intrastate services based on the size and scope of the organisation. Organisational growth could lead to the need for public key infrastructure, PKI an integrated system of the software, encryption methodologies. The information security mechanism used by the large organisation is complex in comparison to a small organisation. The small organisation generally prefers symmetric key encryption of data.

Information Security Principles

Information security is the art and science of protecting valuable information in all the various ways it is stored, transmitted, and used. Information security is a big field, with companies, governments, researchers, and specialists engaged in the work daily. In essence, however, information security rests on four fundamental principles that you can use every day to protect yourself in today's interconnected world.

First Three Principles: CIA Model

These first three principles can be remembered as the CIA model, which stands for confidentiality, integrity, and availability.

- **Confidentiality** means that your information can be seen only by you and those that you want to see the information. Your bank protects the confidentiality of your information by requiring you to enter a PIN that only you know at the ATM to see your balance. They will also require identification when someone conducts a transaction on your account

- **Integrity** involves making sure that your information cannot be changed or removed without your authorization. The information is as you expect it to be, and you'll know if something has changed. Banks put safeguards in place to prevent their employees or anyone else from simply changing your balance without your knowledge. Many banks protect the integrity of your information by letting you set up an alert when money is withdrawn from your account, regardless of who made the withdrawal. These alerts are sent to your phone or e-mail immediately, so you'll know right away if there's a problem.
- **Availability** ensures that you can get to your information when you need it. It wouldn't do you any good to have a bank account if you could never tell how much money was in it or what transactions had occurred. Banks make your information available to you in many ways, such as online banking, ATM balance inquiries, and your monthly statement.

Nonrepudiation is the assurance that someone cannot deny something. Typically, nonrepudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

Anti Virus Software

- Antivirus software is a class of program designed to prevent, detect and remove malware infections on individual computing devices, networks and IT systems.
- Antivirus software, originally designed to detect and remove viruses from computers, can also protect against a wide variety of threats, including other types of malicious software, such as keyloggers, browser hijackers, Trojan horses, worms, rootkits, spyware, adware, botnets and ransomware.

How antivirus software works

- Antivirus software typically runs as a background process, scanning computers, servers or mobile devices to detect and restrict the spread of malware. Many antivirus software programs include real-time threat detection and protection to guard against potential vulnerabilities as they happen, as well as system scans that monitor device and system files looking for possible risks.

Antivirus software usually performs these basic functions :

- Scanning directories or specific files for known malicious patterns indicating the presence of malicious software;
- Allowing users to schedule scans so they run automatically;
- Allowing users to initiate new scans at any time; and
- Removing any malicious software it detects. Some antivirus software programs do this automatically in the background, while others notify users of infections and ask them if they want to clean the files.

Access Control

- Access control is a way of limiting access to a system or to physical or virtual resources. In computing, access control is a process by which users are granted access and certain privileges to systems, resources or information.
- In access control systems, users must present credentials before they can be granted access. In physical systems, these credentials may come in many forms, but credentials that can't be transferred provide the most security.
- There are two types of access control: physical and logical. Physical access control limits access to campuses, buildings, rooms and physical IT assets. Logical access control limits connections to computer networks, system files and data.

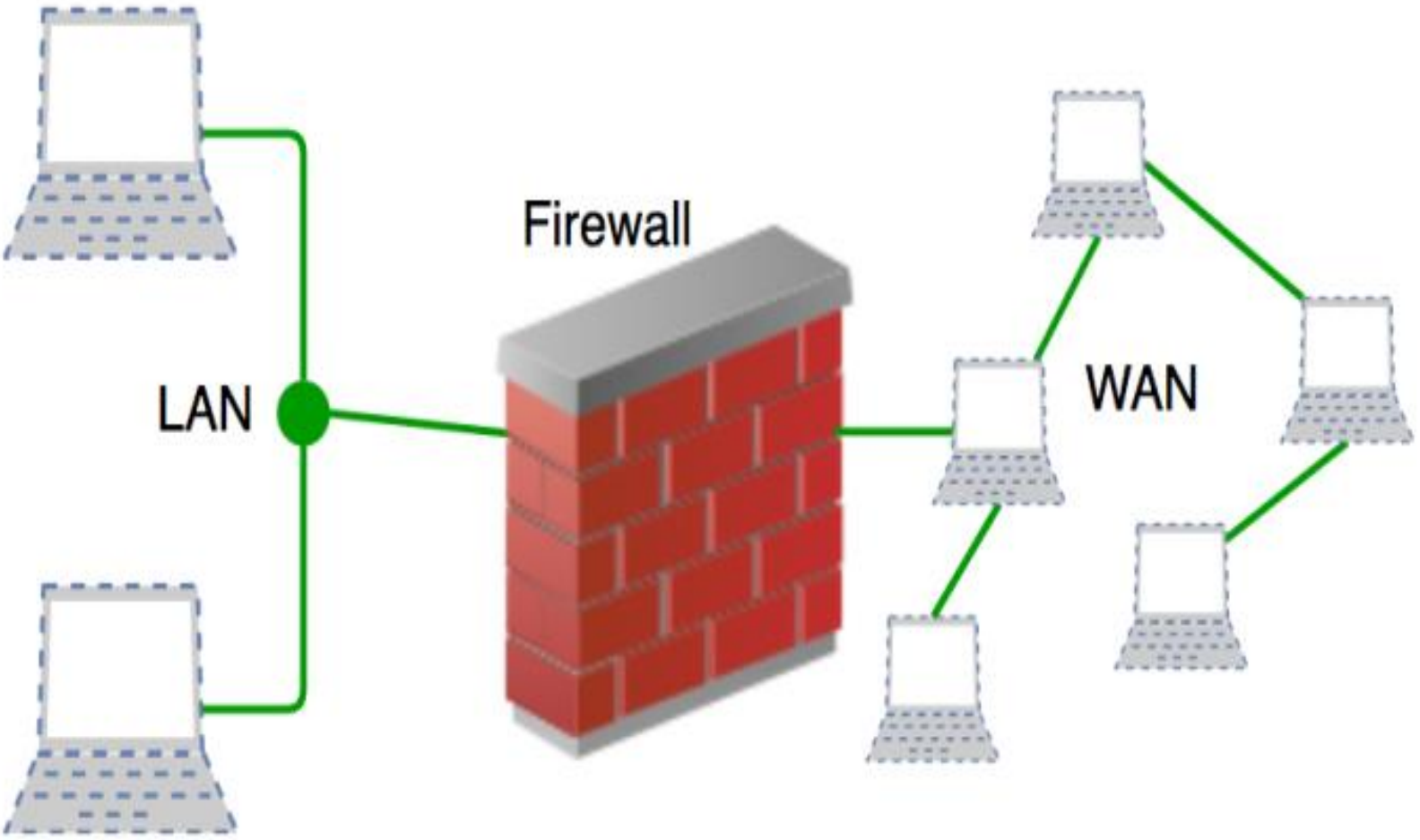
The goal of access control is to minimize the risk of unauthorized access to physical and logical systems. Access control is a fundamental component of security compliance programs that ensures security technology and access control policies are in place to protect confidential information, such as customer data. Most organizations have infrastructure and procedures that limit access to networks, computer systems, applications, files and sensitive data, such as personally identifiable information and intellectual property.

Firewall

A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.

- **Accept:** allow the traffic
  Reject : block the traffic but reply with an "unreachable error"
  Drop : block the traffic with no reply

A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet.


Firewall
LAN
WAN

Smart Card

A smart card is a physical card that has an embedded integrated chip that acts as a security token. Smart cards are typically the same size as a driver's license or credit card and can be made out of metal or plastic. They connect to a reader either by direct physical contact (also known as chip and dip) or through a short-range wireless connectivity standard such as radio-frequency identification (RFID) or near-field communication (NFC).

The chip on a smart card can be either a microcontroller or an embedded memory chip. Smart cards are designed to be tamper-resistant and use encryption to provide protection for in-memory information. Those cards with microcontroller chips can perform on-card processing functions and can manipulate information in the chip's memory.

Smart cards are used for a variety of applications, though most commonly are used for credit cards and other payment cards. Distribution of smart cards in recent years has been driven by the payment card industry's move to support smart cards for the EMV payment card standard.

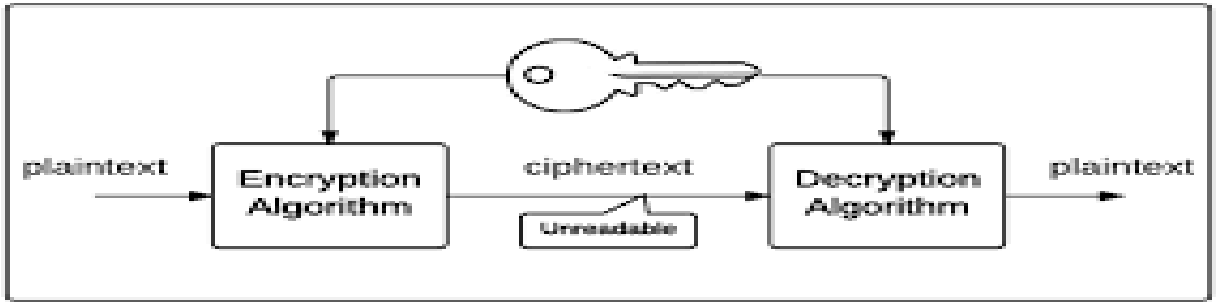
Biometrics

Biometrics are yet another authentication mechanism and they too can reduce the risk of someone guessing a password. There are many types of biometric scanners for verification of any of the following.

- Facial recognition.
- Fingerprints.
- Finger geometry (the size and position of fingers).
- Iris recognition.
- Vein recognition.
- Retina scanning.
- Voice recognition.
- DNA matching.

Encryption

Encryption: Encryption is also one of the important security techniques used to convert the readable data into scramble form. Encryption is the process in which data or information is encoding in a such way that only authorized recipient can read it. In an encryption scheme, the clear information or message, referred to as **plaintext** while the unreadable text is called as **cipher** text.



Unit-2. Malicious Software

Prepared By Dr. B. H. Barhate

Malicious Software

Malicious software, commonly known as malware, is any software that brings harm to a computer system.

Malware can be in the form of worms, viruses, trojans, spyware, adware and rootkits, etc.,

which steal protected data, delete documents or add software not approved by a user.

Malware is software program that is inserted into system, usually covertly, for the purpose of intentionally and deliberately compromising the security principle. such as **Confidentiality, Integrity, Authenticity, Availability**. By compromising the said principle there are so many attack came into picture like **interruption, modification, absorption, fabrication** etc. There are different types of malware based on how malware is spreads called as **propagation** and based on malware takes the action when reaches to victim called as **payload**. **Propagation** includes virus, worms and social engineering and **Payload** includes Steal the information, System corruption, Information theft and Zombies and Bots

Types of Malwares

- **Virus** − A virus is a program that creates copies of itself and inserts these copies into other computer programs, data files, or into the boot sector of the hard-disk. Upon successful replication, viruses cause harmful activity on infected hosts such as stealing hard-disk space or CPU time.
- **Worm** − A worm is a type of malware which leaves a copy of itself in the memory of each computer in its path.
- **Trojan** − Trojan is a non-self-replicating type of malware that contains malicious code, which upon execution results in loss or theft of data or possible system harm.
- **Adware** − Adware, also known as freeware or pitchware, is a free computer software that contains commercial advertisements of games, desktop toolbars, and utilities. It is a web-based application and it collects web browser data to target advertisements, especially pop-ups.
- **Spyware** − Spyware is infiltration software that anonymously monitors users which enables a hacker to obtain sensitive information from the user's computer. Spyware exploits users and application vulnerabilities that is quite often attached to free online software downloads or to links that are clicked by users.
- **Rootkit** − A rootkit is a software used by a hacker to gain admin level access to a computer/network which is installed through a stolen password or by exploiting a system vulnerability without the victim's knowledge.

Computer Virus

- A computer virus is a computer program that can copy itself and infect a computer without the permission or knowledge of the owner.
- One of the first detected virus was the Creeper virus in the early 70's
- Before computer networks became widespread, most viruses spread on removable media, particularly floppy disk.

Basic Computer Viruses

- Trojan Horses
  - appears as interesting program file but when installed it allows intruders to access and read your files
- Worms
  - virus that copies and multiplies itself by computer networks and security fl
- E-mail Viruses
  - use e-mail messages to spread which allow it to automatically forward itself to thousands of people

Types of Viruses

- Boot Sector Virus
  - Infects the boot or MBR of diskettes and hard drives through the sharing of infected disks and pirated software applications
  - Once your hard drive is infected all diskettes that you use in your computer will be infected
- Program Virus
  - Becomes active when the program file (usually with extensions .BIN, .COM, .EXE, .OVL, .DRV) carrying the virus is opened
  - It then makes copies of itself and will infect other programs on the computer
- Multipartite Virus
  - Hybrid of a Boot Sector and Program viruses
  - It infects program files and when the infected program is active it will affect the boot record

Types of Viruses

- Stealth Virus
  - Disguises itself to prevent from being detected by antivirus software
  - It alters its file size or conceals itself in memory
- Polymorphic Virus
  - Act like a chameleon, changing its virus signature (binary pattern) every time it multiples and infects a new file
- Macro Virus
  - Programmed as a macro embedded in a document, usually found in Microsoft Word and Excel
  - Once it gets in to your computer, every document you produce will become infected
  - Relatively new type of virus and may slip by your antivirus software if you don't have the most recent version installed

Signs Your Computer is Infected

- Functions slower than normal
- Responds slowly and freezes often
- Restarts itself often
- See uncommon error messages, distorted menus, and dialog boxes
- Notice applications fail to work correctly
- Fail to print correctly

IT threat evolution Q1 2018. Statistics

- According to KSN:
- Kaspersky Lab solutions blocked 796,806,112 attacks launched from online resources located in 194 countries across the globe.
- 282,807,433 unique URLs were recognized as malicious by Web Anti-Virus components.
- Attempted infections by malware designed to steal money via online access to bank accounts were logged on the computers of 204,448 users.
- Ransomware attacks were registered on the computers of 179,934 unique users.
- Our File Anti-Virus logged 187,597,494 unique malicious and potentially unwanted objects.
- Kaspersky Lab products for mobile devices detected:
  - 1,322,578 malicious installation packages
  - 18,912 installation packages for mobile banking Trojans
  - 8,787 installation packages for mobile ransomware Trojans

Virus Countermeasures

- **Virus Countermeasures:** Countermeasures is term related to security, means identifying vulnerabilities in system and finding the possible solution to protect against threats in the system. In short we can say that it is mechanism for protecting the system against threat.
- **The following point are to considered as counter-measures**
- Install Anti-Virus/Malware Software.
- Keep Your Anti-Virus Software Up to Date.
- Run Regularly Scheduled Scans with Your Anti-Virus Software.
- Keep Your Operating System Current.
- Secure Your Network.
- Think Before You Click.

- **There are Various Anti-Virus are as follows** : It is program use to protect the system from various viruses. It means it provide the security to computer.
- Avira (Windows, Mac)
- Bitdefender (Windows)
- Avast (Windows, Mac)
- AVG (Windows, Mac)
- Lavasoft Ad-Aware Free (Windows)
- eScan Anti-Virus Toolkit (Windows)
- Trend Micro HouseCall (Windows, Mac)
- Malwarebytes Anti-Malware (Windows, Mac)

A **computer worm** is a type of **malicious software** program whose primary function is to infect other computers while remaining active on infected systems. A computer worm is self-replicating **malware** that duplicates itself to spread to uninfected computers.

Types of Worm

Email Worms: Email Worms spread through infected email messages as an attachment or a link of an infected website. Email worms are most often distributed via compromised email attachments. They usually have double extensions (for example, .mp4.exe or .avi.exe) so that the recipient would think that they are media files and not malicious computer programs. When the victims click on the attachment, copies of the same infected file will automatically be sent to addresses from their contacts list.

An email message doesn't have to contain a downloadable attachment to distribute a computer worm. Instead, the body of the message might contain a link that's shortened so that the recipient can't tell what it's about without clicking on it. When they click on the link, they will be taken to an infected website that will automatically start downloading malicious software to their computer.

• **Instant Messaging Worms:** Instant Messaging Worms spread by sending links to the contact list of instant messaging applications.

Instant messaging worms are exactly the same as email worms, the only difference being their method of distribution. Once again, they are masked as attachments or clickable links to websites. They are often accompanied by short messages like "LOL" or "You have to see this!" to trick the victim into thinking that their friend is sending them a funny video to look at.

When the user clicks on the link or the attachment – be it in Messenger, WhatsApp, Skype, or any other popular messaging app – the exact same message will then be sent to their contacts. Unless the worm has replicated itself onto their computer, users can solve this problem by changing their password.

- **Internet Worms:** Internet worm will scan all available network resources using local operating system services and/or scan the Internet for vulnerable machines. If a computer is found vulnerable it will attempt to connect and gain access to them.

  Like they do with computer networks, computer worms also target popular websites with insufficient security. When they manage to infect the site, internet worms can replicate themselves onto any computer being used to access the website in question. From there, internet worms are distributed to other connected computers through the internet and local area network connections.

- **IRC Worms:(Internet Relay Chat)**IRC Worms spread through IRC chat channels, sending infected files or links to infected websites.

  Although illegal, file-sharing and peer-to-peer file transfers are still used by millions of people around the world. Doing so, they are unknowingly exposing their computers to the threat of file-sharing worms. Like email and instant messaging worms, these programs are disguised as media files with dual extensions.

  When the victim opens the downloaded file to view it or listen to it, they will download the worm to their computer. Even if it seems that users have downloaded an actual playable media file, an executable malicious file could be hidden in the folder and discreetly installed when the media file is first opened

- **File-sharing Networks Worms:** File-sharing Networks Worms place a copy of them in a shared folder and spread via P2P network.

  Internet Relay Chat (IRC) is a messaging app that is mostly outdated nowadays but was all the rage at the turn of the century. Same as with today's instant messaging platforms, computer worms were distributed via messages containing links and attachments. The latter was less effective due to an extra layer of protection that prompted users to accept incoming files before any transfer could take place.

Distributed Denial of Service Attacks :

A **Denial-of-Service (DoS) attack** can be defined as an attack bring to shut down (halt) a machine and network or other resources, making it inaccessible to authorized users. DoS attacks achieved this by overloading the target with traffic, or sending information in a such a way that triggers a crash. In both situations, the DoS attack despoils authorized users of the service or resource that what they want to be used. In simple word we say that DoS attacks simply exploit vulnerabilities that cause the target system or service to crash. In this attack attacker use single system and send the multiple request to target system. An additional type of DDoS attack is the Distributed Denial Service of Attack. A DDoS attack occurs instead of being attacked from one location, the target is attacked from many locations at once. It means that the Denial of Service attack is **distributed**.

Distributed Denial of Service Attacks :

A **Denial-of-Service (DoS) attack** can be defined as an attack bring to shut down (halt) a machine and network or other resources, making it inaccessible to authorized users. DoS attacks achieved this by overloading the target with traffic, or sending information in a such a way that triggers a crash. In both situations, the DoS attack despoils authorized users of the service or resource that what they want to be used. In simple word we say that DoS attacks simply exploit vulnerabilities that cause the target system or service to crash. In this attack attacker use single system and send the multiple request to target system. An additional type of DDoS attack is the Distributed Denial Service of Attack. A DDoS attack occurs instead of being attacked from one location, the target is attacked from many locations at once. It means that the Denial of Service attack is **distributed**.

Example

- For example when we access the university web site at the time of result or shopping website while declaring the sales, in this situation every user send same multiple request to web server, which is beyond the capacity of server, then web server cannot identify the request and cannot respond within time. So this is one of simple concept to understand DoS attack.
- Always victims of DoS attacks, target the web servers having heavy-profile like banking sector, Insurance, commerce, and government and Non-government as well as reputed organizations. Though DoS attacks do not typically result in the theft or loss of significant information or other assets, they can cost the victim a great in term of time and money.

Symptoms of DDoS

- Unavailability of a particular websites.
- Performance of Network should be slow
- Unable to access any website and
- Drastically increase spam in your account you receive
- Modern security technologies have developed mechanisms to defend against most forms of DoS attacks, but due to the unique characteristics of DDoS, it is still difficult to prevent easily. However to prevent from DoS/DDoS attack, we have to take some preventive measures like proper bandwidth, optimized website, proper speed, used firewall and implement advance security, identify the legitimate traffic etc.

Types of DDoS attack

- There are different DoS attacks include: **Ping of Death, ICMP flood, SYN flood, Buffer overflow attacks.**
- **Ping of Death** (PoD) is a type of DoS attack in which an attacker attempts to crash, subvert or bring to halt the targeted computer or service by sending malformed or oversized packets using a simple ping command.
- **ICMP (Internet Control Message Protocol) flood : I**n this type of attack, an attacker takes down a victim's computer by capitulate it with **ICMP** echo requests, also known as pings.
- **SYN flood (half-open attack):** In this type of attack an attacker sends a repeated of ***SYN*** requests to a target's system, which aims to make a server unavailable to legitimate traffic by consuming all available server resources.
- **Buffer overflow attacks (**buffer ***overrun) :*** *This type of attack*, occurs when buffer is overloaded more than its capacity i.e When more data is put into a fixed-length ***buffer*** than the ***buffer*** can handle.) This extra information, goes to somewhere, can ***overflow*** into adjacent memory space, which corrupting or overwriting the data held in that space.
-

Types of Attacks

- *Bandwidth Consumption*: All available bandwidth used by the attacker e.g.,ICMP ECHO attack
- *Resource Consumption*: Resources like web server, print or mail server flooded with useless requests e.g., mail bomb

- *Network Connectivity*: The attacker forces the server to stop communicating on the network e.g., SYN Flooding.

What is Denial of Service Attack?

- Main aim to stop the victim's machine from doing it's required job
- Server unable to provide service to legitimate clients
- Damage done varies from minor inconvenience to major financial losses

Unit 3- Types of Attack

Prepared By Dr. B. H. Barhate

Snooping

Snooping, in a security context, is unauthorized access to another person's or company's data. The practice is similar to eavesdropping but is not necessarily limited to gaining access to data during its transmission. Snooping can include casual observance of an e-mail that appears on another's computer screen or watching what someone else is typing. More sophisticated snooping uses software programs to remotely monitor activity on a computer or network device.

Snooping

Malicious hacker keyloggers to monitor keystrokes, capture passwords and login information, and to intercept e-mail and other private communications and data transmissions. Corporations sometimes snoop on employees legitimately to monitor their use of business computers and track Internet usage; governments may snoop on individuals to collect information and avert crime and terrorism.

DHCP

Dynamic Host Configuration Protocol (DHCP) is a network protocol that enables a server to automatically assign an IP address to a computer from a defined range of numbers (that is, a scope) configured for a given network.

An Internet Protocol address (IP address) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. An IP address serves two main functions: host or network interface identification and location addressing.

IGMP ,DHCP Snooping

IGMP snooping is the process of listening to Internet Group Management Protocol (**IGMP**) network traffic to control delivery of IP multicasts. Network switches with **IGMP snooping** listen in on the **IGMP** conversation between hosts and routers and maintain a map of which links need which IP multicast transmission.

In Computer networking, **DHCP snooping** is a series of techniques applied to improve the security of a DHCP infrastructure.

When DHCP servers are allocating IP addresses to the clients on the LAN, DHCP snooping can be configured on LAN switches to prevent malicious or malformed DHCP traffic, or rogue DHCP servers. In addition, information on hosts which have successfully completed a DHCP transaction is accrued in a database of "bindings" which may then be used by other security or accounting features.

Eavesdropping

- Majority of network communications occur in an unsecured or “cleartext” format.
- Allows attacker to “listen in” or read the network traffic.
- Known as Sniffing or Snooping
- Biggest security issue faced by network administrators in an enterprise.

Eavesdropping (cont.)

- Prevention
  - In order to prevent the eavesdropping of data traversed on your network, you must have strong encryption services based on cryptography.

How to prevent Eavesdropping attacks?

- **Military-grade encryption:** encryption is a great way to defend an eavesdropping attack. In case an attacker manages to intervene between a communication, he would be successful only if he can read the data that is being exchanged. By using a 256-bit, also known as military-grade encryption, the attacker may gather the data via eavesdropping, but the data will still be safe as it will take him around 500 billion years to decode it.
- **Spread awareness:** training and informing the employees of the organization about cybersecurity is of utmost importance. An employee, unaware of cybercrimes such as eavesdropping attacks may unknowingly put the organization at risk. So, the employee should have complete knowledge about eavesdropping attacks before he/she downloads an application, software or connects over a weak network.
- **Network segmentation:** it is ideal to split the computer network and allowing only certain teams or key personnel to connect to the network; for instance, the marketing team does not need to access the HR system. Network division or segmenting helps in decongesting the network traffic, improves security and prevents unwanted connectivity.

Implications of Eavesdropping

- **Loss of privacy:** Every business has confidential information that could lead the organization astray if it becomes public. While eavesdropping, the attackers will absorb vital business information, ideas and conversations being exchanged within the organization, thereby affecting its privacy
- **Identity theft:** Say, two employees are having a conversation about their access to critical applications. One of them says, “my password to application XYZ has been changed from abdcde to 1234” now, the attacker who has been eavesdropping on their conversation has easy access to their credentials; will easily access the application and steal all the important information.
- **Financial loss:** Once the cyber attacker has vital business information, essential database or passwords to vital business applications, it can be used to full advantage by exposing the data or selling it to the competitors; the attackers will earn, and the organization will lose in millions.

Interception:

Interception: The phenomenon of confidentiality plays an important role in this type of attack. The data or message which is sent by the sender is intercepted by an unauthorized individual where the message will be changed to the different form or it will be used by the individual for his malicious process. So the confidentiality of the message is lost in this type of attack.

There are **different types of security attacks** which affect the communication process in the network and they are as follows

Interruption: This type of attack is due to the obstruction of any kind during the communication process between one or more systems. So the systems which are used become unusable after this attack by the unauthorized users which results in the wastage of systems.

Modification: As the name indicates the message which is sent by the sender is modified and sent to the destination by an unauthorized user. The integrity of the message is lost by this type of attack. The receiver cannot receive the exact message which is sent by the source which results in the poor performance of the network.

Fabrication: In this type of attack a fake message is inserted into the network by an unauthorized user as if it is a valid user. This results in the loss of confidentiality, authenticity and integrity of the message.

Effects :

- The unauthorized person or program may gain ownership of your data or even programs
- One can change your data or even program
- Due to authorized change in data or program, you may lose consistency in data as well as the program.
- Even unauthorized persons/program can transmit modified data to the receiver. can send no ethical or wrong data from your account, for which you may be responsible.

Example :

- Overloading a server host so that it cannot respond.
- Cutting a communication line.
- Blocking access to a service by overloading an intermediate network or network device.
- Redirecting requests to invalid destinations.
- Theft or destruction of software or hardware involved

Hacking Techniques

Hacking is identifying weakness in computer systems or networks to exploit its weaknesses to gain access. Example of Hacking: Using password cracking algorithm to gain access to a system

Open sharing :

A physical threat is any threat to your sensitive information that results from other people having direct physical access to your devices like laptops, hard drives, and mobile devices.
Physical security threats are often underestimated in favour of technical threats such as phishing and malware. Physical device threats occur when someone is able to physically gain access to your confidential data like data gathered from stolen devices.

How to stay safe :

- Be careful, how you store confidential information. Use encrypted computer hard drives, USBs, etc. if they contain sensitive information.
- Never write your passwords on a post-it or notepad.
- Never leave your system unattended. Always protect it with a strong password.
- Don‘t leave your phone unlocked and unattended.
- Make sure proper backup and remote wipe services are enabled in case you lose your device.

Bad Password :

A password cracker is to find a user‘s password. It is used by both computer crackers and system administrators for recovering unknown or lost passwords. There are three major types of crackers. The first type is the smart guessing cracker, which infers or guesses the password based on the user information, such as user name, birthday and phone number. The second is the dictionary-based cracker, which generates a large set of possible passwords, called the dictionary, from a collection of words and phrases. These two types of crackers are smart and quick, but may not work if the password is gene rated randomly. Hence, the third type is to enumerate and test all possible passwords in a brute-force way. When the password is extremely long, the last type will usually take a tremendous amount of time.

Here are 10 bad password habits :

1. Including any part of your name in your password (like _henrik19‘)
2. Using the characters, in order, on the first row of your keyboard (_qwerty‘)
3. Including your birthday, or other meaningful numbers (worst of all your social security number)
4. Choosing _password‘ as your password
5. Using the same password on multiple websites, or cycling between a handful of passwords
6. Using all lowercase letters (mixing lowercase and capital letters make it harder to guess)
7. Storing passwords in memory, on paper, or anywhere else they could be easily lost and/or stolen
8. Neglecting to change your passwords for more than 6 months
9. Sharing your password too frequently or with people who you don‘t trust 110%
10. Storing your password on your browser (especially on a mobile device that you might lend or lose!)

Programming Flaw:

A term used to describe a problem that exists in a software program. A flaw can be a security risk, cause the program to crash, or cause other issues. To resolve flaws, the software developer release updates or patches that updates the code and corrects the issue.

Computers are complex machines that contain hardware from different companies, run software containing thousands of lines of code, and use several drivers. Honestly, it's amazing that they are as stable as they are today.

Security expert discovered severe flaws in most popular programming languages that could expose to hack any secure application built on top of them.

Most problems are related to a software programming error that can be fixed by obtaining an update version (patch) of the software code. Patches are released by the developer and can be downloaded from the Internet or through the program. Below are the reasons why a computer could experience a problem become unstable, or encounter an error.

Reasons to fail Computers

- Data corruption
- Dust and dirt
- Hardware failure
- Hardware confliction
- Heat
- Electrical interference
- Improper drivers
- Lack of resources
- Malicious user
- Outdated software
- Outdated drivers
- Outdated operating system
- Programming error
- Software confliction
- User error
- Viruses or malware
- Movement

Sniffing Switch Network

Sniffing is the process of monitoring and capturing all the packets passing through a given network using sniffing tools. It is a form of "tapping phone wires" and get to know about the conversation. It is also called wiretapping applied to the computer networks.

There is so much possibility that if a set of enterprise switch ports is open, then one of their employees can sniff the whole traffic of the network. Anyone in the same physical location can plug into the network using Ethernet cable or connect wirelessly to that network and sniff the total traffic.

In other words, Sniffing allows you to see all sorts of traffic, both protected and unprotected. In the right conditions and with the right protocols in place, an attacking party may be able to gather information that can be used for further attacks or to cause other issues for the network or system owner.

One can sniff the following sensitive information from a network

- Email traffic ,FTP passwords ,Web traffics, Telnet passwords, Router configuration
- Chat sessions, DNS traffic

What is IP spoofing?

IP spoofing is the creation of Internet Protocol (IP) packets which have a modified source address in order to either hide the identity of the sender, to impersonate another computer system, or both. It is a technique often used by bad actors to invoke DDoS attacks against a target device or the surrounding infrastructure.

Sending and receiving IP packets is a primary way in which networked computers and other devices communicate, and constitutes the basis of the modern internet. All IP packets contain a header which precedes the body of the packet and contains important routing information, including the source address. In a normal packet, the source IP address is the address of the sender of the packet. If the packet has been spoofed, the source address will be forged.

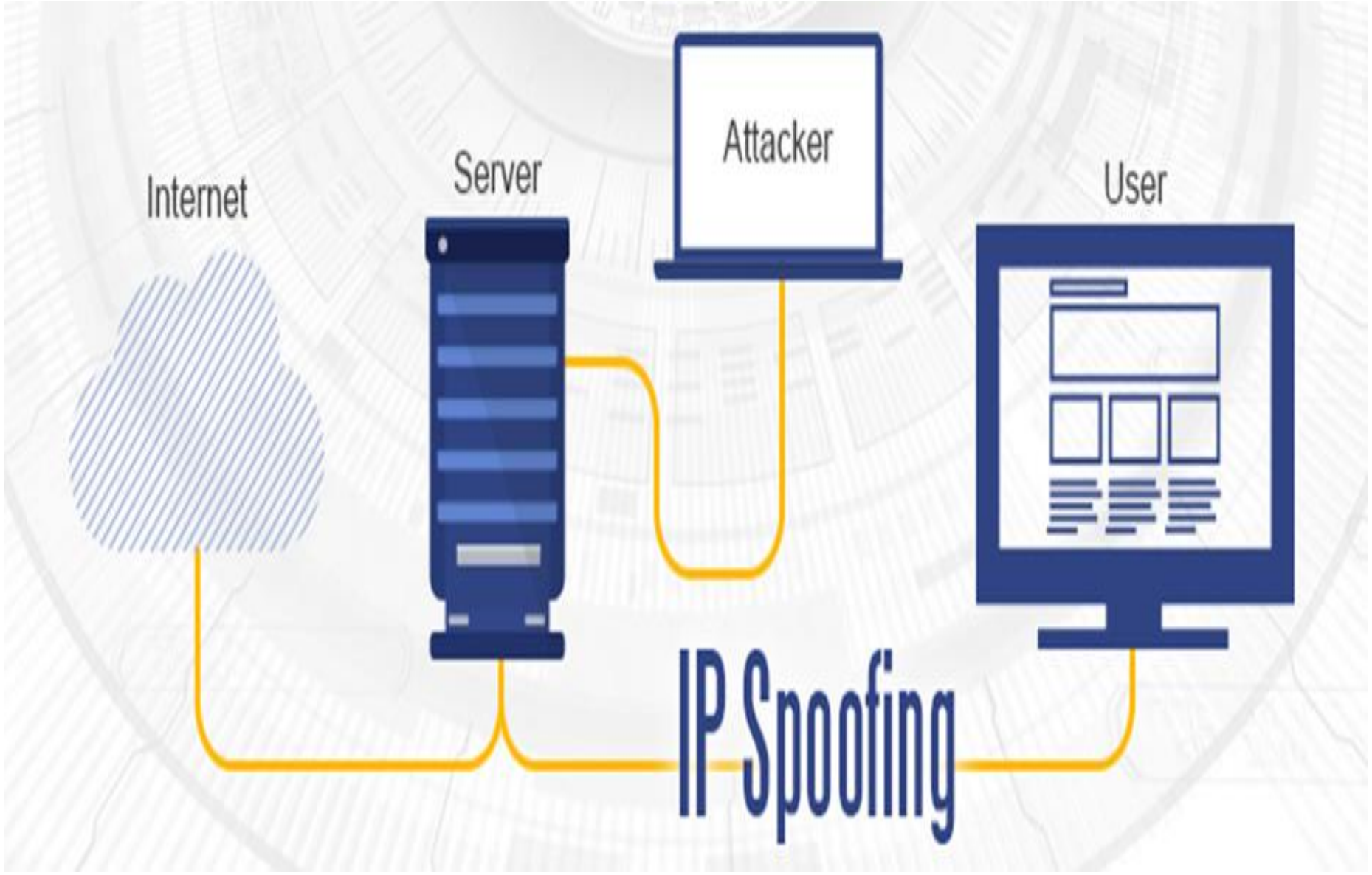
Spoofing is a specific type of cyber-attack in which someone attempts to use a computer, device, or network to trick other computer networks by masquerading as a legitimate entity. It's one of many tools hackers use to gain access to computers to mine them for sensitive data, turn them into zombies (computers taken over for malicious use), or launch Denial-of-Service (DoS) attacks. Of the several types of spoofing, IP spoofing is the most common.

How spoofing works :

To start, a bit of background on the internet is in order. The data transmitted over the internet is first broken into multiple packets, and those packets are transmitted independently and reassembled at the end. Each packet has an IP (Internet Protocol) header that contains information about the packet, including the source IP address and the destination IP address.

In IP spoofing, a hacker uses tools to modify the source address in the packet header to make the receiving computer system think the packet is from a trusted source, such as another computer on a legitimate network, and accept it. Because this occurs at the network level, there are no external signs of tampering.

This type of attack is common in Denial-of-Service (DoS) attacks, which can overwhelm computer networks with traffic. In a DoS attack, hackers use spoofed IP addresses to overwhelm computer servers with packets of data, shutting them down. Geographically dispersed botnets — networks of compromised computers - are often used to send the packets. Each botnet potentially contains tens of thousands of computers capable of spoofing multiple source IP addresses. As a result, the automated attack is difficult to trace.


Internet
Server
Attacker
User
IP Spoofing

Firewall

Prepared By Dr. B. H. Barhate

Firewall

What is Firewall

Broadly speaking, a computer firewall is a software program that prevents unauthorized access to or from a private network. Firewalls are tools that can be used to enhance the security of computers connected to a network, such as LAN or the Internet. They are an integral part of a comprehensive security framework for your network.

A firewall absolutely isolates your computer from the Internet using a "wall of code" that inspects each individual "packet" of data as it arrives at either side of the firewall — inbound to or outbound from your computer — to determine whether it should be allowed to pass or be blocked.

Need of Firewall

Firewalls can be an effective means of protecting a local system or network of systems from network-based security threats while at the same time affording access to the outside world via wide area networks and the internet.

Information systems in corporations, government agencies, and other organizations have undergone a steady evolution. The following are notable developments:

- Centralized data processing system, with a central mainframe supporting a number of directly connected terminals
- Local area networks (LANs) interconnecting PCs and terminals to each other and the mainframe
- Premises network, consisting of a number of LANs, interconnecting PCs, servers, and perhaps a mainframe or two
- Enterprise-wide network, consisting of multiple, geographically distributed premises networks interconnected by a private wide area network (WAN)
- Internet connectivity, in which the various premises networks all hook into the Internet and may or may not also be connected by a private WAN

Characteristics of Firewall

•All traffic from inside to outside, and vice versa, must pass throug h the firewall. This is achieved by physically blocking all access to the local network except via the firewall. Various configurations are possible.

•Only authorized traffic, as defined by the local security policy, will be allowed to pass. Various types of firewalls are used, which impl ement various types of security policies.

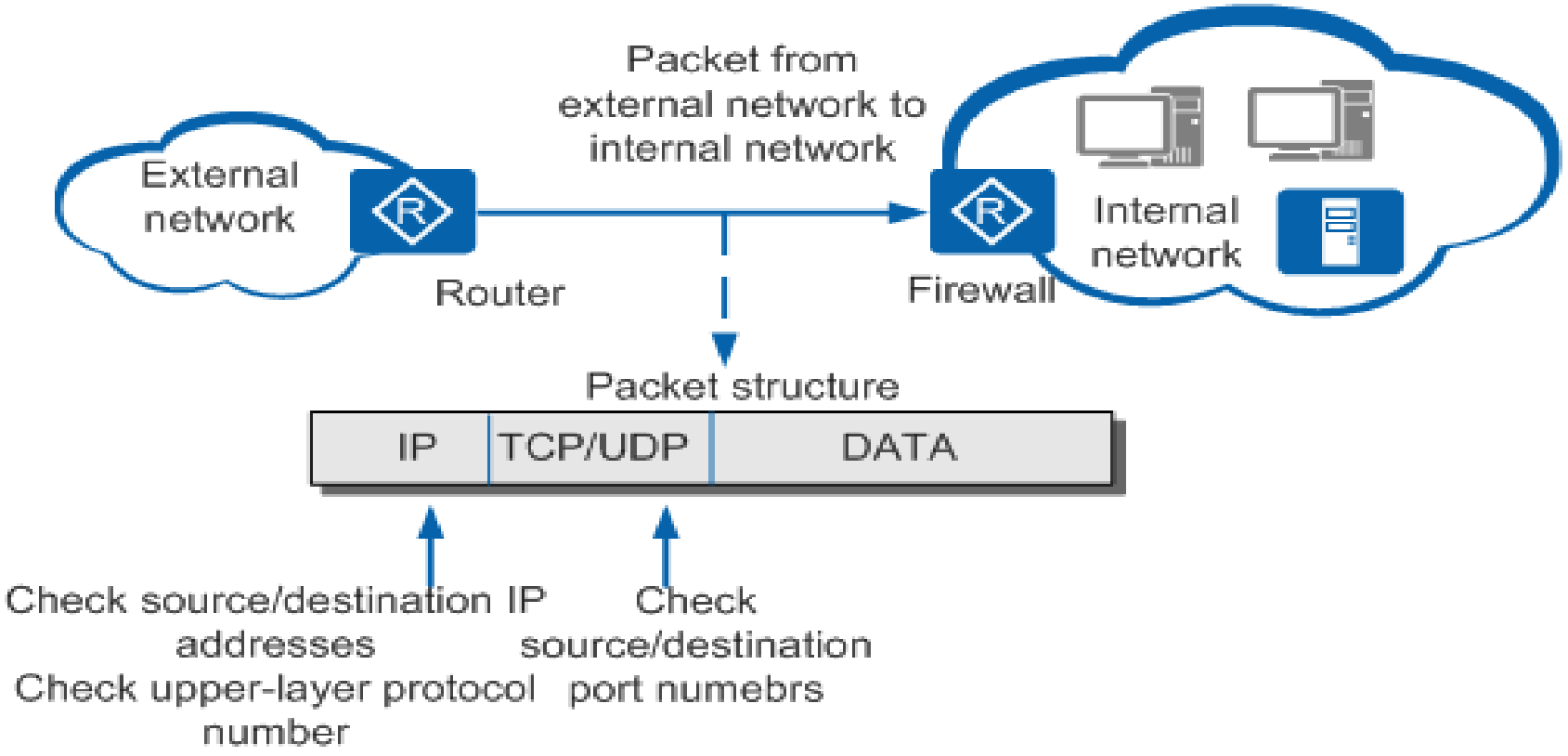
•The firewall itself is immune to penetration. This implies the use o f a hardened system with a secured operating system. Trusted computer system are suitable for hosting a firewall and often required in government applications

Types of Firewall

1.Packet filtering firewalls

This, the original type of firewall, operates inline at junction points where devices such as routers and switches do their work. However, this firewall doesn't route packets, but instead compares each packet received to a set of established criteria — such as the allowed IP addresses, packet type, port number, etc.

When receiving an IP datagram, the firewall obtains the packet header, and then compares the packet header information with ACL rules to determine whether to forward or discard the IP datagram. Following Figure shows how packet filtering is implemented on the firewall.



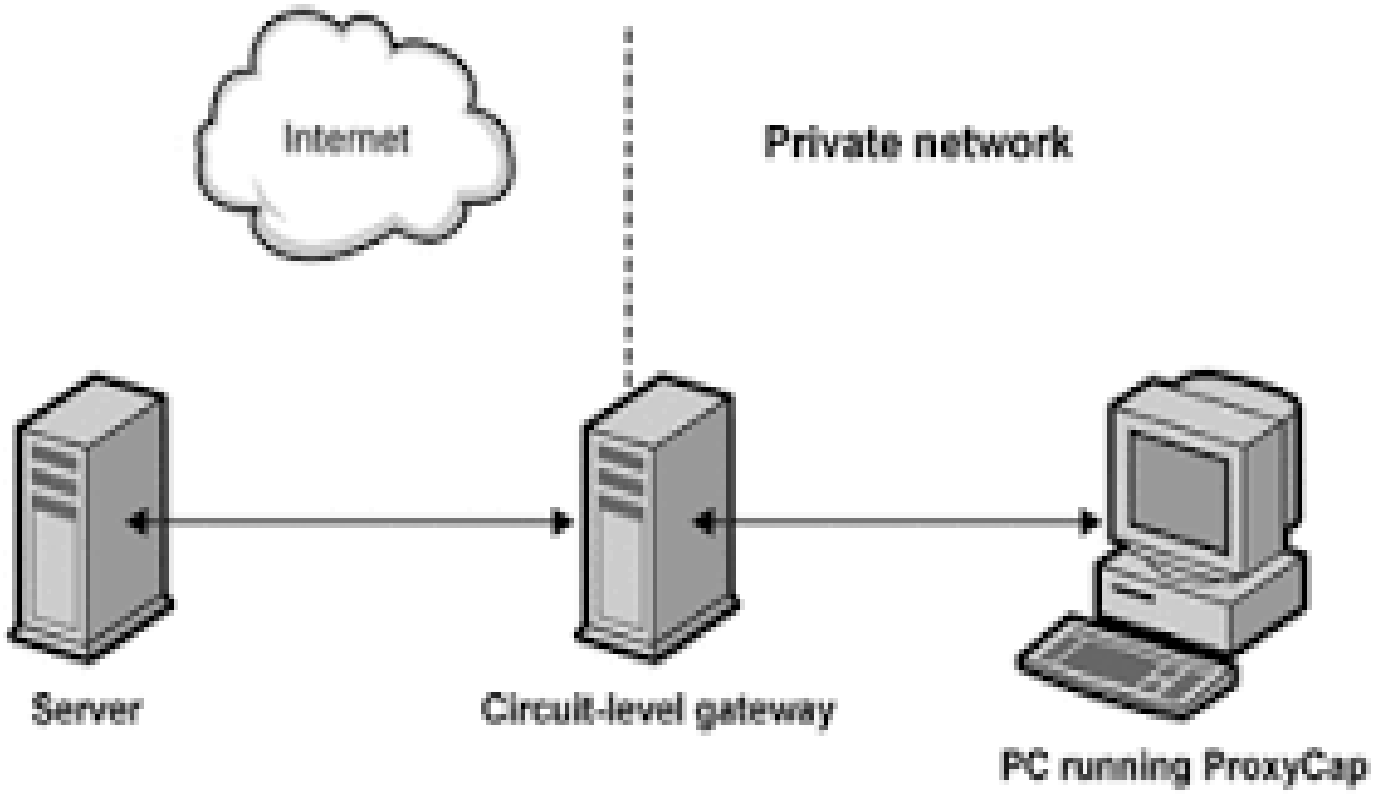
The device supports packet filtering firewall and can filter the following packets:

- Common IP packets: The firewall checks the source and destination IP addresses, source and destination port numbers, and protocol IDs of
- IP packets against an ACL. It forwards the packets permitted by the ACL and discards the packets denied by the ACL.
- The information that the firewall checks is contained in the IP, TCP, or UDP header.

2.Circuit-level gateways

A circuit-level gateway is a firewall that provides User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) connection security, and works between an Open Systems Interconnection (OSI) network model's transport and application layers such as the session layer. Unlike application gateways, circuit-level gateways monitor TCP data packet handshaking and session fulfilment of firewall rules and policies.

Using another relatively quick way to identify malicious content, these devices monitor the TCP handshakes across the network as they are established between the local and remote hosts to determine whether the session being initiated is legitimate — whether the remote system is considered trusted.


Internet
Private network
Server
Circuit-level gateway
PC running ProxyCap

3.Stateful inspection firewalls

State-aware devices, on the other hand, not only examine each packet, but also keep track of whether or not that packet is part of an established TCP session. This offers more security than either packet filtering or circuit monitoring alone, but exacts a greater toll on network performance.

A firewall does all of the following tasks:

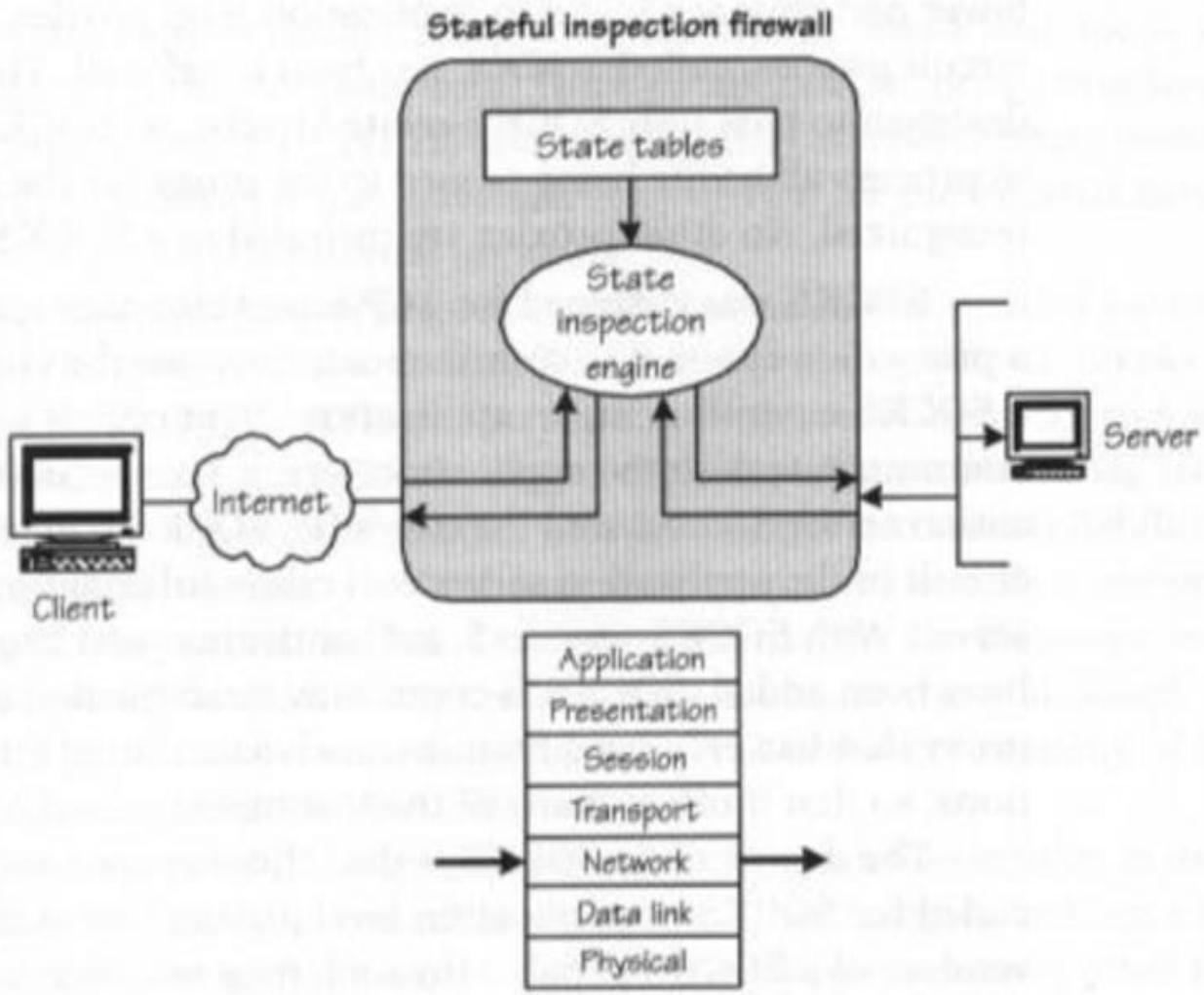
•Prevents any unauthorized users from accessing the computers and networks in your organization that connect to the Internet

•Monitors the communication between your computers and other computers on the Internet

•Creates a shield that allows or blocks attempts to access the information on your computer

•Warns you of connection attempts from other computers

•Warns you of connection attempts by the applications on your computer that connect to other computers

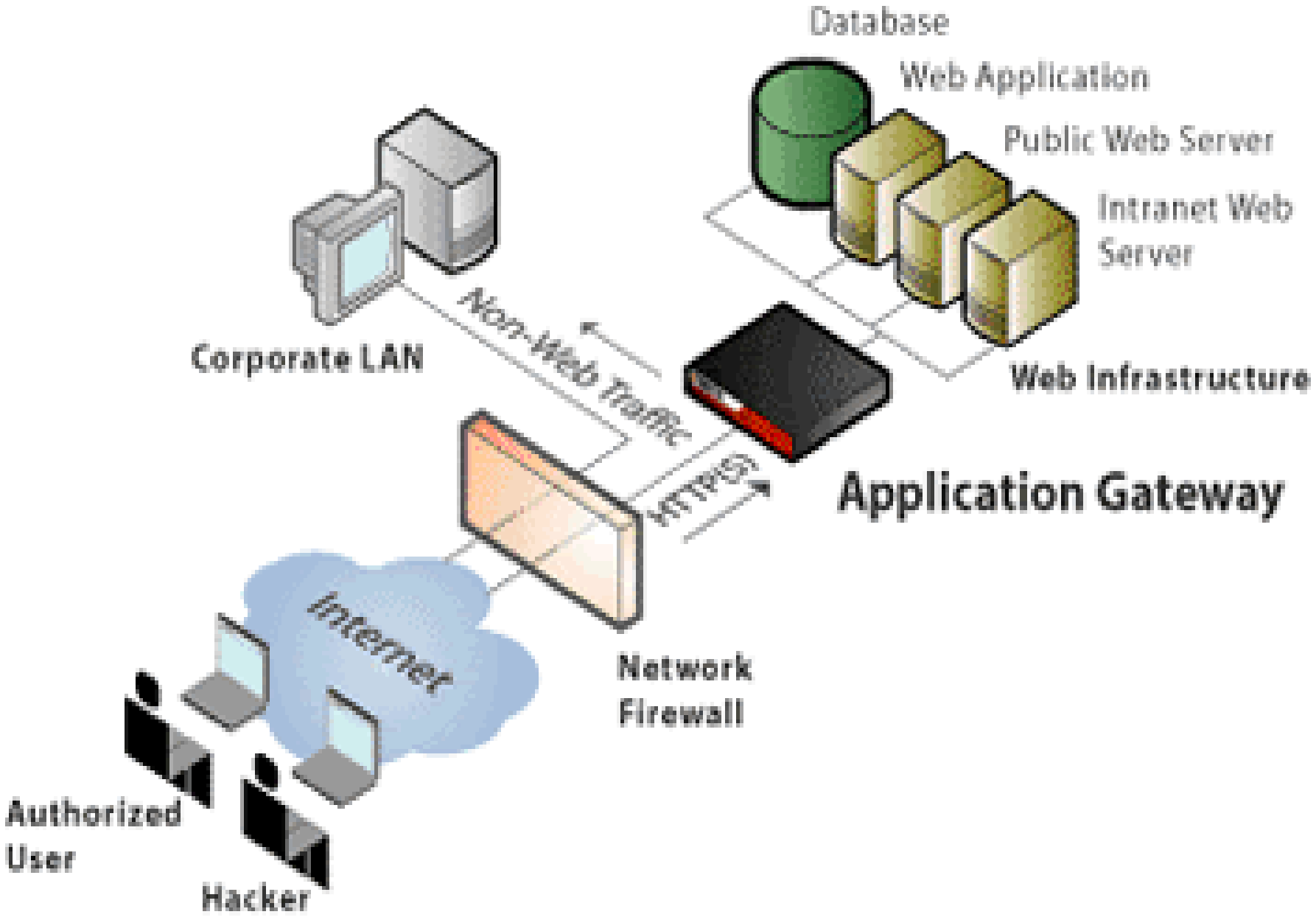

Stateful inspection firewall
State tables
State inspection engine
Internet
Client
Server
Application
Presentation
Session
Transport
Network
Data link
Physical

4.Application-level gateways

An application gateway or application level gateway (ALG) is a firewall proxy which provides network security. It filters incoming node traffic to certain specifications which mean that only transmitted network application data is filtered. Such network applications include File Transfer Protocol (FTP), Telnet, Real Time Streaming Protocol (RTSP) and BitTorrent.

Application gateways provide high-level secure network system communication. For example, when a client requests access to server resources such as files, Web pages and databases, the client first connects with the proxy server, which then establishes a connection with the main server.

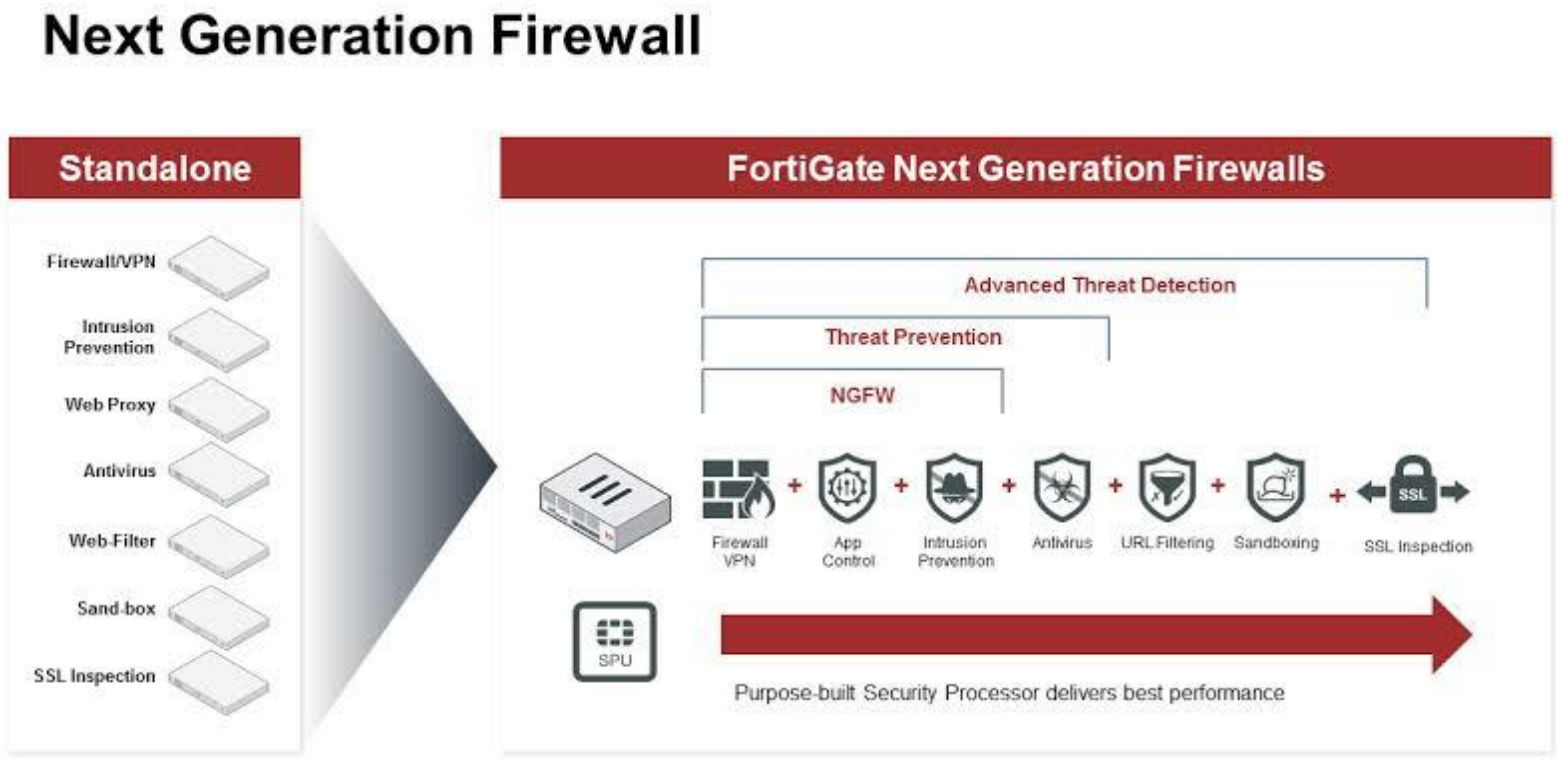
The application gateway resides on the client and server firewall. The proxy server hides Internet Protocol (IP) addresses and other secure information on the client's behalf. A computer's internal system may communicate with an external computer using firewall protection. The application gateway and external computer function without client information or knowledge of the proxy server IP address


Database
Web Application
Public Web Server
Intranet Web Server
Web Infrastructure
Corporate LAN
Non-Web Traffic
HTTP(S)
Application Gateway
Internet
Network Firewall
Authorized User
Hacker

5.Next-gen firewalls

A next generation firewall (NGFW) is, as Gartner defines it, a “deep-packet inspection firewall that moves beyond port/protocol inspection and blocking to add application-level inspection, intrusion prevention, and bringing intelligence from outside the firewall.”

As their name suggests, next generation firewalls are a more advanced version of the traditional firewall, and they offer the same benefits. Like regular firewalls, NGFW use both static and dynamic packet filtering and VPN support to ensure that all connections between the network, internet, and firewall are valid and secure. Both firewall types should also be able to translate network and port addresses in order to map IPs.



FIREWALL BASING

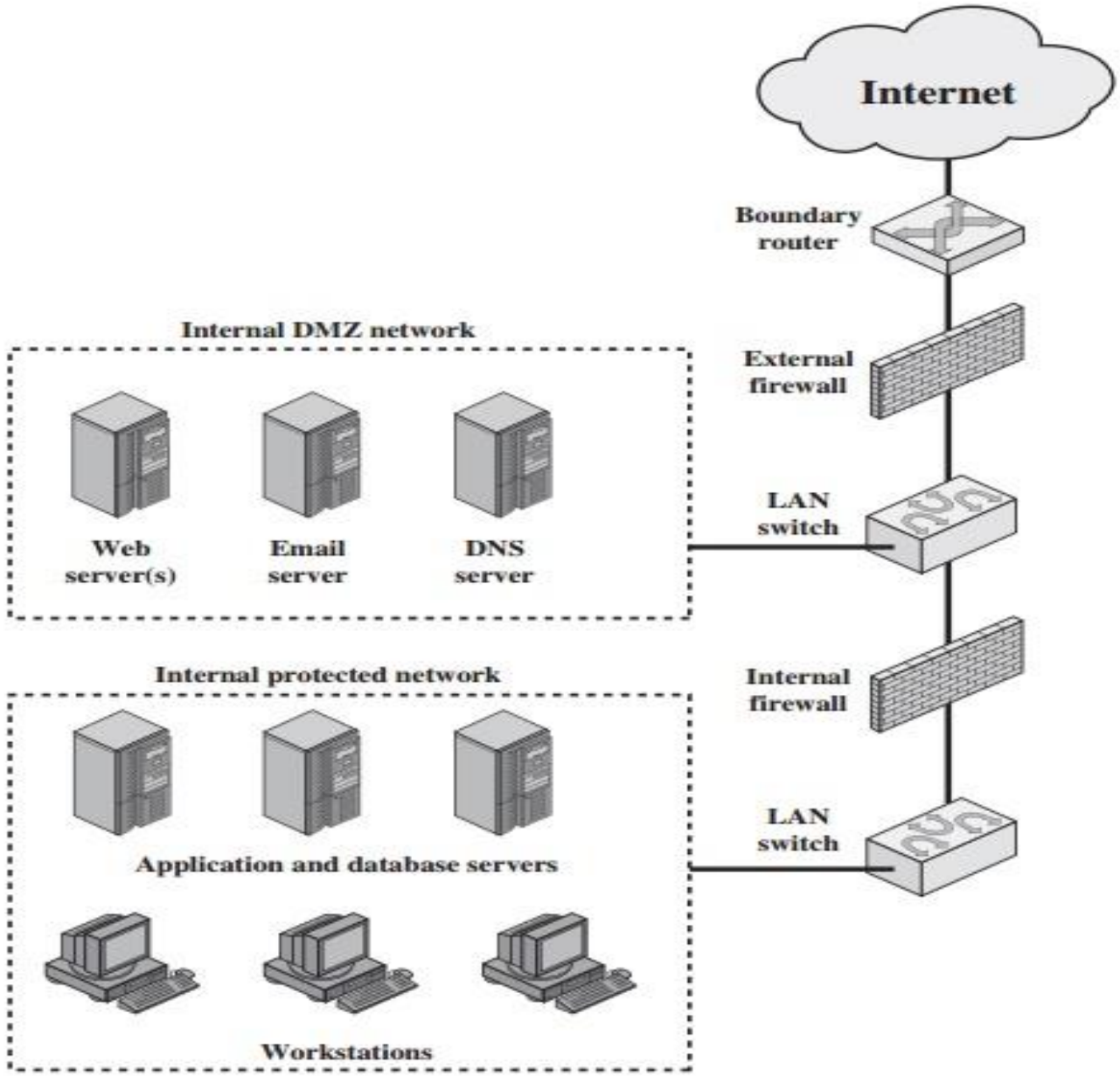
It is common to base a firewall on a stand-alone machine running a common operating system such as UNIX or Linux. Firewall functionality can also be implemented as a software module in a router or LAN switch. In this section, we look at some additional firewall basing considerations.

The bastion host hardware platform executes a secure version of its operating system, making it a hardened system.

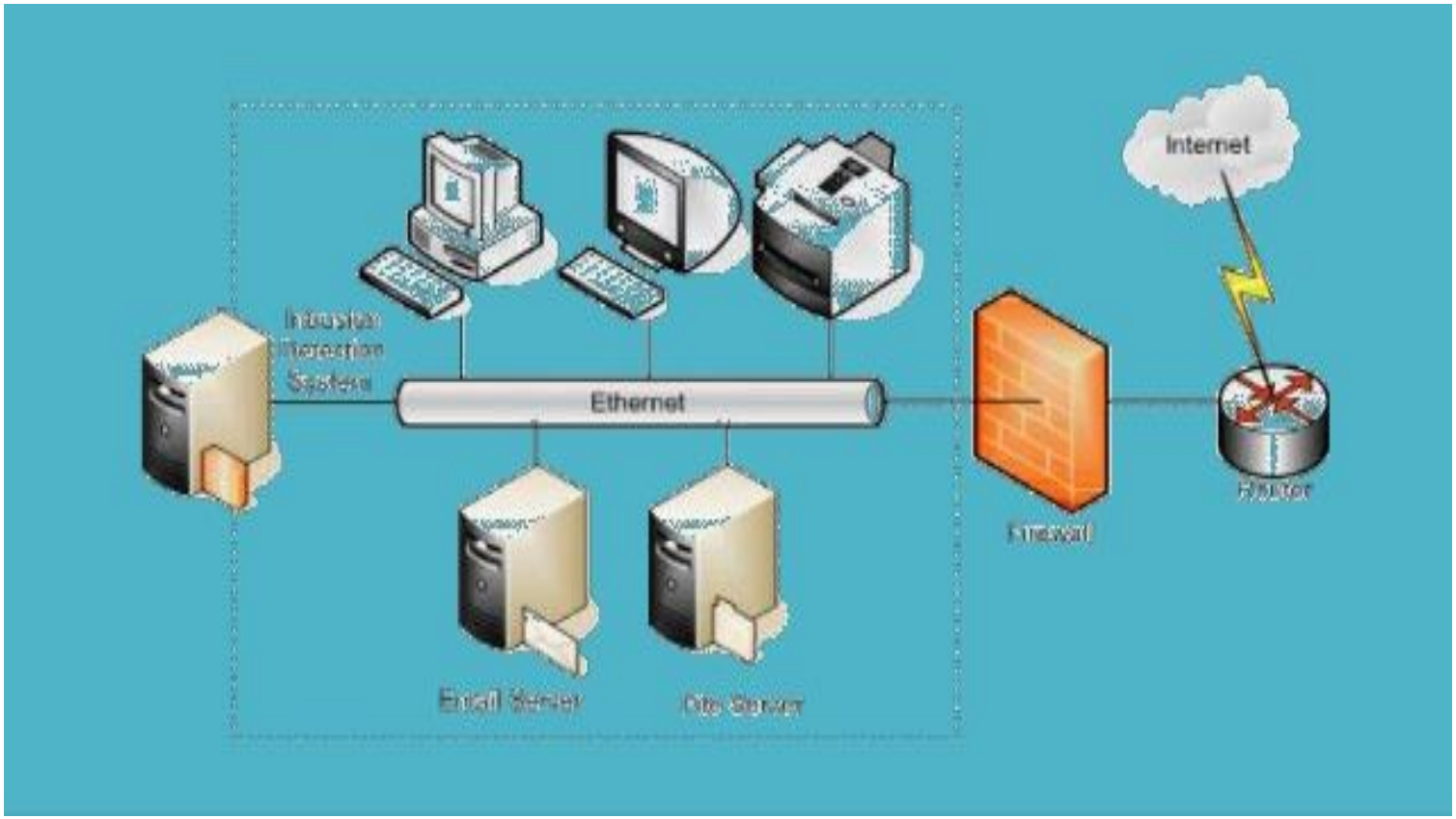
•Only the services that the network administrator considers essential are installed on the bastion host.These could include proxy applications for DNS, FTP, HTTP, and SMTP.
•The bastion host may require additional authentication before a user is allowed access to the proxy services. In addition, each proxy service may require its own authentication before granting user access.
•Each proxy is configured to support only a subset of the standard application's command set
•Each proxy is configured to allow access only to specific host systems. This means that the limited command/feature set may be applied only to a subset of systems on the protected network.

Firewall Location and Configurations

Following figure suggests the most common distinction, that between an internal and an external firewall. An external firewall is placed at the edge of a local or enterprise network, just inside the boundary router that connects to the Internet or some wide area network (WAN). One or more internal firewalls protect the bulk of the enterprise network. Between these two types of firewalls are one or more networked devices in a region referred to as a DMZ (demilitarized zone) network. Systems that are externally accessible but need some protections are usually located on DMZ networks. Typically, the systems in the DMZ require or foster external connectivity, such as a corporate Web site, an e-mail server, or a DNS (domain name system) server


Internet
Boundary router
External firewall
LAN switch
Internal firewall
LAN switch
Internal DMZ network
Web server(s)
Email server
DNS server
Internal protected network
Application and database servers
Workstations

Unit 5 -Intrusion Detection System (IDS)

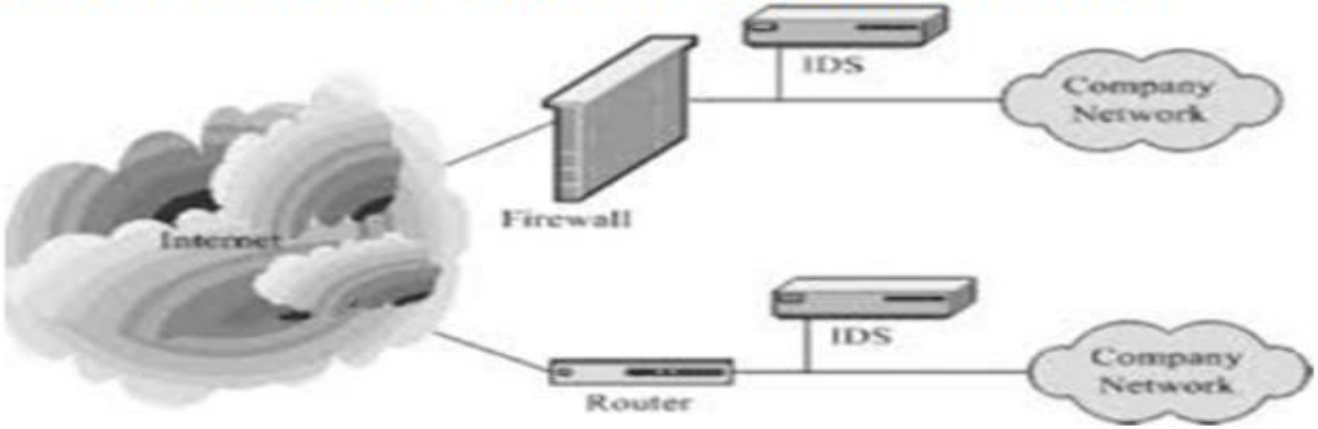


Prepared By Dr. B. H. Barhate

Intrusion Detection System (IDS)

What is IDS?

- IDS are tools for obtaining security in networks.
- It helps the administrator to detect & respond to the malicious attacks which the firewall was not able to detect & filter.



- An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities.

- An Intrusion Detection System is required to detect all types of malicious network traffic and computer usage that can't be detected by a conventional firewall.

  - This includes network attacks against services, attacks on applications, unauthorized logins and access to sensitive files etc...
  - IDS thus forms the second line of defence against malicious hacker & attackers.

Intrusion Detection System (IDS)

An **Intrusion Detection System (IDS)** is a system that monitors **network traffic** for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a **S**ecurity **I**nformation and **E**vent **M**anagement (SIEM) system. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms

Although intrusion detection systems monitor networks for potentially malicious activity, they are also disposed to false alarms. Hence, organizations need to fine-tune their IDS products when they first install them. It means properly setting up the intrusion detection systems to recognize what normal traffic on the network looks like as compared to malicious activity.

Intrusion prevention systems also monitor network packets inbound the system to check the malicious activities involved in it and at once sends the warning notifications.

IDS TYPES

(I) NIDS

→ Network Based

→ Analysis: Matches traffic to the library of known attack.

→ Monitors, Capture & Analyze network traffic.

→ Detect malicious data present into packets.

→ NIDS Analysis very difficult in busy n/w.

(II) HIDS

→ Host Based

→ installed on individual host or device on network.

→ It monitor data packets from the device only and will alert the admin if suspicious activity is detected

→ Snapshot

Existing system ⇌ Previous system

→ files deleted or modifi

Limitations

- avoiding an IDS is a first priority for successful attackers.
- An IDS that is not well defended is useless.
- Similar IDS have identical vulnerabilities so
  - there selection criteria will miss similar attack.
- IDS is sensitive
  - Which is difficult to measure and adjust.
- An IDS does not run itself.
- **General:**
- IDS ARE EXCELLENT ADDITION TO NETWORK SECURITY

- IDS is unable to catch the events of tear drop attack.
- A tear drop attack occurs when an attack sends fragments of data that a system is unable to reassemble.
- Such an attack may lead to freezing of the system.

- Most of them are unable to detect & prevent the misuse or unintended consequences.
- A direct attack on IDS by an attacker also finishes up its ability to detect intrusion. So the attacker tries to shut down the IDS & then attack on network.
- Not all IDS are compatible with all routers.

Host based ID system (HIDS)

- These are concerned with what is happening on each individual computer or host .
- They are able to detect such things such as repeated failed access attempts or changes to system files.
- HIDS are installed on hosts to which they have to keep an eye & perform monitoring.
- Host can be server, workstation or any network device such as router, printer or gateway.
- HIDS do monitoring, reporting & direct interactions at application layer.
- It can inspect each incoming command, look for signs of maliciousness & unauthorized file changes.

- The disadvantage of Host based IDS is: they are harder to manage, as information must be configured & managed for every host monitored.
- Most of the HIDS can monitor only specific types of systems E.g. the HIDS cyber cop server can only protect web servers.
- If the server is running multiple services like file sharing, DNS etc then HIDS might not be able to detect an intrusion.

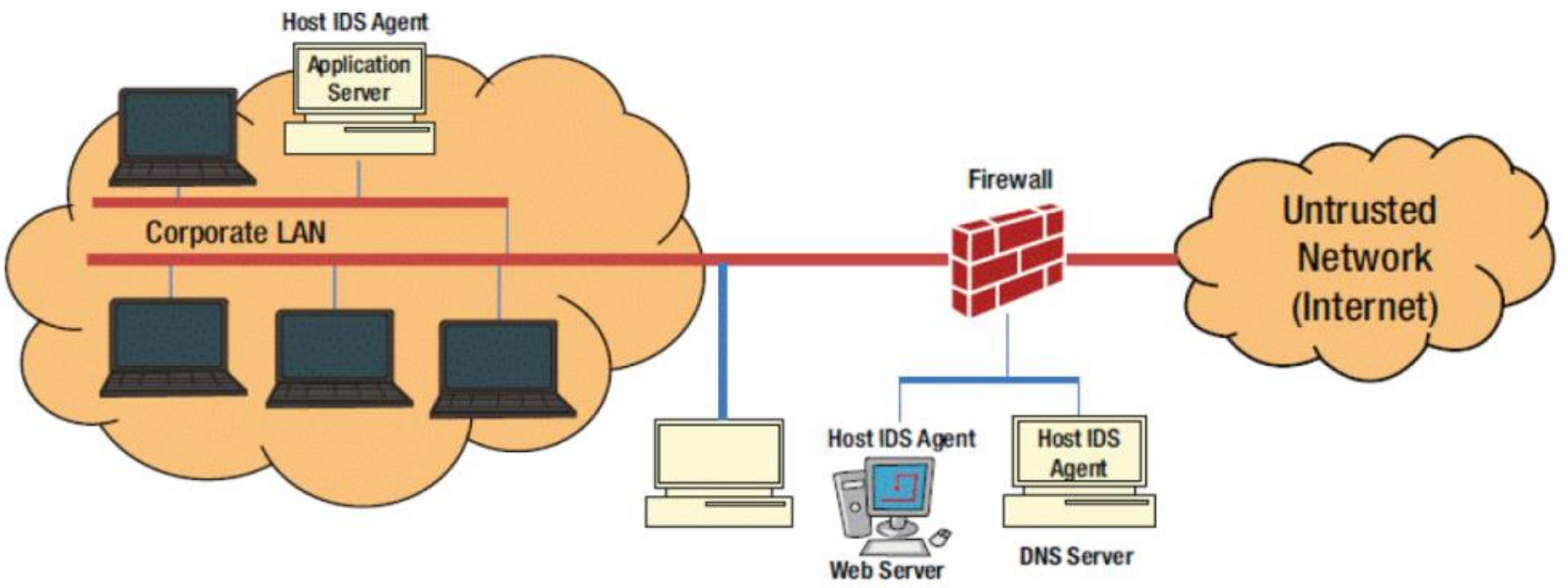
Teardrop attack

- A teardrop attack is a denial of service attack (DoS).
- This attack causes fragmented packets to overlap one another on the host receipt, the host attempts to reconstruct them during the process but fails.

1 Teardrop Attack (Dos Attack)
2 A teardrop attack is a denial-of-service (DoS) attack that involves sending fragmented packets to a target machine. Since the machine receiving such packets cannot reassemble them due to a bug in TCP/IP fragmentation reassembly, the packets overlap one another, crashing the target network device. This generally happens on older operating systems such as Windows 3.1x, Windows 95, Windows NT and versions of the Linux kernel 2.1.63.
3
4 Kali Linux 2018| IP:192.168.28.146 | (Hacker Machine)
5 MS Windows 95 | IP:192.168.28.149 | (Victim Machine)

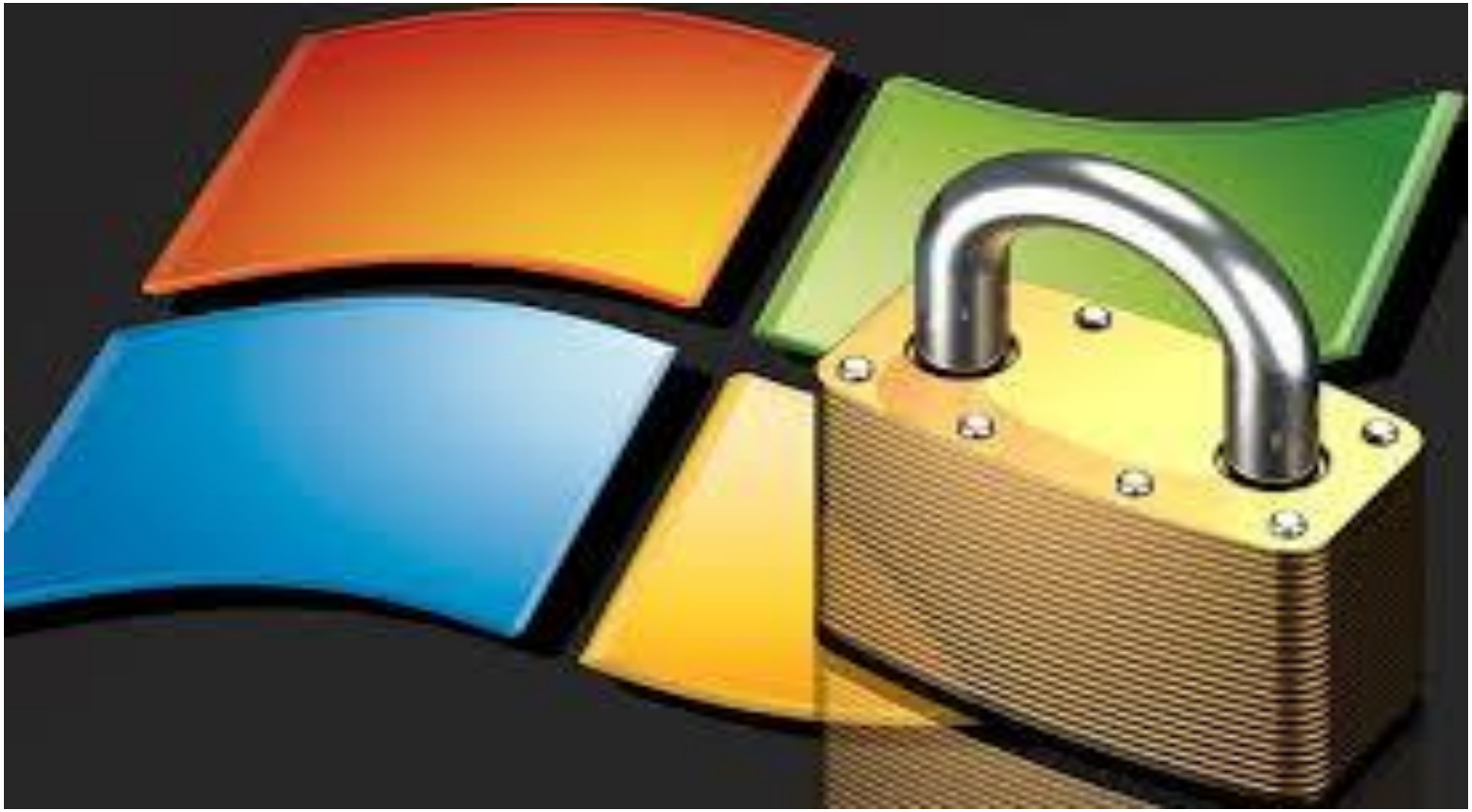
Host Based IDS Set up

Host-based Intrusion Detection System refers to the detection of intrusion on a single system. This is normally a software-based deployment where an agent, as shown in Figure , is installed on the local host that monitors and reports the application activity. HIDS monitors the access to the system and its application and sends alerts for any unusual activities. It constantly monitors event logs, system logs, application logs, user policy enforcement, root kit detection, file integrity, and other intrusions to the system. It constantly monitors these logs and creates a baseline. If any new log entries appear, HIDS checks the data against the baseline and if any entries are found outside of this baseline, HIDS triggers an alert. If any unauthorized activity is detected, HIDS can alert the user or block the activity or perform any other decision based on the policy that is configured on the system.



A host-based **intrusion detection system** (HIDS) is additional software installed on a system such as a workstation or a server.
It provides protection to the individual host and can detect potential attacks and protect critical operating system files. The primary goal of any IDS is to monitor traffic. The role of a host Intrusion Detection System is passive, only gathering, identifying, logging, and alerting. Examples of HIDS:

Unit 6 – System Security



Prepared By Dr. B. H. Barhate

Operating System Hardening

Operating system hardening includes configuring log files and auditing, changing default administrator account names and default passwords, and the institution of account lockout and password policies to guarantee strong passwords that can resist brute-force attacks. File-level security and access control mechanisms serve to isolate access attempts within the operating system environment.

Disabling Unnecessary Services

Some of the more attack-prone services include IIS, FTP, and other common web technologies. Make sure these services are disabled if they aren't needed, and keep them up-to-date with the most recent security and service packs.

Here are some tips:

- File and Print Servers
  - Vulnerable to DoS and access attacks. Make sure these servers run only the protocols needed to support the network.
- Networks with PC-Based Systems
  - Make sure NetBIOS services are disabled (ports 135, 137, 138, and 139) on servers or that an effective firewall is in place between the server and the Internet. On Unix, disable port 111, the Remote Procedure Call.
- Directory Sharing
  - Limit directory sharing to what is essential. Make sure root directories are hidden from browsing. Do not share the root directory.
- Root Directories
  - If an attacker penetrates the root directory, all the subdirectories under that directory are vulnerable.

Password Protection

Passwords should always be as long and as complicated as possible. Most vendors recommend that you use nonalphabetic characters such as #, $, and % in your password, and some go so far as to require it.

Disabling Unnecessary Accounts

Enabled accounts that are not needed on a system provide a door in which attackers can gain access. You should disable all accounts that are not needed immediately, on servers and workstations. Following are some types of accounts you should disable:

- Employees who have left the company
- Temporary employees
- Default Guest account – a likely target for hackers.

General steps for securing windows operating system

1. Keep your Windows operating system up to date

Probably the most important step to do is checking for the latest security updates and patches available for your Windows operating system.

To get the security updates automatically, go to “Control Panel” and check if your automatic updating system is enabled or follow these steps:

- Access the search box in your Windows operating system, type Windows Update.
- Select Advanced options.
- Click on Automatically download updates in case it is not already selected/turned on.

After checking for available updates for your Windows operating system, keep the automatic update turned on in order to download and install the important updates that can help protect your PC against new viruses or next-generation malware

2. Create a Restore point

If you already installed the security updates for Windows OS, the next step recommended is to create a **restore point in Windows**.

You can do this by clicking on the **Start** button, then select **Control Panel -> System and Maintenance** (or **System and Security**) -> **System**. Then select **System protection** and click the **Create** button.

After installing Windows, you can create the **Restore Point** and name it **Clean installation,** and continue installing drivers and applications.

If one of the drivers causes issues on the system, you can always go back to the **Clean installation** restore point.

3. Install a traditional antivirus product

Install and use antivirus software. It is important to have a reliable security solution on your system, which should include real-time scanning, automatic update, and a firewall.

4. Back up your system

It may creates some hardware issues due to this it may creates problem to the data or operating system. To make sure your data stays safe, you should be using a *twofold strategy*, which should include combining an external hard drive usage with an online backup service.

At the same time, you could simply use your Windows Backup system. To set it up, access your Windows Control Panel and then click Backup and Restore to access the location. From this place, you can set an automatic backup, create a schedule and even choose a network location for your backup files.

5. Enable User Account Control:

Make sure all local accounts including the built-in local administrator or owner account have strong passwords. A strong password will be 6 or more characters in length, contain numbers and letters as well as special characters, and not are found in a dictionary.

6. Automatic Patches Updating:

Apply all current patches via Windows Update. It may be necessary to reboot the computer several times during this process. You should repeat this step as needed until there are no more critical or recommended patches that need to be applied

Hardening Unix/Linux based operating system

1. *Install security updates and patches*
2. Use strong passwords
3. *Implement a firewall*
4. *Keep things clean*
5. Secure configurations
6. *Limited access to users*
7. Monitor your systems
8. Create backups
9. Perform system auditing

Patch

A patch is a software update comprised code inserted (or patched) into the code of an executable program. Typically, a patch is installed into an existing software program. Patches are often temporary fixes between full releases of a software package.

Patches may do any of the following:

- Fix a software bug
- Install new drivers
- Address new security vulnerabilities
- Address software stability issues
- Upgrade the software

Software patches can be free or available for sale. Some companies deliver patches to registered users only. Patches are usually available as Internet downloads.

Service Pack

A service pack is a software package that contains several updates for an application or operating system. Individual updates are typically called software updates or patches. When a software company has developed several updates to a certain program or operating system, the company may release all the updates together in a service pack.

Many Windows users are familiar with service packs because of the popular service pack released for Windows XP, called SP2. Windows XP SP2 not only included typical updates such as bug fixes and security updates, it added new features.