Unit – I

Planning for Security: In the security planning process, the organization identifies which assets require protection and the types of risks that could compromise those assets. This critical function determines the level of appropriate countermeasure that is required based upon a formally documented process. Risks are usually categorized into three categories:

1.People—Human resources are usually the most critical asset within any organization, and as such, must receive a stronger consideration when assessing risk.

2.Property—Physical property or intellectual assets.

3.Legal liability—Legal risks can also affect people and property, but need to be considered as a separate category. This is due, in part, to the extent which lawsuits affect the security industry these days.

Additionally, the security planning process should determine the probability of such occurrences and the impact on the organization if loss should ever occur. These steps are critical to determine how to best protect organizational assets and must be performed periodically. An added benefit of the security planning process is the potential for increased security awareness throughout every level of the organization.
The security planning process consists of the following five steps:

1.Assets are identified.
2.Loss events are exposed.
3.Occurrence probability factors are assigned.
4.Impact of occurrence is assessed.
5.Countermeasures are selected.

Introduction, Information Security Policy

What is a security policy?

A security policy (also called an information security policy or IT security policy) is a document that spells out the rules, expectations, and overall approach that an organization uses to maintain the confidentiality, integrity, and availability of its data. Security policies exist at many different levels, from high-level constructs that describe an enterprise's general security goals and principles to documents addressing specific issues, such as remote access or Wi-Fi use.

A security policy is frequently used in conjunction with other types of documentation such as standard operating procedures. These documents work together to help the company achieve its security goals. The policy defines the overall strategy and security stance, with the other documents helping build structure around that practice. You can think of a security policy as answering the "what" and "why," while procedures, standards, and guidelines answer the "how."

Four reasons a security policy is important

Security policies may seem like just another layer of bureaucracy, but in truth, they are a vitally important component in any information security program. Some of the benefits of a well-designed and implemented security policy include:

1. Guides the implementation of technical controls

A security policy doesn't provide specific low-level technical guidance, but it does spell out the intentions and expectations of senior management in regard to security. It's then up to the security or IT teams to translate these intentions into specific technical actions.

For example, a policy might state that only authorized users should be granted access to proprietary company information. The specific authentication systems and access control rules used to implement this policy can change over time, but the general intent remains the same. Without a place to start from, the security or IT teams can only guess senior management's desires. This can lead to inconsistent application of security controls across different groups and business entities.

2. Sets clear expectations

Without a security policy, each employee or user will be left to his or her own judgment in deciding what's appropriate and what's not. This can lead to disaster when different employees apply different standards.

Is it appropriate to use a company device for personal use? Can a manager share passwords with their direct reports for the sake of convenience? What about installing unapproved software? Without clear policies, different employees might answer these questions in different ways. A security policy should also clearly spell out how compliance is monitored and enforced.

3. Helps meet regulatory and compliance requirements

Documented security policies are a requirement of legislation like HIPAA and Sarbanes-Oxley, as well as regulations and standards like PCI-DSS, ISO 27001, and SOC2. Even when not explicitly required, a security policy is often a practical necessity in crafting a strategy to meet increasingly stringent security and data privacy requirements.

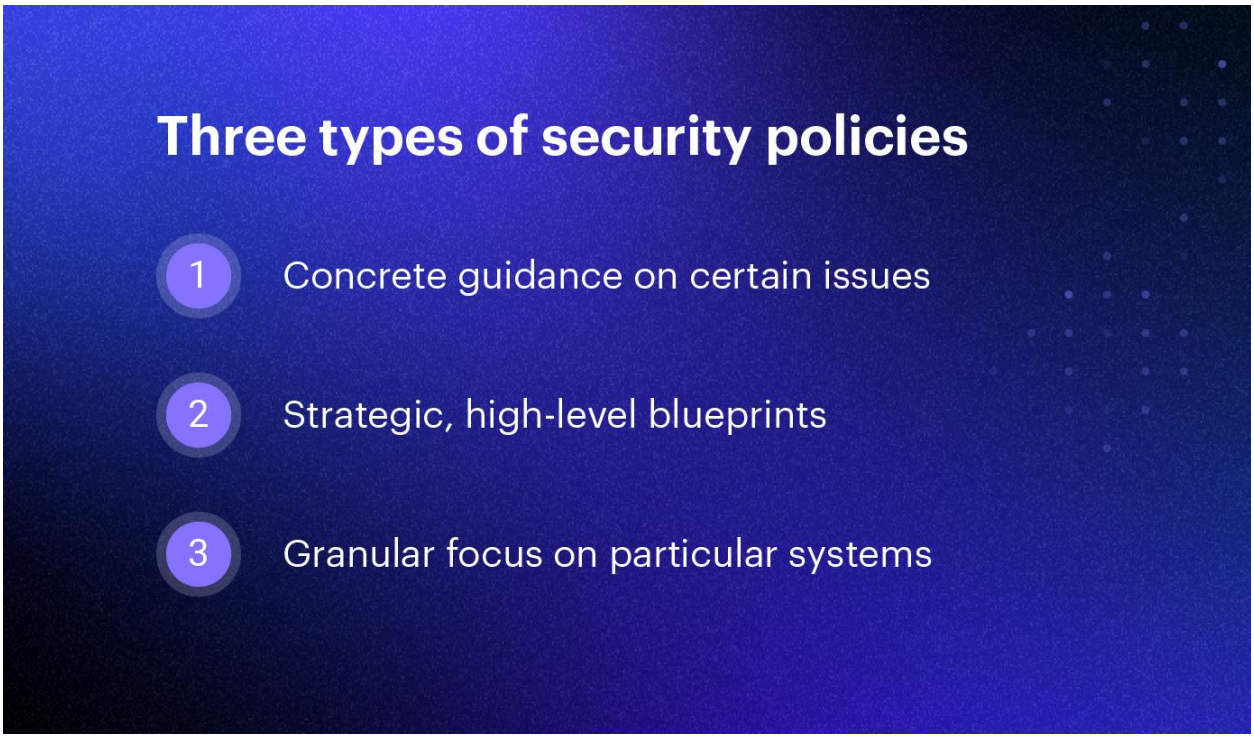
4. Improves organizational efficiency and helps meet business objectives

A good security policy can enhance an organization's efficiency. Its policies get everyone on the same page, avoid duplication of effort, and provide consistency in monitoring and enforcing

compliance. Security policies should also provide clear guidance for when policy exceptions are granted, and by whom.

To achieve these benefits, in addition to being implemented and followed, the policy will also need to be aligned with the business goals and culture of the organization.

Three types of security policies



Security policies can vary in scope, applicability, and complexity, according to the needs of different organizations. While there's no universal model for security policies, the National Institutes of Standards and Technology (NIST) spells out three distinct types in Special Publication (SP) 800-12:

1. Program policy

Program policies are strategic, high-level blueprints that guide an organization's information security program. They spell out the purpose and scope of the program, as well as define roles and responsibilities and compliance mechanisms. Also known as master or organizational policies, these documents are crafted with high levels of input from senior management and are typically technology agnostic. They are the least frequently updated type of policy, as they should be written at a high enough level to remain relevant even through technical and organizational changes.

2. Issue-specific policy

Issue-specific policies build upon the generic security policy and provide more concrete guidance on certain issues relevant to an organization's workforce. Common examples could include a

network security policy, bring-your-own-device (BYOD) policy, social media policy, or remote work policy. These may address specific technology areas but are usually more generic. A remote access policy might state that offsite access is only possible through a company-approved and supported VPN, but that policy probably won't name a specific VPN client. This way, the company can change vendors without major updates.

3. System-specific policy

A system-specific policy is the most granular type of IT security policy, focusing on a particular type of system, such as a firewall or web server, or even an individual computer. In contrast to the issue-specific policies, system-specific policies may be most relevant to the technical personnel that maintains them. NIST states that system-specific policies should consist of both a security objective and operational rules. IT and security teams are heavily involved in the creation, implementation, and enforcement of system-specific policies but the key decisions and rules are still made by senior management.

Information Security Standards and Practices:

A security standard is "a published specification that establishes a common language, and contains a technical specification or other precise criteria and is designed to be used consistently, as a rule, a guideline, or a definition." The goal of security standards is to improve the security of information technology (IT) systems, networks, and critical infrastructures. The Well-Written cybersecurity standards enable consistency among product developers and serve as a reliable standard for purchasing security products.

Security standards are generally provided for all organizations regardless of their size or the industry and sector in which they operate. This section includes information about each standard that is usually recognized as an essential component of any cybersecurity strategy.

1. ISO

ISO stands for International Organization for Standardization. International Standards make things to work. These standards provide a world-class specification for products, services and computers, to ensure quality, safety and efficiency. They are instrumental in facilitating international trade.

ISO standard is officially established On 23 February 1947. It is an independent, non-governmental international organization. Today, it has a membership of 162 national standards bodies and 784 technical committees and subcommittees to take care of standards development. ISO has published over 22336 International Standards and its related documents which covers almost every industry, from information technology, to food safety, to agriculture and healthcare.

ISO 27000 Series

It is the family of information security standards which is developed by the International Organization for Standardization and the International Electrotechnical Commission to provide a globally recognized framework for best information security management. It helps the organization to keep their information assets secure such as employee details, financial information, and intellectual property.

The need of ISO 27000 series arises because of the risk of cyber-attacks which the organization face. The cyber-attacks are growing day by day making hackers a constant threat to any industry that uses technology.

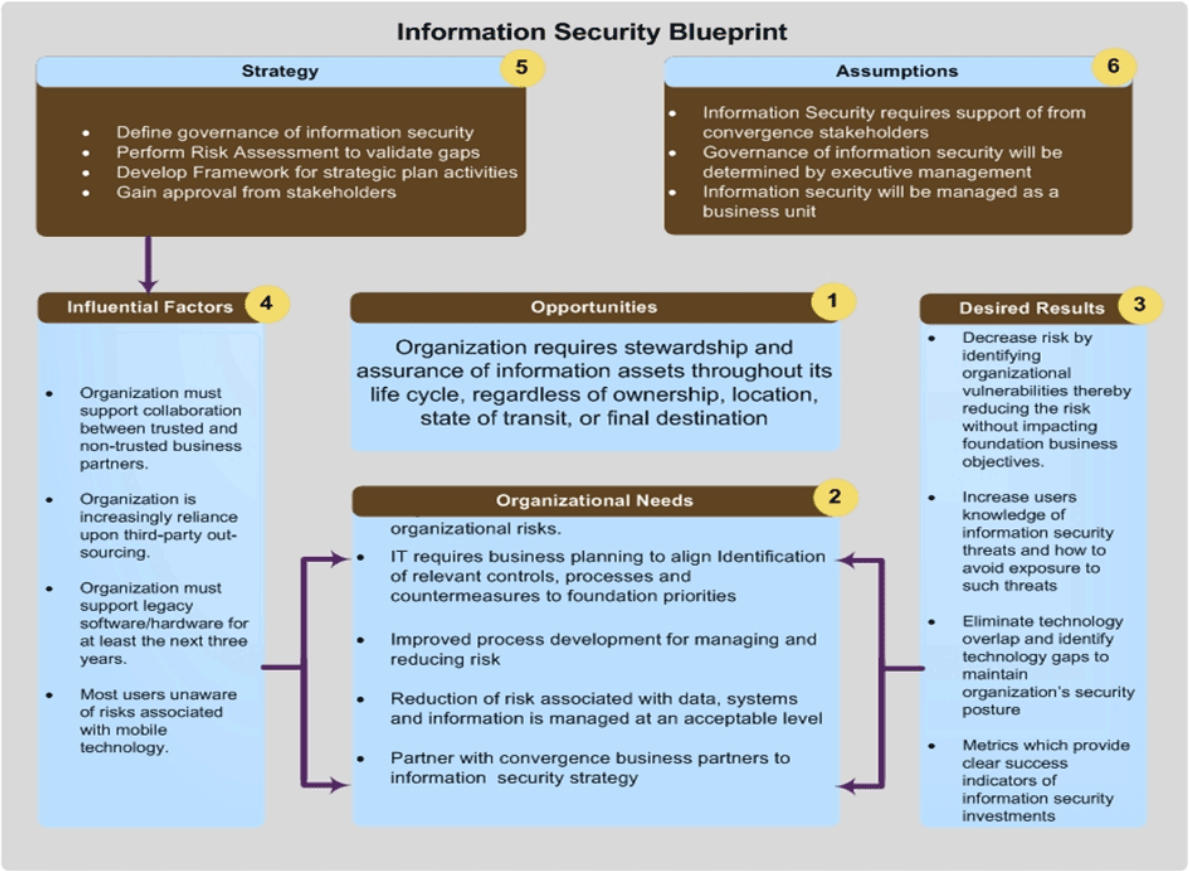
The ISO 27000 series can be categorized into many types. They are-

ISO 27001- This standard allows us to prove the clients and stakeholders of any organization to managing the best security of their confidential data and information. This standard involves a process-based approach for establishing, implementing, operating, monitoring, maintaining, and improving our ISMS.

ISO 27000- This standard provides an explanation of terminologies used in ISO 27001.

The Information Security Blue Print:

The goal of an information security blueprint is to gather an organization's requirements, provide a visualization of those requirements and initiate the process of interweaving information security as part of the organization's culture. The blueprint explains an organization's needs, desired results, factors that could influence the outcome and a strategy to execute.



Contingency plans and a model for contingency plan:

What Is a Contingency?

A contingency is a potential occurrence of a negative event in the future, such as an economic recession, natural disaster, fraudulent activity, terrorist attack, or a pandemic.

Although contingencies can be prepared for, the nature and scope of such negative events are typically unknowable in advance. Companies and investors plan for various contingencies through analysis and implementing protective measures.

In finance, managers often attempt to identify and plan using predictive models for possible contingencies that they believe may occur. Financial managers tend to err on the conservative side to mitigate risk, assuming slightly worse-than-expected outcomes.

A contingency plan might include arranging a company's affairs so that it can weather negative outcomes with the least distress possible.

KEY TAKEAWAYS

- A contingency is a potentially negative event that may occur in the future, such as an economic recession, natural disaster, or fraudulent activity.
- Companies and investors plan for various contingencies through analysis and implementing protective measures.
- A thorough contingency plan minimizes loss and damage caused by an unforeseen negative event.
- Contingency plans can include the purchase of options or insurance for investment portfolios.
- Banks must set aside a percentage of capital for negative contingencies, such as a recession, to protect the bank against losses.

How a Contingency Works

To plan for contingencies, financial managers may often also recommend setting aside significant reserves of cash so that the company has strong liquidity, even if it meets with a period of poor sales or unexpected expenses.

Managers may seek to proactively open credit lines while a company is in a strong financial position to ensure access to borrowing in less favorable times. For example, pending litigation would be considered a contingent liability. Contingency plans typically include insurance policies that cover losses that may arise during and after a negative event.

Types of Contingency Plans

Contingency plans are utilized by corporations, governments, investors, and central banks, such as the Fed. Contingencies can involve real estate transactions, commodities, investments, currency exchange rates, and geopolitical risks.

Protecting Assets

Contingencies might also include contingent assets, which are benefits (rather than losses) that accrue to a company or individual given the resolution of some uncertain event in the future. A favorable ruling in a lawsuit or an inheritance would be an example of contingent assets.

Contingency plans might involve purchasing insurance policies that pay cash or a benefit if a particular contingency occurs. For example, property insurance might be purchased to protect against fire or wind damage.

Security Technology: Introduction; Physical designs:

Security Technology

1. What is Security?

quality or state of being secure—to be free from danger”

·A successful organization should have multiple layers of security in place:

Physical security

Personal security

Operations security

Communications security

Network security

Information security

Physical Design

Physical design of an information security program is made up of two parts:

Security technologies

Physical security

Physical design process:

·- Identifies complete technical solutions based on these technologies (deployment, operations and maintenance elements)

·- Design physical security measures to support the technical solution.

·2. Firewalls

A software or hardware component that restricts network communication between two computers or networks.

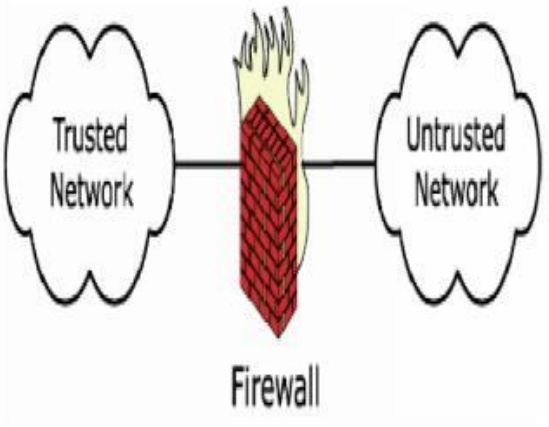
·- In buildings, a firewall is a fireproof wall that restricts the spread of a fire.

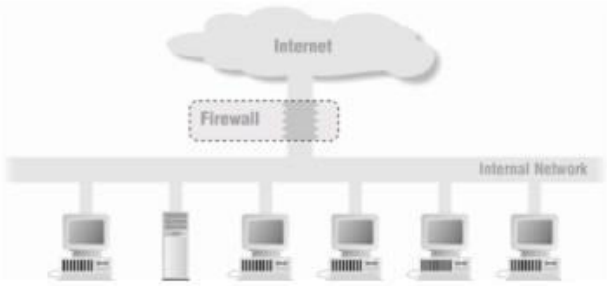
- Network firewall prevents threats from spreading from one network to another

·Prevent specific types of information from moving between the outside world (untrusted networks) and the inside world (trusted networks)

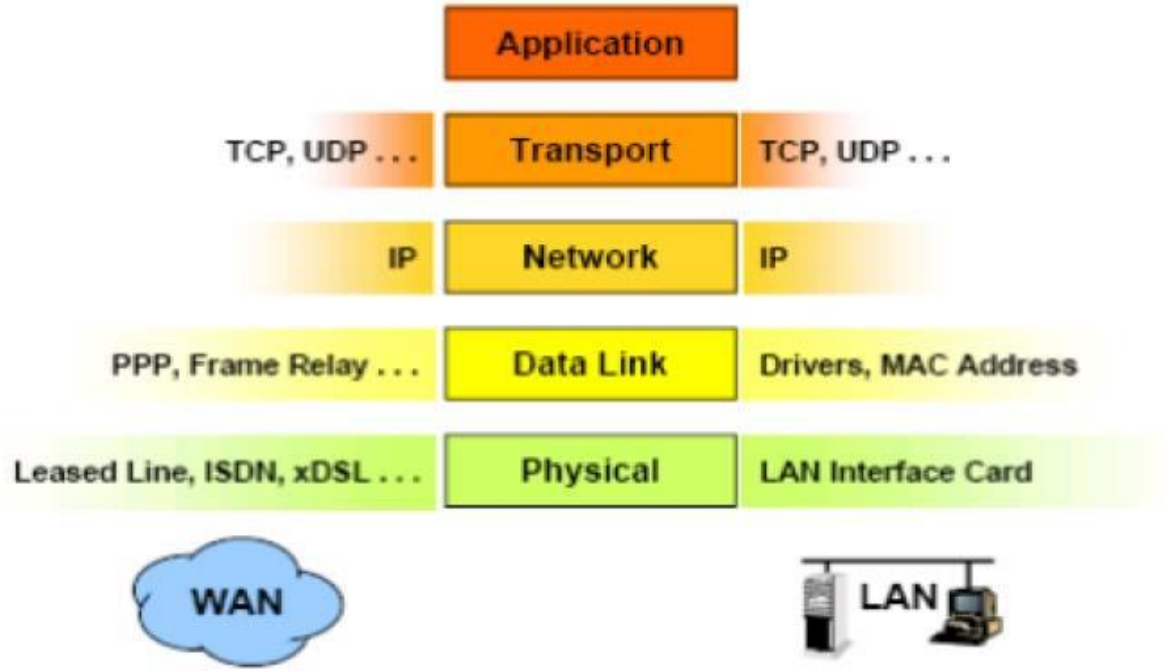
✓·The firewall may be a separate computer system, a software servic e running on an·existing router all serve r, or a separate network containing a number of supporting devices.

Internet Firewalls





The Internet Protocol Stack



1 What Firewalls do

Protects the resources of an internal network.

Restrict external access.

Log Network activities.

Intrusion detection

DoS

Act as intermediary

Centralized Security Management

Carefully administer one firewall to control internet traffic of many machines.

Internal machines can be administered with less care.

2 Types of Firewalls (General)

Firewalls types can be categorized depending on:

·The Function or methodology the firewall use

Whether the communication is being done between a single node and the network, or between two or more networks.

Whether the communication state is being tracked at the firewall or not.

With regard to the scope of filtered communications the done between a single node and the network, or between two or more networks there exist :

·Personal Firewalls, a software application which normally filters traffic entering or leaving a single computer.

Network firewalls, normally running on a dedicated network device or computer positioned on the boundary of two or more networks.

3 Firewall categorization methods

The Function or methodology the firewall use

Five processing modes that firewalls can be categorized by are :

- packet filtering
- application gateways
- circuit gateways
- MAC layer firewalls
- hybrids

3.1.Packet filtering:

examine the header information of data packets that come into a network.

·a packet filtering firewall installed on TCP/IP based network and determine wether to drop a packet or forward it to the next network connection based on the rules programmed in the firewall.

·Packet filtering firewalls scan network data packets looking for violation of the rules of the firewalls database.

·Filtering firewall inspect packets on at the network layers.

·If the device finds a packet that matches a restriction it stops the packet from traveling from network to another.

·filters packet-by-packet, decides to *Accept/Deny/Discard* packet based on certain/configurable criteria – *Filter Rule sets*.

·Typically stateless: do not keep a table of the connection *state* of the various traffic that flows through them

·Not dynamic enough to be considered true firewalls.

Usually located at the boundary of a network.

Their main strength points: ***Speed*** and ***Flexibility***.

There are three subsets of packet filtering firewalls:

static filtering

dynamic filtering

stateful inspection

static filtering:

requires that the filtering rules coverning how the firewall decides which packets are allowed and which are denied.

✓·This type of filtering is common in network routers and gateways.

2. Dynamic filtering

allows the firewall to create rules to deal with event.

This reaction could be positive as in allowing an internal user to engage in a specific activity upon request or negative as in dropping all packets from a particular address

3. Stateful inspection

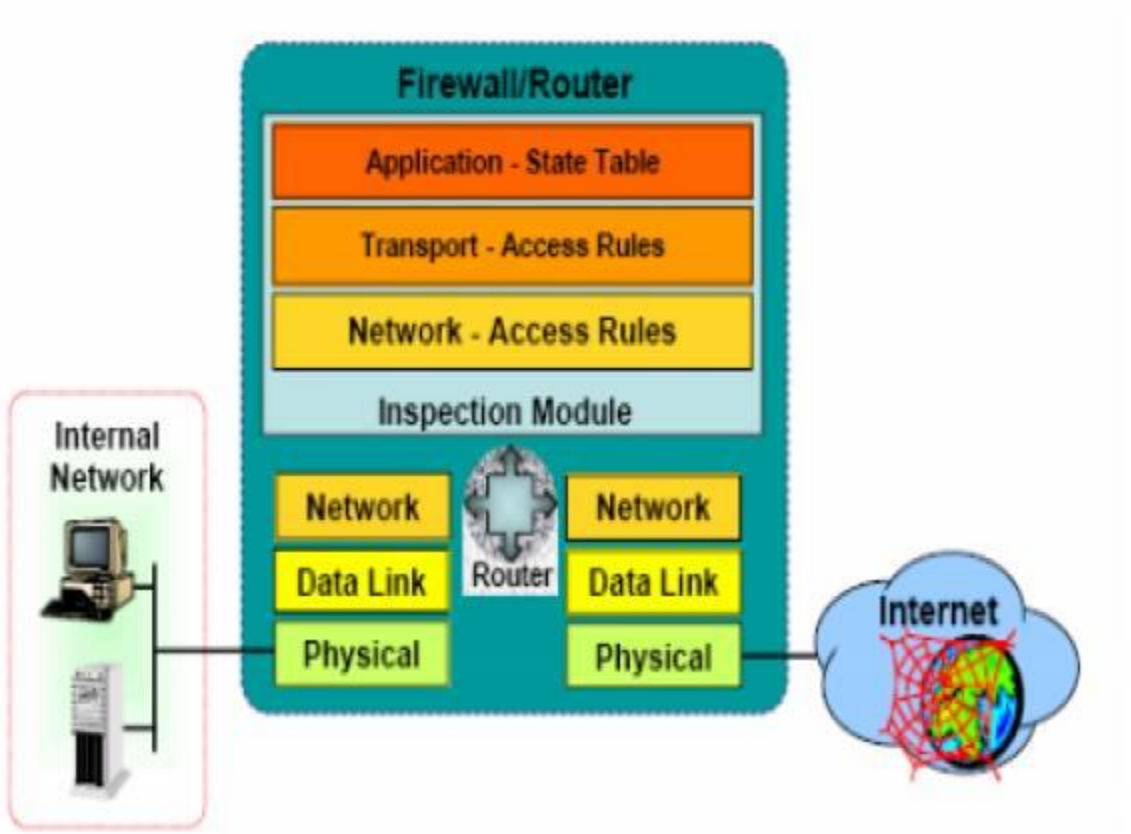
keep track of each network connection between internal and external systems using a state table.

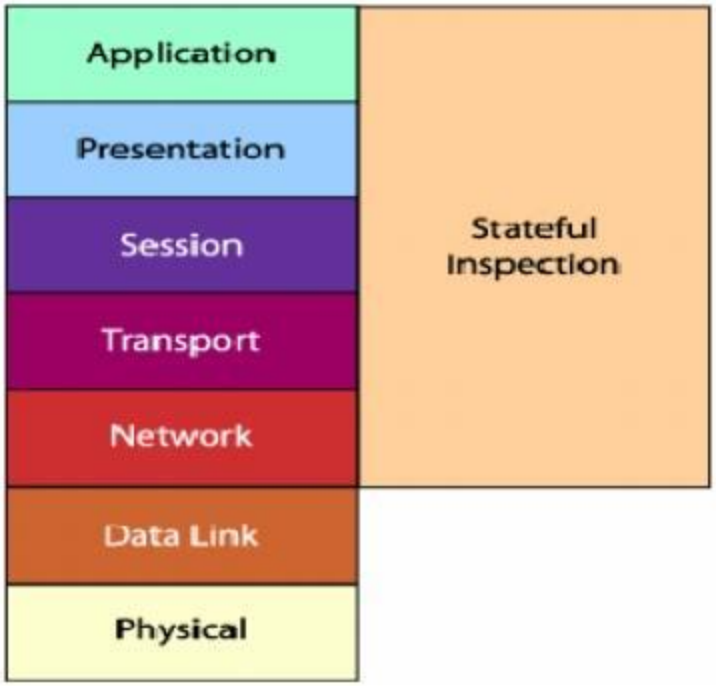
·A state table tracks the state and context of each packet in the conversation by recording which station send , what packet and when.

·More complex than their constituent component firewalls

·Nearly all modern firewalls in the market today are staful

Stateful Inspection Firewalls


Firewall/Router
Application - State Table
Transport - Access Rules
Network - Access Rules
Inspection Module
Internal Network
Network
Data Link
Physical
Router
Network
Data Link
Physical
Internet



Basic Weaknesses Associated w ith Packet Filters\ Statful

They cannot pre vent attacks that employ application-specific vulnerabilities or functions.

Logging function ality present in packet filter firewalls is limited

-Most packet filter firewalls do not support advanced user authent ication schemes.

Vulnerable to attacks and exploits that take advantage of pro blems within the TCP/IP specification and protocol stack, such as network layer ad dress spoofing.

Susceptible to sec urity breaches caused by improper configurations.

Advantages:

One packet filter can protect an entire network

Efficient (require s little CPU)

Supported by mosst routers

Disadvantages:

Difficult to config ure correctly

Must consider rule set in its entirety

Difficult to test co mpletely

Performance penalty for complex rulesets

Stateful packet filtering much more expensive

.

Enforces ACLs at layer 3 + 4, without knowing any application details

Packet Filtering Firewalls

The original firewall

.

Works at the network level of the OSI

.

model

.

Applies packet filters based on access

- Rules:
- Source IP address

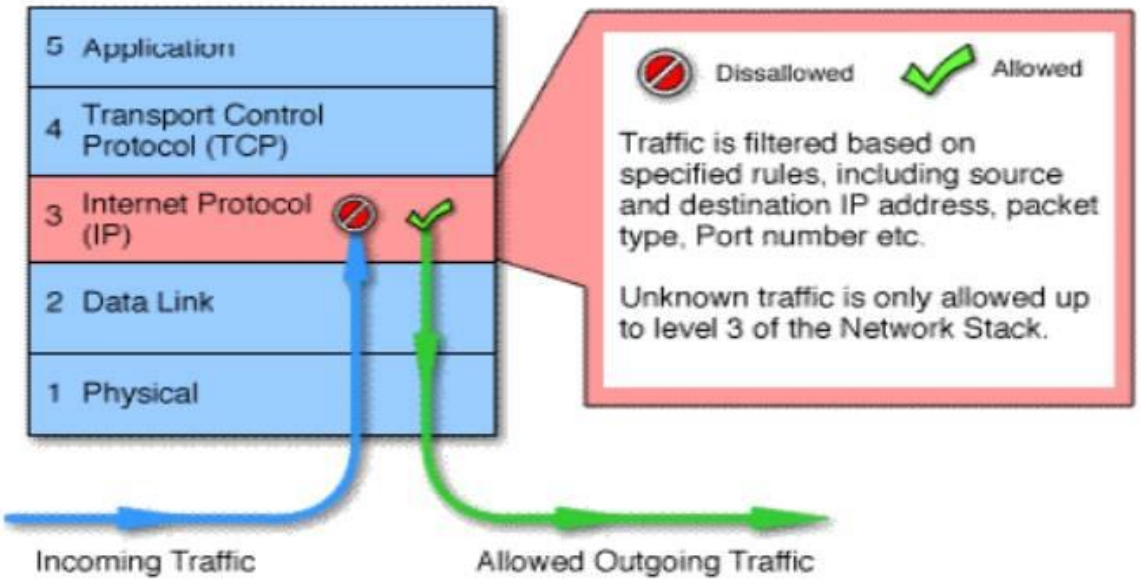
  Destination IP address

  Application or protocol

  Source port number

  Destination port number

Packet Filtering Firewalls



Application gateways:

is also known as proxy server since it runs special software that acts as a proxy for a service request.

One common example of proxy server is a firewall that blocks or requests for and responses to request for web pages and services from the internal computers of an organization.

The primary disadvantag e of application level firewalls is that they ar e designed for a specific protocols and c annot easily be reconfigured to protect against attacks in other protocols.

Application firewalls work at the application layer

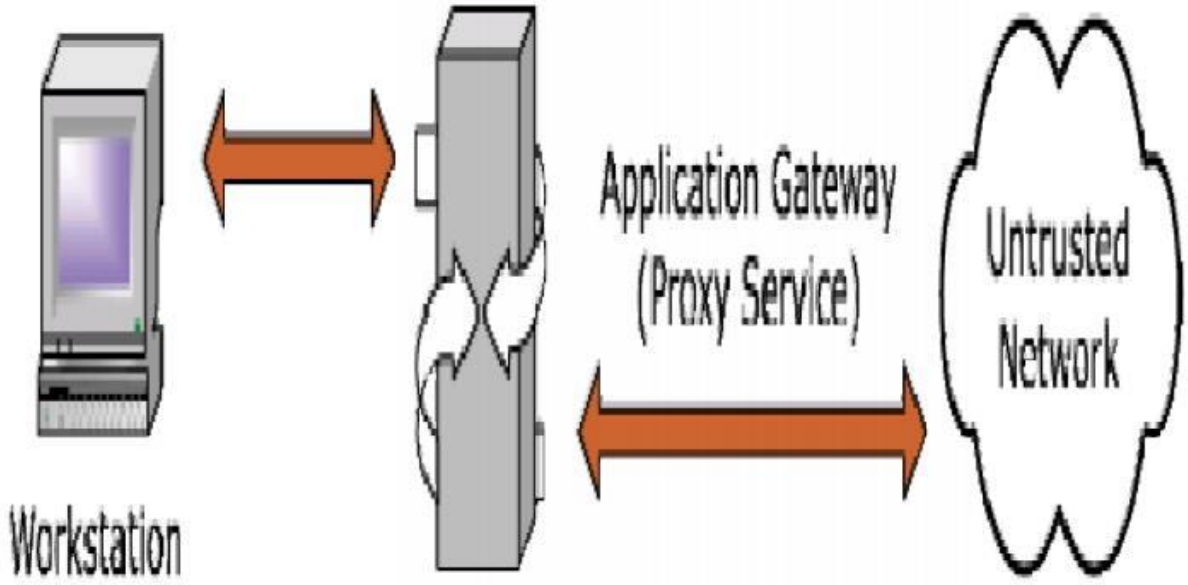
Filters packets on application data as well as on IP/TCP/UDP fields.

The interaction is controlled at the application layer

A proxy server is an application that mediates traffic between two network segments.

With the proxy acting a s mediator, the source and destination system s never actually “connect”.

Filtering Hostile Code: Proxies can analyze the payload of a packet o f data and make decision as to whether thiis packet should be passed or dropped.



4.Circuit gateways:

operates at the transport layer.

.

Connections are authorized based on addresses , they prevent direct connections between network and another.

.

They accomplish this prevention by creating channels connecting specific systems on each side of the firewall and then allow only authorized traffic.

.

relays two TCP connections (session layer)

.

imposes security by limiting which such connections are allowed

.

once created usually relays traffic without examining contents

.

Monitor handshaking between packets to decide whether the traffic is legitimate

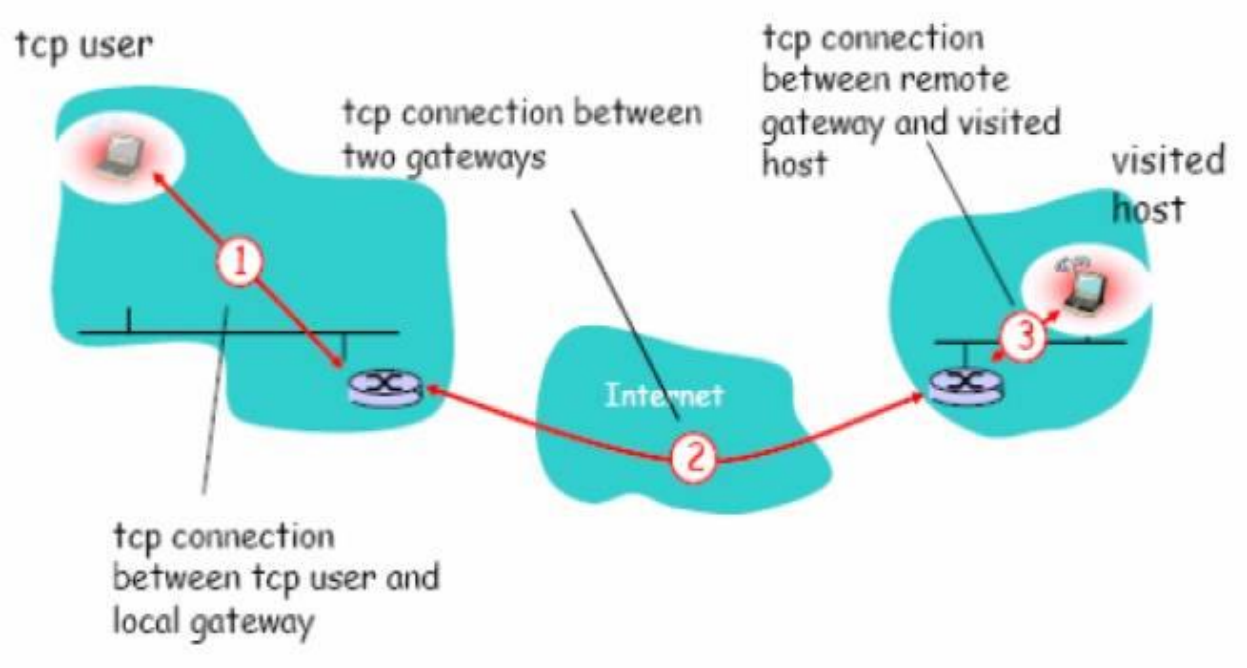
.

typically used when trust internal users by allowing general outbound connections

.

SOCKS commonly used for this

Circuit Level Firewalls Example



4.MAC layer firewalls:

✓·design to operate at the media access control layer.

Using this approach the MAC addresses of specific host computers are linked to ACL entries that identify the specific types of packets that can be send to each host and all other traffic is blocked.

5.Hybrids firewalls:

companied the elements of other types of firewalls , example the elements of packet filtering and proxy services, or a packet filtering and circuit gateways.

.

That means a hybrids firewalls may actually of two separate firewall devices; each is a separate firewall system, but they are connected so that they work together.

Types of Firewalls

Finally, Types depending on whether the firewalls keeps track of the state of network connections or treats each packet in isolation, two additional categories of firewalls exist:

- Stateful firewall
- Stateless firewall

Stateful firewall

keeps track of the state of network connections (such as TCP streams) traveling across it.

·Stateful firewall is able to hold in memory significant attributes of each connection, from start to finish. These attributes, which are collectively known as the state of the connection, may include such details as the IP addresses and ports involved in the connection and the sequence numbers of the packets traversing the connection.

Stateless firewall

Treats each network frame (Packet) in isolation. Such a firewall has no way of knowing if any given packet is part of an existing connection, is trying to establish a new connection, or is just a rogue packet.

- The classic example is the File Transfer Protocol, because by design it opens new connections to random ports.

Advantages of a Firewall

Stop incoming calls to insecure services

- such as rlogin and NFS
- Control access to other services
- Control the spread of viruses
- Cost Effective
- More secure than securing every
- system

Disadvantages of a Firewall

- Central point of attack
- Restrict legitimate use of the Internet
- Bottleneck for performance
- Does not protect the ‘back door’
- Cannot always protect against
- smuggling
-

Cannot prevent insider attacks.

Intrusion Detection System (IDS)

An Intrusion Detection System (IDS) maintains network traffic looks for unusual activity and sends alerts when it occurs. The main duties of an Intrusion Detection System (IDS) are anomaly detection and reporting; however, certain Intrusion Detection Systems can take action when malicious activity or unusual traffic is discovered. In this article, we will discuss every point about the Intrusion Detection System.

What is an Intrusion Detection System?

A system called an intrusion detection system (IDS) observes network traffic for malicious transactions and sends immediate alerts when it is observed. It is software that checks a network or system for malicious activities or policy violations. Each illegal activity or violation is often recorded either centrally using an SIEM system or notified to an administration. IDS monitors a network or system for malicious activity and protects a computer network from unauthorized access from users, including perhaps insiders. The intrusion detector learning task is to build a predictive model (i.e. a classifier) capable of distinguishing between 'bad connections' (intrusion/attacks) and 'good (normal) connections'.

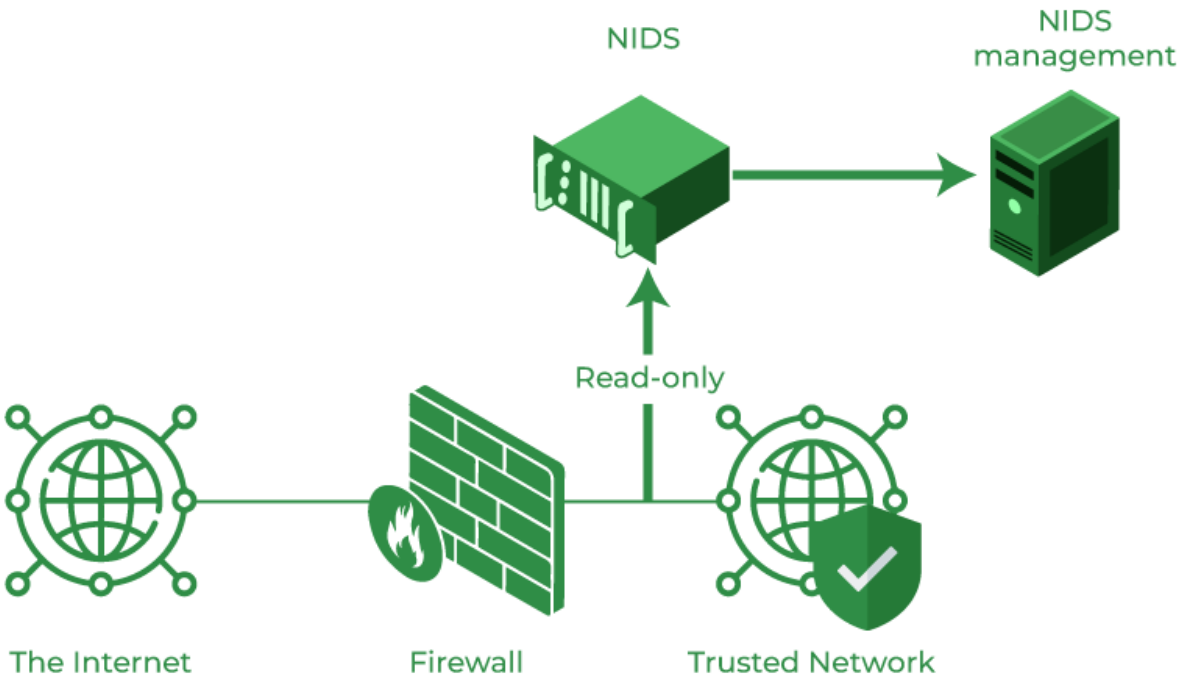
Working of Intrusion Detection System(IDS)

- An IDS (Intrusion Detection System) monitors the traffic on a computer network to detect any suspicious activity.
- It analyzes the data flowing through the network to look for patterns and signs of abnormal behavior.
- The IDS compares the network activity to a set of predefined rules and patterns to identify any activity that might indicate an attack or intrusion.
- If the IDS detects something that matches one of these rules or patterns, it sends an alert to the system administrator.
- The system administrator can then investigate the alert and take action to prevent any damage or further intrusion.

Classification of Intrusion Detection System(IDS)

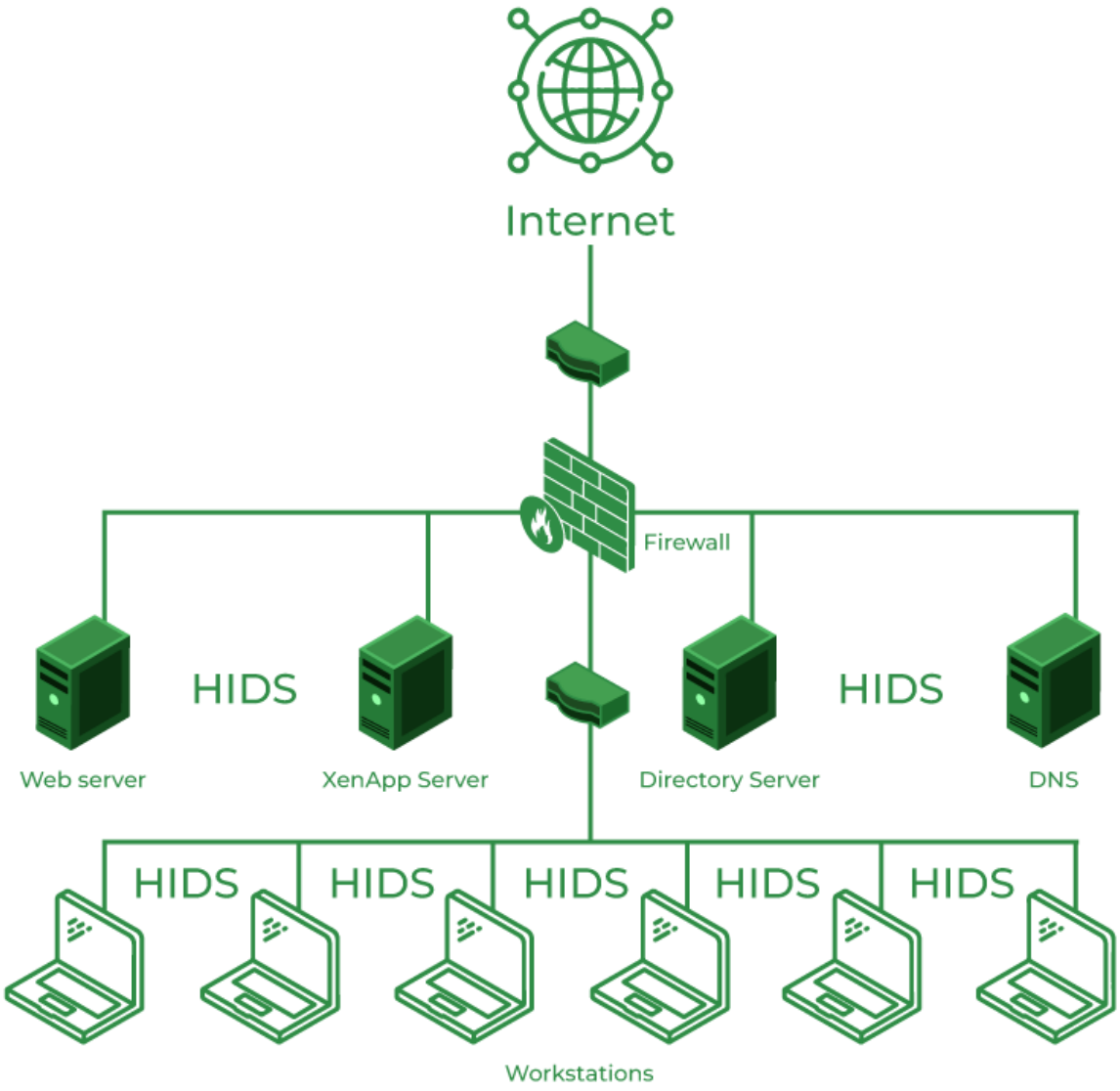
Intrusion Detection System are classified into 5 types:

- **Network Intrusion Detection System (NIDS):** Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator. An example of a NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying to crack the firewall.



Network Intrusion Detection System

- **Host Intrusion Detection System (HIDS):** Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission-critical machines, which are not expected to change their layout.



- **Protocol-based Intrusion Detection System (PIDS):** Protocol-based intrusion detection system (PIDS) comprises a system or agent that would consistently reside at the front end of a server, controlling and interpreting the protocol between a user/device and the server. It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accepting the related HTTP protocol. As HTTPS is unencrypted and before instantly entering its web presentation layer then this system would need to reside in this interface, between to use the HTTPS.
- **Application Protocol-based Intrusion Detection System (APIDS):** An application Protocol-based Intrusion Detection System (APIDS) is a system or agent that generally resides within a group of servers. It identifies the intrusions by monitoring and interpreting the communication on application-specific protocols. For example, this would monitor the SQL protocol explicitly to the middleware as it transacts with the database in the web server.

- **Hybrid Intrusion Detection System:** Hybrid intrusion detection system is made by the combination of two or more approaches to the intrusion detection system. In the hybrid intrusion detection system, the host agent or system data is combined with network information to develop a complete view of the network system. The hybrid intrusion detection system is more effective in comparison to the other intrusion detection system. Prelude is an example of Hybrid IDS.

Intrusion Detection System Evasion Techniques

- **Fragmentation:** Dividing the packet into smaller packet called fragment and the process is known as fragmentation. This makes it impossible to identify an intrusion because there can't be a malware signature.
- **Packet Encoding:** Encoding packets using methods like Base64 or hexadecimal can hide malicious content from signature-based IDS.
- **Traffic Obfuscation:** By making message more complicated to interpret, obfuscation can be utilised to hide an attack and avoid detection.
- **Encryption:** Several security features, such as data integrity, confidentiality, and data privacy, are provided by encryption. Unfortunately, security features are used by malware developers to hide attacks and avoid detection.

Benefits of IDS

- **Detects malicious activity:** IDS can detect any suspicious activities and alert the system administrator before any significant damage is done.
- **Improves network performance:** IDS can identify any performance issues on the network, which can be addressed to improve network performance.
- **Compliance requirements:** IDS can help in meeting compliance requirements by monitoring network activity and generating reports.
- **Provides insights:** IDS generates valuable insights into network traffic, which can be used to identify any weaknesses and improve network security.

Detection Method of IDS

- **Signature-based Method:** Signature-based IDS detects the attacks on the basis of the specific patterns such as the number of bytes or a number of 1s or the number of 0s in the network traffic. It also detects on the basis of the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures. Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in the system but it is quite difficult to detect new malware attacks as their pattern (signature) is not known.
- **Anomaly-based Method:** Anomaly-based IDS was introduced to detect unknown malware attacks as new malware is developed rapidly. In anomaly-based IDS there is the use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in the model. The machine learning-based method has a better-generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.

Comparison of IDS with Firewalls

IDS and firewall both are related to network security but an IDS differs from a firewall as a firewall looks outwardly for intrusions in order to stop them from happening. Firewalls restrict access between networks to prevent intrusion and if an attack is from inside the network it doesn't signal. An IDS describes a suspected intrusion once it has happened and then signals an alarm.

What is Honeypot?

Honeypot is a network-attached system used as **a trap for cyber-attackers** to detect and study the tricks and types of attacks used by hackers. It acts as a potential target on the internet and informs the defenders about any unauthorized attempt to the information system.
Honeypots are mostly used by large companies and organizations involved in cybersecurity. It helps cybersecurity researchers to learn about the different type of attacks used by attackers. It is suspected that even the cybercriminals use these honeypots to decoy researchers and spread wrong information.

The **cost of a honeypot** is generally **high** because it requires specialized skills and resources to implement a system such that it appears to provide an organization's resources still preventing attacks at the backend and access to any production system.
A **honeynet** is a combination of two or more honeypots on a network.

Types of Honeypot:

Honeypots are classified based on their deployment and the involvement of the intruder. Based on their deployment, honeypots are divided into :

1. **Research honeypots-** These are used by researchers to analyze hacker attacks and deploy different ways to prevent these attacks.
2. **Production honeypots-** Production honeypots are deployed in production networks along with the server. These honeypots act as a frontend trap for the attackers, consisting of false information and giving time to the administrators to improve any vulnerability in the actual system.

Based on interaction, honeypots are classified into:

1. **Low interaction honeypots:**Low interaction honeypots gives very little insight and control to the hacker about the network. It simulates only the services that are frequently requested by the attackers. The main operating system is not involved in the low interaction systems and therefore it is less risky. They require very fewer resources and are easy to deploy. The only disadvantage of these honeypots lies in the fact that experienced hackers can easily identify these honeypots and can avoid it.
2. **Medium Interaction Honeypots:** Medium interaction honeypots allows more activities to the hacker as compared to the low interaction honeypots. They can expect certain activities and are designed to give certain responses beyond what a low-interaction honeypot would give.
3. **High Interaction honeypots:**A high interaction honeypot offers a large no. of services and activities to the hacker, therefore, wasting the time of the hackers and trying to get complete information about the hackers. These honeypots involve the real-time operating system and therefore are comparatively risky if a hacker identifies the honeypot. High interaction honeypots are also very costly and are complex to implement. But it provides us with extensively large information about hackers.

Advantages of honeypot:

1. Acts as a rich source of information and helps collect real-time data.
2. Identifies malicious activity even if encryption is used.
3. Wastes hackers' time and resources.
4. Improves security.

Disadvantages of honeypot:

1. Being distinguishable from production systems, it can be easily identified by experienced attackers.
2. Having a narrow field of view, it can only identify direct attacks.
3. A honeypot once attacked can be used to attack other systems.
4. Fingerprinting(an attacker can identify the true identity of a honeypot).

Introduction to Honeypots, Honeynets, and Padded Cells:

In the world of computer security, there are a lot of different terms and technologies that can be used to protect systems and data. One of these technologies is called a honeypot. A honeypot is a system that is designed to lure in attackers and then track or monitor their activities. Honeypots can be used for a variety of purposes, including research, detection, and prevention of attacks. Honeypots are often confused with honeynets. A honeynet is a network of honeypots. A honeynet can be used for the same purposes as a single honeypot, but it has the added benefit of being able to track attacks across multiple systems. Padded cell systems are similar to honeypots in that they are designed to lure in attackers. However, instead of tracking or monitoring attackers, padded cell systems are designed to contain them. Padded cell systems are often used in conjunction with honeypots to provide a two-pronged approach to security. Do you want to learn more about honeypots, honeynets, and padded cell systems? Continue reading our blog for more information.

Honeypots and Honeynets

Honeypots are deception systems used to divert potential attackers' attention away from important systems.

A honeynet is formed when many honeypot systems are linked together on a network segment. A honeypot system, also known as a honeynet subnetwork, has pseudo-services that mimic well-known services, but it is designed in such a way that it appears vulnerable to assaults. This combination is intended to entice attackers into disclosing themselves; the idea being that once these attackers are identified, companies can better secure their networks against future attacks that target actual assets.

What can a Honeypot do?

Honeypots are intended to perform the following:

- Shift an attacker's concentration away from key systems.
- Obtain data about the bad actor's behavior and urge the attacker to be on the desired system for an adequate time. This way you could record and maybe respond to the incident. Since the information in a honeypot looks to be valuable, any unwanted access to it raises suspicions.
- Honeypots are supplied with sophisticated detectors and incident recorders. These features help identify attempted system access and collect data on the behavior of the potential attacker.

What is a Padded Cell?

A padded cell is a tightened honeypot that works in unison with the traditional Intrusion Detection and Prevention System (which is abbreviated as IDPS).

- Honeypot lures the attackers with enticing material,
- The IDPS makes a discovery
- Moves them to a unique mock environment (padding cell) where they are neutralized.

Padded cells, like honeypots, are well-equipped and provide a unique opportunity for a target company to watch an attacker's operations.

Here are some advantages of these tools:

- You can direct attackers to destinations they can't harm.
- You have time to create a response plan.
- You can record and analyze the attackers' actions.
- You can also detect inside threats prowling about a network.

Hovewer there are some points you should also take into consideration if you want to integrate these systems to your defense:

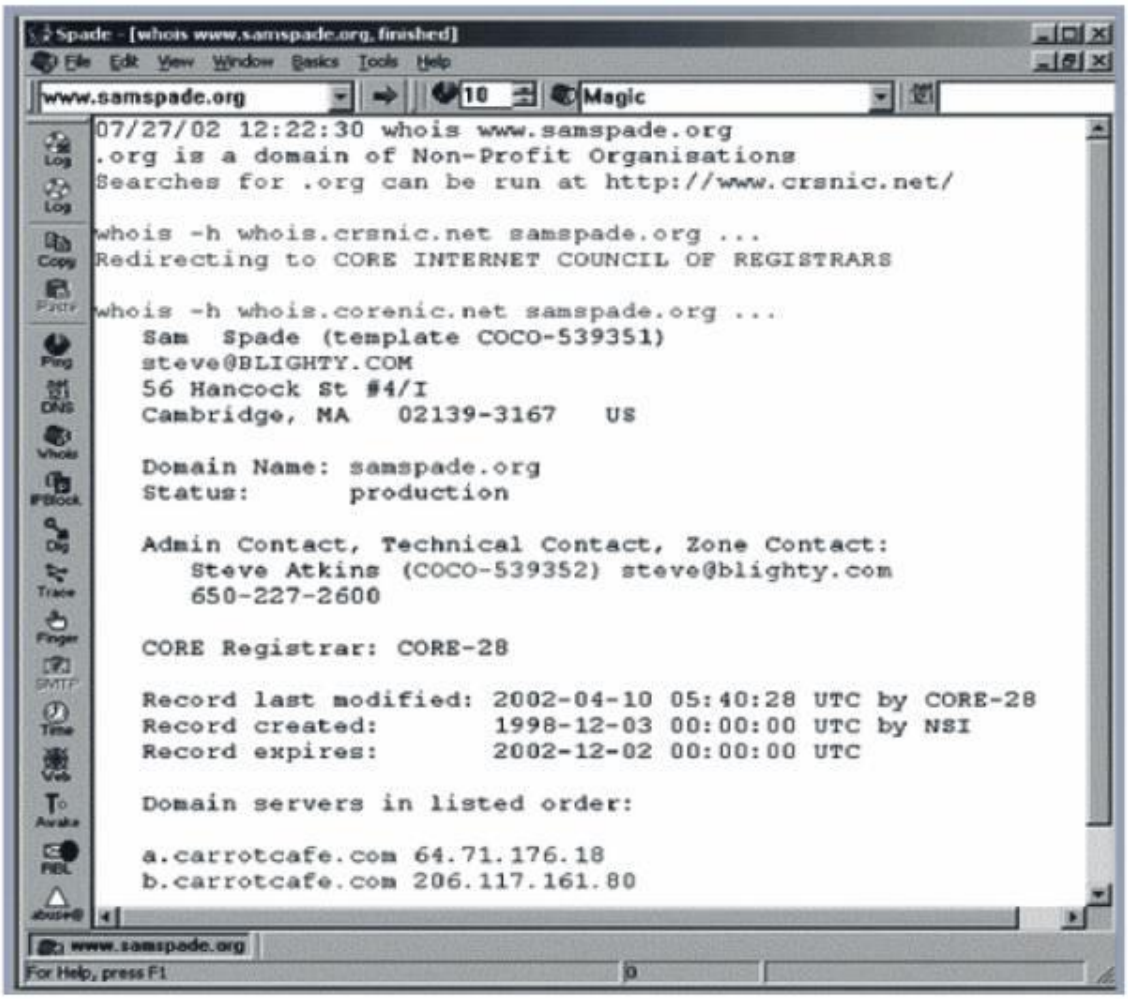
- You should clearly understand the legal consequences of utilizing such tools.
- Honeypots and padded cells have yet to be proven to be general-purpose security systems.
- Once you redirect a skilled attacker into this baiting system, he or she may launch a more aggressive attack on your systems.
- You need specialists to operate these systems. In such cases, the dangers are almost certainly well known, and suitable security safeguards, protocols, and procedures are almost certainly already in place (and properly practiced).

SCANNING AND ANALYSIS TOOLS:

Typically used to collect information that attacker would need to launch successful attack

Attack protocol is series of steps or processes used by an attacker, in a logical sequence, to launch attack against a target system or network

Footprinting: the organized research of Internet addresses owned or controlled by a target organization



Fingerprinting: systematic survey of all of target organization's Internet addresses collected during the footprinting phase

Fingerprinting reveals useful information about internal structure and operational nature of target system or network for anticipated attack

These tools are valuable to network defender since they can quickly pinpoint the parts of the systems or network that need a prompt repair to close the vulnerability

Port Scanners

Tools used by both attackers and defenders to identify computers active on a network, and other useful information

-Can scan for specific types of computers, protocols, or resources, or their scans can be generic

-The more specific the scanner is, the better it can give attackers and defenders useful information

Firewall Analysis Tools

Several tools automate remote discovery of firewall rules and assist the administrator in analyzing the rules

Administrators who feel wary of using same tools that attackers use should remember:

It is intent of user that will dictate how information gathered will be used

In order to defend a computer or network well, necessary to understand ways it can be attacked

A tool that can help close up an open or poorly configured firewall will help network defender minimize risk from attack

Packet Sniffers

Network tool that collects copies of packets from network and analyzes them

Can provide network administrator with valuable information for diagnosing and resolving networking issues

In the wrong hands, a sniffer can be used to eavesdrop on network traffic

To use packet sniffer legally, administrator must be on network that organization owns, be under direct authorization of owners of network, and have knowledge and consent of the content creators

Wireless Security Tools

Organization that spends its time securing wired network and leaves wireless networks to operate in any manner is opening itself up for security breach

Security professional must assess risk of wireless networks

A wireless security toolkit should include the ability to sniff wireless traffic, scan wireless hosts, and assess level of privacy or confidentiality afforded on the wireless network

Scanning and its Tools

After making a list of attack-able IPs from Reconnaissance phase, we need to work on phase 2 of Ethical hacking i.e., Scanning. Process of scanning is divided into 3 parts.

1. Determine if system is on and working.
2. Finding ports on which applications are running.
3. Scanning target system for vulnerabilities.

Ping and Ping Sweeps :

Simplest way to check if a system is alive is to ping that system's IP address. A ping is a special form of packet called ICMP packet. On pinging a device IP, an ICMP echo request message is sent to target, and target system send an Echo reply packet in response of echo request message.
Echo reply message tells other valuable information other than telling whether system is alive. It also tells round trip time of packets i.e, time taken by ping message to reach back to us from target system. It also provides information about packet loss which can be helpful in determining reliability of network.

A ping sweep is a method of pinging a list of IP automatically. Pinging a large list of IPs can be time-consuming and problematic. Tool for Ping sweep is Fping. Fping can be invoked by following command.

```
Fping -a -g 172.16.10.1 172.16.10.20
```

- The "-a" switch is used to show a list of only alive IP in our output.
- "-g" switch is used to specify a range of IP.
- In above command range of IP is 172.16.10.1 to 172.16.10.20.

Port Scanning :

In a Computer, there are a total of 65, 536 (0-65, 535) ports. Depending upon nature of communication and application using a port, it can be either UDP or TCP. Scanning system for checking which ports are alive and which ports are used by different applications gave us a better idea about target system.

Port Scanning is done by a tool called Nmap. Nmap is written by Gordon "Fyodor" Lyon. It is available in both GUI and command-line interface.

Command :

```
nmap -sT/U -p 172.16.10.5
```

- "-s" is used to specify connection type.
- -sT means TCP and -sU means UDP connection.
- "-p" means to scan all ports of target IP.

Vulnerability Scanning :

Vulnerability is a weakness in software or system configuration that can be exploited. Missing patches may result in the vulnerability of software.
Software vendors regularly provide patches for known issues. Some Vulnerability leads to remote code execution which is a holy grail of hacking. One of the tools for vulnerability scanning is Nessus. It can be downloaded from website nessus.org. It contains thousands of plugins for

vulnerability scanning. A plugin is a small block of code send to target system IP for purpose of vulnerability scanning.