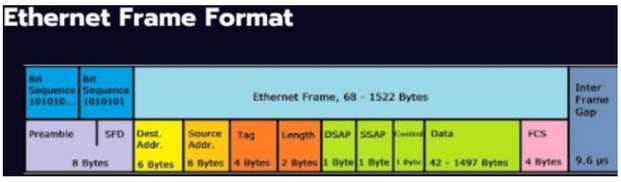
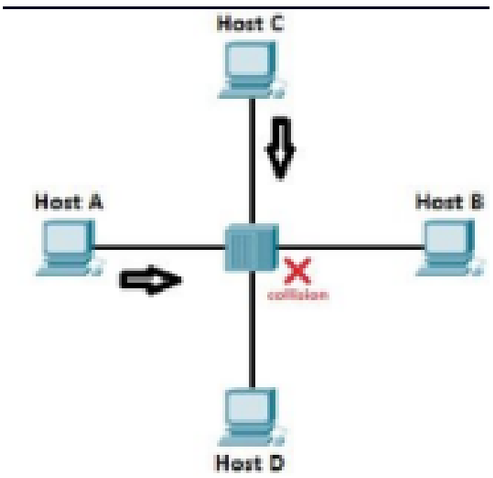
NETWORKING TECHNOLOGY

LOCAL AREA NETWORK

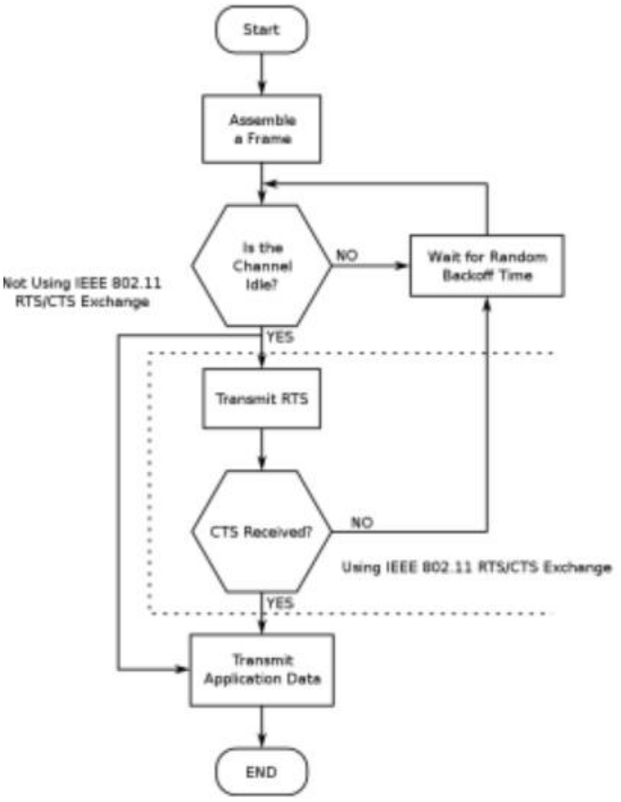
A. ETHERNET
-A LAN standard originally developed by Xerox and later extended by a joint venture between DEC, Intel and Xerox
-The access mechanism used in an Ethernet
-CSMA/CD



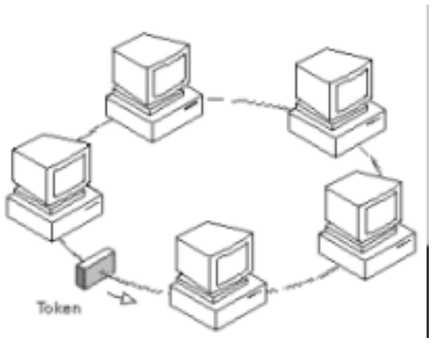
CSMA/CD
-Carrier Sense Multiple Access/Collision Detection
-As indicated by CSMA name, the Ethernet is a multiple access network (a set of nodes send and receive frames over a shared link)
-"carrier sense" in CSMA/CD means that all node can distinguish between an idle and a busy link
-"collision detection" means a node listens as it transmit and can detect when a frame it is transmitting has interfered (collided) with a frame transmitted by another node.



CSMA/CA
- Carrier Sense Multiple Access/Collision Avoidance
- Carrier-sense multiple access with collision avoidance (CSMA/CA) in computer networking, is a network multiple access method in which carrier sensing is used, but nodes attempt to avoid collisions by beginning transmission on after the channel is sensed to be "idle". When they do transmit, nodes transmit their packet data in its entirety.



B. TOKEN RING
- A LAN standard originally developed by IBM, uses a logical ring topology
- Access method
- The token is passed from station to station in sequence until it encounters a station with data to send.



Pros - Token Ring

- In this data flows in one direction which reduces the chance of packet collisions.

- In this topology additional workstations can be added after without impacting performance of the network.

- Equal access to the resources.

- There is no need of server to control the connectivity among the nodes in the topology.

- It is cheap to install and expand.

- Minimum collision.

- Speed to transfer the data is very high in this type of topology.

- Due to the presence of token passing the performance of ring topology becomes better than bus topology under heavy traffic.

- Easy to manage.

- Ring network is extremely orderly organized where every device has access to the token and therefore the opportunity to transmit.

Cons- Token Ring

- Due to the Uni-directional Ring, a data packet (token) must have to pass through all the nodes.

- If one workstation shuts down, it affects whole network or if a node goes down entire network goes down.

- It is slower in performance as compared to the bus topology

- It is Expensive.

- Addition and removal of any node during a network is difficult and may cause issue in network activity.

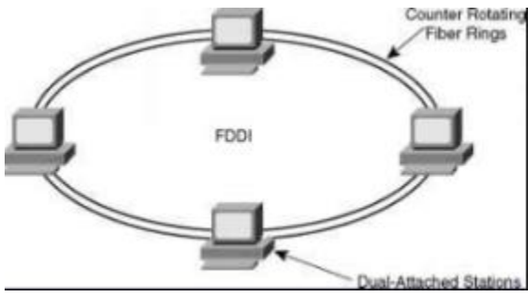
- Difficult to troubleshoot the ring.

- In order for all the computer to communicate with each other, all computer must be turned on.

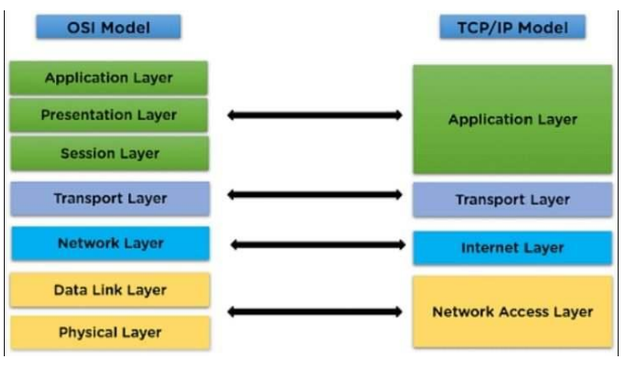
- Total dependence in on one cable.

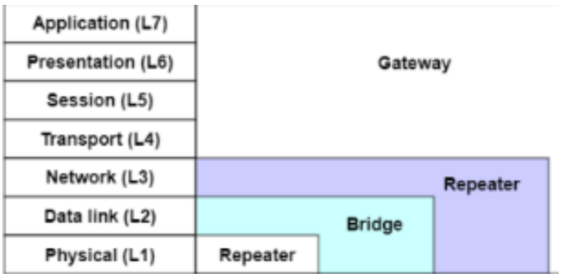
- They were not Scalable.

C. FIBER DISTRIBUTED DATA INTERFACE (FDDI)
   - A LAN protocol standard by ANSI and ITU-T
   - American National Standard Institute
   - International Telecommunications Union – Telecommunication Standardization Sector
   - Access method
   - Token passing
   - If a station receives the token earlier than the designed time, it can keep the token and send data until the scheduled leaving time.



OSI MODEL





(History)

-The design of Ethernet preceded the development of the seven-layer OSI model

- The Open System Interconnection (OSI) model was developed and published in 1982 by the International Organization for Standard (ISO) as a generic model for data communication

- The OSI reference model specifies the seven layers of functionality

Physical Layer

-Provides the interface with physical media Interface : mechanical connection from the device to physical medium used to transmit the digital bit stream

- Responsible for converting the digital data into a bit stream for transmission over the network

- Includes the method of connection used between the network cable and the network adapter

Data link Layer

-Represents the basic communication link that exists between computers

- Responsible for sending/receiving frames or packets of data without errors

- Manages transmission, error acknowledgement and recovery

- When a packet of data is received incorrectly, the data link layer makes system send the data again.

- Defined in IEEE 802.2 logical link control specifications

- Data link control protocols

- High-level Data Link Control (HDLC)

- Advanced Data Communication Control Procedures (ADCCP)

- Link Access Procedure, Balanced (LAP-B)

Transport Layer

- Responsible for ensuring that message are delivered error-free and in the correct sequence

- Splits messages into smaller segments if necessary and provides network traffic control of messages

- Traffic Control

- When data is received, a certain amount of processing must take place before the buffer is clear and ready to receive more data.

- In the absence of flow control, the receiver's buffer may overflow while it is processing old data.

Session Layer

-Controls the network connection between the computers in the network

- Recognizes nodes on the LAN and sets up tables of source and destination addresses

- Responsible for session connection (I.e. for creating, terminating and maintaining network sessions), exception reporting, etc.

Presentation Layer

-Responsible for the data format, which includes the task of hashing the data to reduce the number of bits (hash code) that will be transferred

- Transfers information from the application software to the network session layer to the operating system

- Translates data from application layer into the format used when transmitting across network

- On the receiving end, this layer translates the data back into a format that the application layer can understand

Application Layer

-Highest layer defined in the OSI model

- Responsible for providing user-layer applications and network management functions

- Supporting file service, print service, remote login and e-mail

TCP/IP MODEL

OSI model (7 layers)	TCP/IP model (4 layers)	Internet Protocol suite
Application Presentation Session	Application	HTTP, FTP, TFTP, NFS, etc.
Transport	Transport	TCP, UDP
Network	Internet	IP, ICMP, IGMP, ARP, RARP
Data link Physical	Network Access	Ethernet, token ring, FDDI PPP, X.25, frame relay, ATM

Network Access Layer

-Contains protocols that provide access to a communication network

- Ethernet, Token Ring, FDDI, PPP, etc.

- One function is to route data between hosts attached to the same network

- Provides the device drivers that support interactions with communications hardware such as the token ring or Ethernet

Internet Layer

-Provides Routing function

- Allows data to traverse multiple networks

- Consists of the Internet Protocol (IP) and the Internet Control Message Protocol (ICMP)

Transport Layer

-Delivers data between two processes in different host computers

- Provides a logical connection between higher-level entities

- E-mail ------ E-mail

- Contains the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP)

Application Layer

-Contains protocols for resource sharing and remote access

- Represents the higher-level protocols that are used to provide a direct interface with users or applications

- FTP(File Transfer Protocol)

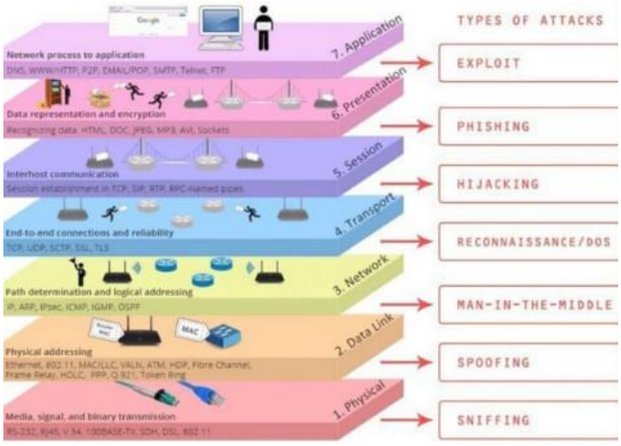
- HTTP(Hyper-Text Transfer Protocol)

- SNMP(Simple Network Management Protocol)

- DNS(Domain Name Service)

- SMPT(Simple Mail Transport Protocol)

- POP(Post Office Protocol)



PENETRATION TESTING

Network penetration tests, or pen testing, simulate attacks from malicious sources. The goal is to determine the feasibility of an attack and consequences if one were to occur. Some pen testing may involve accessing a client's premises and using social engineering skills to test their overall security posture.

Metasploit - This tool provides information about vulnerabilities and aids in penetration testing and IDS signature development.

Tools, such as Nmap and SuperScan, can provide effective penetration testing on a network and determine network vulnerabilities while helping to anticipate attack mechanisms. However, network testing cannot prepare a network administrator for every security problem.

• Penetration testing, or pen testing, is a way of testing the areas of weaknesses in systems by using various malicious techniques. A penetration test simulates methods that an attacker would use to gain unauthorized access to a network and compromise the systems and allows an organization to understand how well it would tolerate a real attack.

• It is important to note that pen testing is different from vulnerability testing, which only identifies potential problems. Pen testing involves hacking a website, network, or server with an organization's permission to try to gain access to resources using various methods that real-life malicious hackers would use.

• One of the primary reasons why an organization would use pen testing is to find and fix vulnerabilities before the cybercriminals do. Penetration testing is a technique used in ethical hacking.

• **Black box testing** is the least time consuming and the least expensive. When conducting black box testing, the specialist has no knowledge of the inner workings of the system and attempts to attack it from the viewpoint of a regular user.

• **Gray box testing** is a combination of black box and white box testing. The specialist will have some limited knowledge about the system, so it is a partially known environment, which gives some advantage to these hacking attempts.

• **White box testing** is the most time consuming and the most expensive because it is conducted by a specialist with knowledge of how the system works. It is therefore a known environment when they attempt to hack into it, emulating a malicious attack by an insider or by someone who has managed to gain such information beforehand, at the recon stage.

4 Penetration Phases

Phase 1: Planning - Establishes the rules of engagement for conducting the test.

Phase 2: Discovery - Conducting reconnaissance on the target to gain information. This can include:

• Passive techniques, which do not require active engagement with the targeted system and are referred to as foot printing — for instance, you might look at the organization's website or other public sources for information.

• Active reconnaissance, such as port scanning, which requires active engagement with the target.

Phase 3: Attack - At this phase, you seek to gain access or penetrate the system using the information gathered in the previous phase. The tester tries to gain escalated privileges and perhaps delve deeper into the network through lateral movement. To move laterally through the network, the tester must pivot through multiple systems. The tester may try to install additional tools or plant a backdoor — this process is known as persistence. The tester will then clean up the system, removing any signs left behind.

Phase 4: Reporting - At this phase, the tester delivers to the organization detailed documentation that includes the vulnerabilities identified, actions taken and the results.

Penetration Testing:

• Penetration testing, or pen testing, is a way of testing the areas of weaknesses in systems by using various malicious techniques.

• A penetration test simulates methods that an attacker would use to gain unauthorized access to a network and compromise the systems and allows an organization to understand how well it would tolerate a real attack.

• There are four phases that make up a penetration test: 1 Planning, 2. Discovery, 3. Attack, and 4. Reporting.

• Some organizations create competing teams to conduct penetration exercises that are longer than a penetration test.

• There is usually a red team (trying to attack the system) and a blue team (trying to defend the system).

• Packet analyzers, or packet sniffers, intercept, and log network traffic.

• Sniffing is also used by network administrators, who can analyze network traffic, identify bandwidth issues, and troubleshoot other network issues using sniffers.

• It uses authorized simulated attacks to test the strength of network security. Internal personnel with hacker experience, or professional ethical hackers, identify assets that could be targeted by threat actors. A series of exploits is used to test security of those assets. Simulated exploit software tools are frequently used. Penetration testing does not only verify that vulnerabilities exist, but it exploits those vulnerabilities to determine the potential impact of a successful exploit.

• Use of hacking techniques and tools to penetrate network defenses and identify depth of potential penetration.

TOOLS: Metasploit, CORE Impact, ethical hackers

Penetration testing uses authorized simulated attacks to test the strength of network security.

NETWORK ANOMALY DETECTION

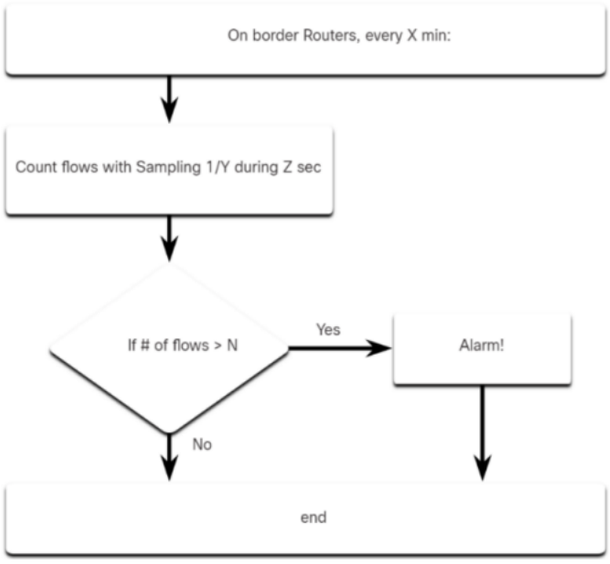
-Network behavior is described by a large amount of diverse data such as the features of packet flow, features of the packets themselves, and telemetry from multiple sources.

- One approach to detection of network attacks is the analysis of this diverse, unstructured data using Big Data analytics techniques.

- This is known as network behavior analysis (NBA) that entails the use of sophisticated statistical and machine learning techniques to compare normal performance baselines with network performance at a given time.

- Significant deviations can be indicators of compromise and network behavior can be analyzed for known network behaviors that indicate compromise.

- Anomaly detection can recognize network traffic caused by worm activity that exhibits scanning behavior and can also identify infected hosts on the network that are scanning for other vulnerable hosts.



-The figure illustrates a simplified version of an algorithm designed to detect an unusual condition at the border routers of an enterprise.

- For example, the cybersecurity analyst provided the following values: X = 5, Y = 100, Z = 30, N = 500

- Now, the algorithm can be interpreted as: every fifth minute, get a sampling of 1/100th of the flows during second thirty.

- If the number of flows is > 500, generate an alarm.

- If the number of flows is < 500, do nothing.

- This is a simple example of using a traffic profile to identify the potential for data loss.

- Rule-based detection analyzes decoded packets for attacks based on pre-defined patterns.

COMMON VULNERABILITY SCORING SYSTEM (CVSS)

-The Common Vulnerability Scoring System (CVSS) is a risk assessment tool that is designed to convey the common attributes and severity of vulnerabilities in computer hardware and software systems.

- The third revision, CVSS 3.0, is a vendor-neutral, industry standard, open framework for weighting the risks of a vulnerability using a variety of metrics.

- These weights combine to provide a score of the risk inherent in a vulnerability.

- The numeric score can be used to determine the urgency of the vulnerability, and the priority of addressing it.

- *The benefits of the CVSS can be summarized as follows:*

1. It provides standardized vulnerability scores that should be meaningful across organizations.

2. It provides an open framework with the meaning of each metric openly available to all users.

3. It helps prioritize risk in a way that is meaningful to individual organizations.

- The Forum of Incident Response and Security Teams (FIRST) has been designated as the custodian of the CVSS to promote its adoption globally.

- The Version 3 standard was developed with contributions by Cisco and other industry partners. Version 3.1 was released in June of 2019.

- The CVSS calculator yields a number (from zero to ten) that describes the severity of the risk that is posed by the vulnerability. The higher the rating level, the greater the urgency for remediation.

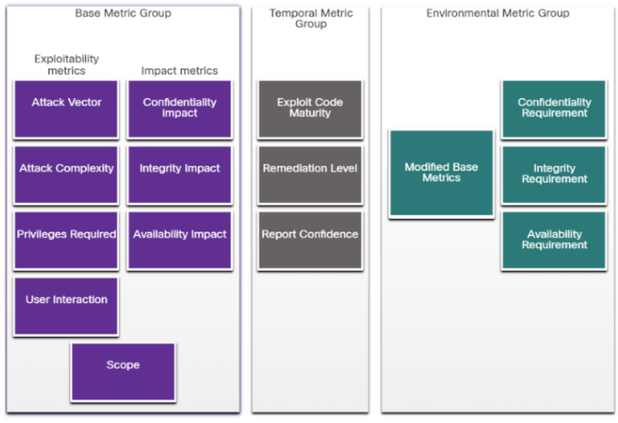
CVSS Metric Groups

-Before performing a CVSS assessment, it is important to know key terms that are used in the assessment instrument.

- Many of the metrics address the role of what the CVSS calls an authority.

- An authority is a computer entity, such as a database, operating system, or virtual sandbox, which grants and manages access and privileges to users.

Base metric group



The CVSS uses three groups of metrics to assess vulnerability:

1. **Basic Metric Group**

This represents the characteristics of a vulnerability that are constant over time and across contexts. It has two classes of metrics:

- Exploitability - These are features of the exploit such as the vector, complexity, and user interaction required by the exploit.
- Impact metrics - The impacts of the exploit are rooted in the CIA triad of confidentiality,

integrity, and availability.

2. **Temporal Metric Group**

This measures the characteristics of a vulnerability that may change over time, but not across user environments. Over time, the severity of a vulnerability will change as it is detected and measures to counter it are developed. The severity of a new vulnerability may be high, but will decrease as patches, signatures, and other countermeasures are developed.

3. **Environmental Metric Group**

This measures the aspects of a vulnerability that are rooted in a specific organization's environment. These metrics help to rate consequences within an organization and allow adjustment of metrics that are less relevant to what an organization does.

The CVSS Process

-The CVSS Base Metrics Group is designed to assess security vulnerabilities found in software and hardware systems.

- It describes the severity of a vulnerability based on the characteristics of a successful exploit of the vulnerability.

- The other metric groups modify the base severity score by accounting for how the base severity rating is affected by time and environmental factors.

- The calculator is like a questionnaire in which choices are made that describe the vulnerability for each metric group.

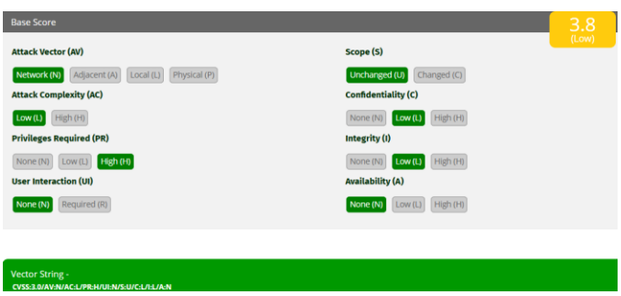
- After all choices are made, a score is generated.

- Pop-up text that explains each metric and metric value is displayed by hovering the mouse over each.

- Choices are made by choosing one of the values for the metric. Only one choice can be made per metric.

- The CVSS calculator can be accessed on the CVSS portion of the FIRST website.

- The Common Vulnerability Scoring System (CVSS) is a vendor-neutral, industry standard, open framework for rating the risks of a given vulnerability by using a variety of metrics to calculate a composite score.



After the Base Metric group is completed, the numeric severity rating is displayed, as shown in the figure.

-A vector string is also created that summarizes the choices made.

- If other metric groups are completed those values are appended to the vector string.

- The string consists of the initial(s) for the metric, and an abbreviated value for the selected metric value separated by a colon.

- The metric-value pairs are separated by slashes.

- The vector strings allow the results of the assessment to be easily shared and compared.

The key for the Base Metric group is:

Metric Name	Initials	Possible Values	Values
Attack Vector	AV	[N, A, L, P]	N = Network, A = Adjacent, L = Local, P = Physical
Attack Complexity	AC	[L, H]	L = Low, H = High
Privileges Required	PR	[N, L, H]	N = None, L = Low, H = High
User Interaction	UI	[N, R]	N = None, R = Required
Scope	S	[U, C]	U = Unchanged, C = Changed
Confidentiality Impact	C	[H, L, N]	H = High, L = Low, N = None
Integrity Impact	I	[H, L, N]	H = High, L = Low, N = None
Availability Impact	A	[H, L, N]	H = High, L = Low, N = None

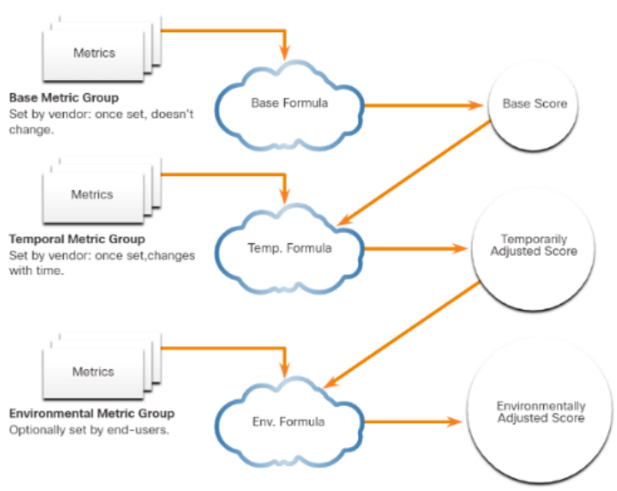
The values for the numeric severity rating string CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N are listed in the table:

Metric Name	Values
Attack Vector, AV	Network
Attack Complexity, AC	Low
Privileges Required, PR	High
User Interaction, UI	None
Scope, S	Unchanged
Confidentiality Impact, C	Low
Integrity Impact, I	Low
Availability Impact, A	None

For a score to be calculated for the Temporal or Environmental metric groups, the Base Metric group must first be completed.

The Temporal and Environmental metric values then modify the Base Metric results to provide an overall score.

The interaction of the scores for the metric groups is shown in the figure.



CVSS Reports

Rating	CVSS Score
None	0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

The table shows the ranges of scores and the corresponding qualitative meaning.

-Frequently, the Base and Temporal metric group scores will be supplied to customers by the application or security vendor in whose product the vulnerability has been discovered.

-The affected organization completes the environmental metric group to tailor the vendor-supplied scoring to the local context.

- The resulting score serves to guide the affected organization in the allocation of resources to address the vulnerability.

- The higher the severity rating, the greater the potential impact of an exploit and the greater the urgency in addressing the vulnerability.

- While not as precise as the numeric CVSS scores, the qualitative labels are especially useful for communicating with stakeholders who are unable to relate to the numeric scores.

- In general, any vulnerability that exceeds 3.9 should be addressed.

Other Vulnerability Information Sources

There are other important vulnerability information sources. These work together with the CVSS to provide a comprehensive assessment of vulnerability severity.

There are two systems that operate in the United States:

1. **Common Vulnerabilities and Exposures (CVE)**
   - A dictionary of common names, in the form of CVE identifiers, for known cybersecurity vulnerabilities.
   - The CVE identifier provides a standard way to research a reference to vulnerabilities.
   - When a vulnerability has been identified, CVE identifiers can be used to access fixes.
   - In addition, threat intelligence services use CVE identifiers, and they appear in various security system logs.
   - The CVE Details website provides a linkage between CVSS scores and CVE information.
   - It allows browsing of CVE vulnerability records by CVSS severity rating.
2. **National Vulnerability Database (NVD)**
   - This utilizes CVE identifiers and supplies additional information on vulnerabilities such as CVSS threat scores, technical details, affected entities, and resources for further investigation.
   - The database was created and is maintained by the U.S. government National Institute of Standards and Technology (NIST) agency.

1. Attack Vector (AV)

- **N (Network)**: The vulnerability can be exploited remotely.
- **A (Adjacent)**: The attack is limited to the same shared physical or logical network (e.g., Bluetooth, local network).
- **L (Local)**: The attacker must have physical or logical access to the vulnerable system.
- **P (Physical)**: Exploitation requires physical interaction (e.g., plugging in a USB drive).

2. Attack Complexity (AC)

- **L (Low)**: The attack does not require any special conditions or circumstances.
- **H (High)**: There are special circumstances or conditions that are necessary for the attack to be successful (e.g., certain configurations).

3. Privileges Required (PR)

- **N (None)**: The attacker does not need to be authenticated to exploit the vulnerability.
- **L (Low)**: The attacker needs low privileges (e.g., user-level access).
- **H (High)**: The attacker needs high privileges (e.g., admin-level access).

4. User Interaction (UI)

- **N (None)**: The attack does not require any interaction from a user.
- **R (Required)**: The attack requires user interaction (e.g., the user needs to click a link or open a file).

5. Scope (S)

- **U (Unchanged)**: The exploited vulnerability only affects resources managed by the same security authority.
- **C (Changed)**: The vulnerability affects resources beyond the vulnerable component's security authority (e.g., exploiting one service to affect another).

6. Confidentiality (C)

- **H (High)**: Exploiting the vulnerability results in a total compromise of confidential data.
- **L (Low)**: Some confidential information is compromised.
- **N (None)**: No impact on confidentiality.

7. Integrity (I)

- **H (High)**: Complete compromise of data integrity, including modification or destruction.
- **L (Low)**: Some impact on data integrity.
- **N (None)**: No impact on integrity.

8. Availability (A)

- **H (High)**: The vulnerability results in a total loss of availability (e.g., service is completely down).
- **L (Low)**: Some loss of availability, such as performance degradation.
- **N (None)**: No impact on availability.

PATCH MANAGEMENT

-Patch management is related to vulnerability management and involves all aspects of software patching, including acquiring, distributing, installing, and verifying patches.

- There are different patch management techniques such as agent-based, agentless scanning, and passive network monitoring.

- Patch management is related to vulnerability management.

- Vulnerabilities frequently appear in critical client, server, and networking device operating systems and firmware.

- Patch management involves all aspects of software patching, including identifying required patches, acquiring, distributing, installing, and verifying that the patch is installed on all required systems.

- Installing patches is frequently the most effective way to mitigate software vulnerabilities.

- Patch management is required by some compliance regulations, such as SOX and HIPAA.

- Failure to implement patches in a systematic and timely manner could result in audit failure and penalties for non-compliance.

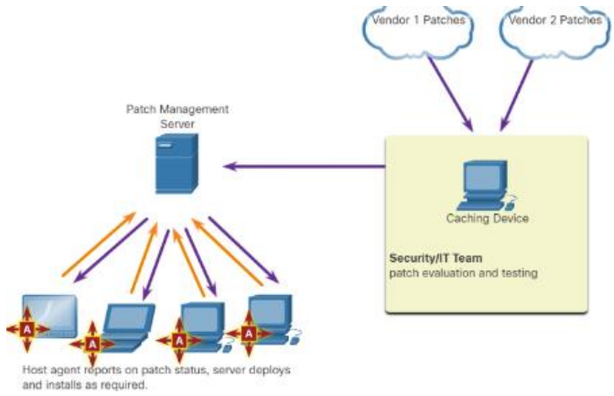
- Patch management depends on asset management data to identify systems that are running software that requires patching.

- Patch management software is available from companies such as SolarWinds and LANDesk.

- Microsoft System Center Configuration Manager (SCCM) is an enterprise-level tool for automated distribution of patches to many Microsoft Windows workstations and servers.

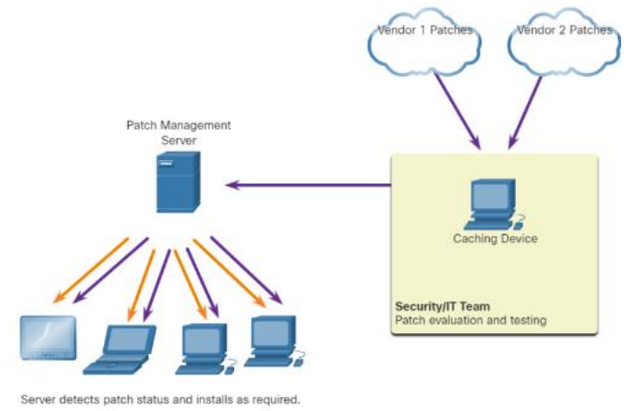
Patch Management Techniques

1. **Agent-based**



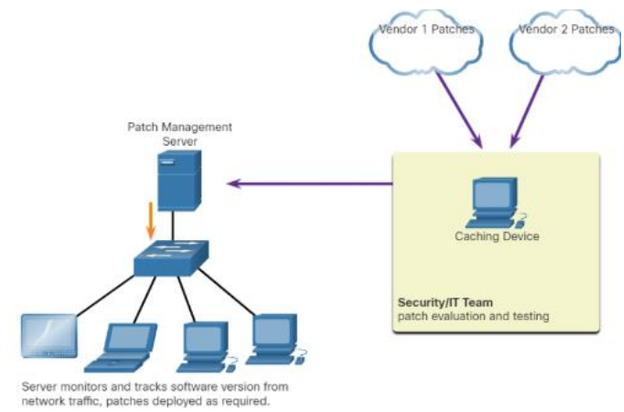
- This requires a software agent to be running on each host to be patched.
- The agent reports whether vulnerable software is installed on the host.
- The agent communicates with the patch management server, determines if patches exist that require installation, and installs the patches.
- The agent runs with sufficient privileges to allow it to install the patches.
- Agent-based approaches are the preferred means of patching mobile devices.

2. **Agentless Scanning**



- Patch management servers scan the network for devices that require patching.
- The server determines which patches are required and installs those patches on the clients.
- Only devices that are on scanned network segments can be patched in this way.
- This can be a problem for mobile devices.

3. **Passive Network Monitoring**



- Devices requiring patching are identified through the monitoring of traffic on the network.

- This approach is only effective for software that includes version information in its network traffic.

Patch management is related to vulnerability management and involves all aspects of software patching, including acquiring, distributing, installing, and verifying patches.

There are different patch management techniques such as agent-based, agentless scanning, and passive network monitoring.