

Information Security Operations Center

Prepared by
Dr. Ibrahim Gomaa

جامعة الجميع الذكية

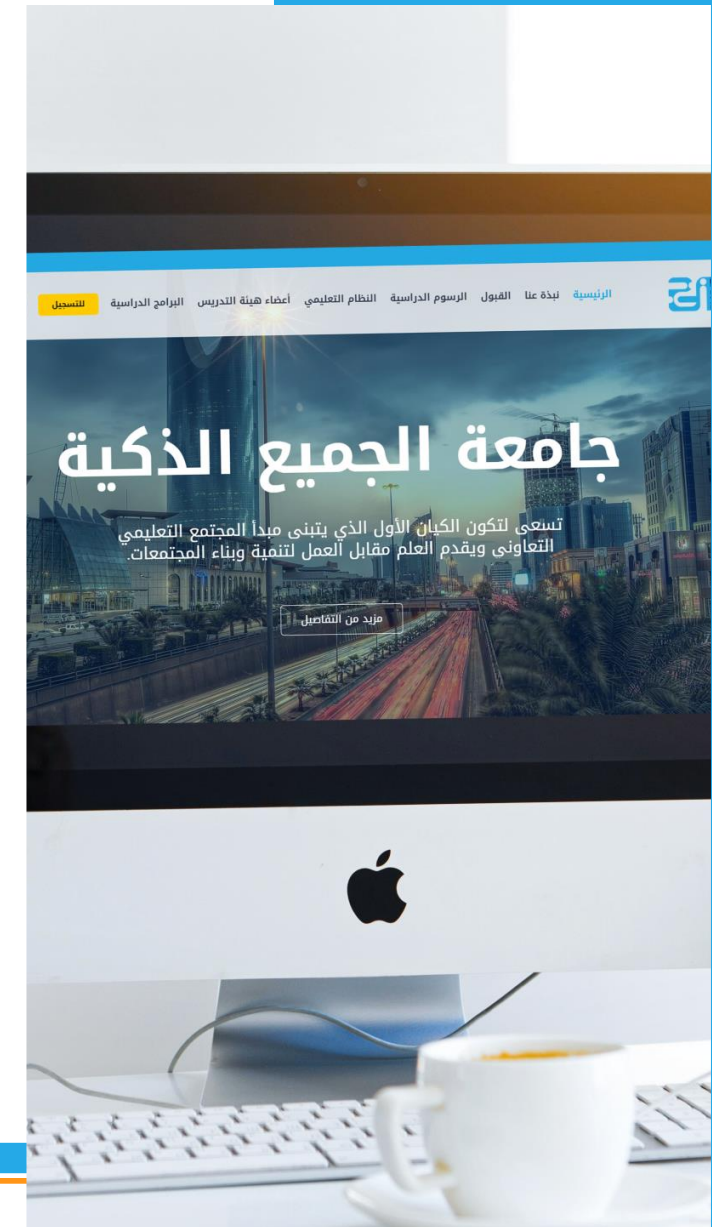
تسعى لتكون الكيان الأول الذي يتبنى مبدأ المجتمع التعليمي
التعاوني ويقدم العلم مقابل العمل لتنمية وبناء المجتمعات.

Lecture 5: Investigate endpoint vulnerabilities and attacks

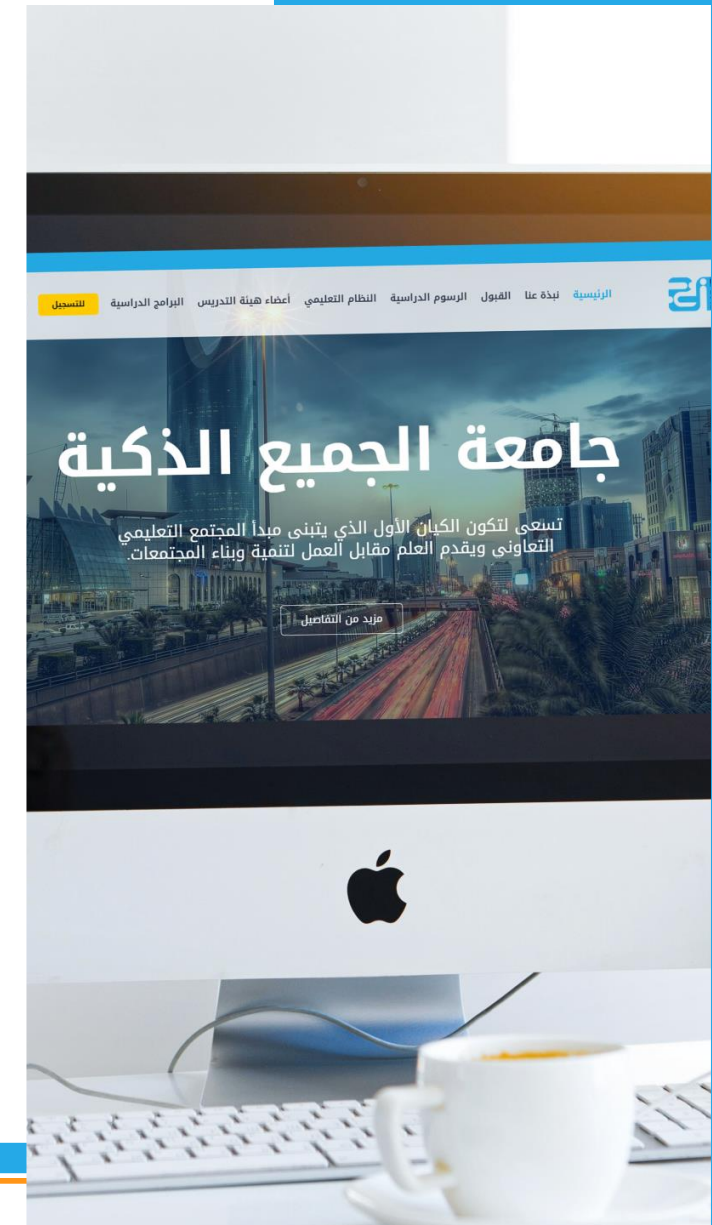


جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

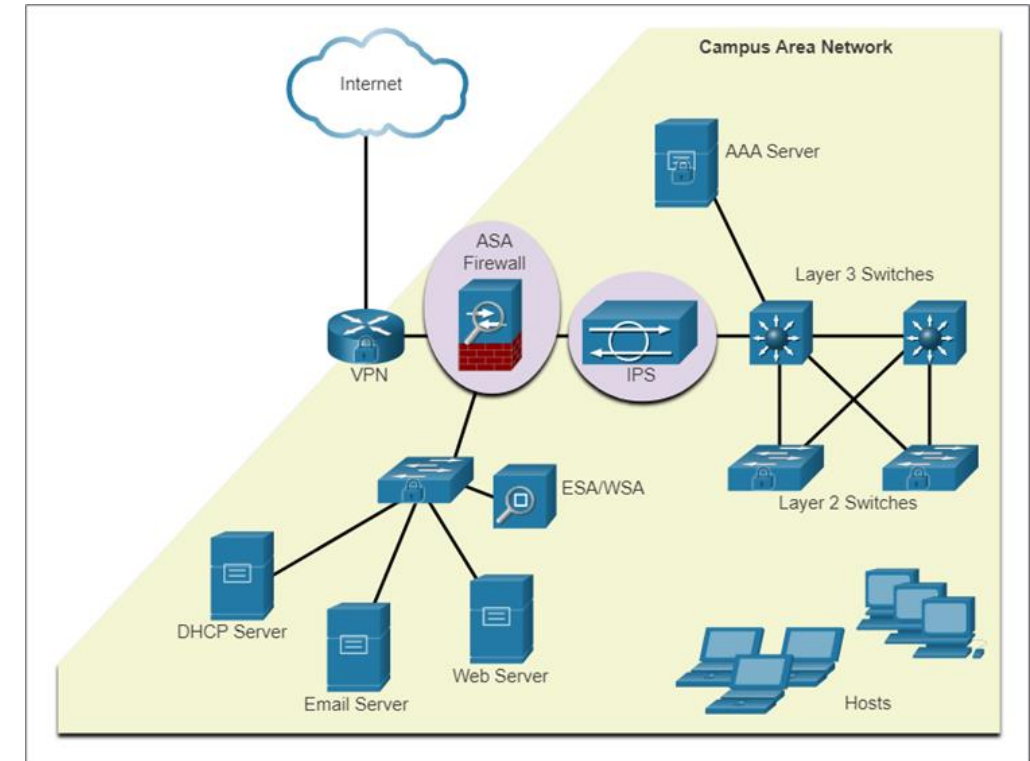
Topic Title	Topic Objective
Antimalware Protection	Explain methods of mitigating malware
Host-based Intrusion Prevention	Explain host-based IPS/IDS log entries
Application Security	Explain how a sandbox is used to analyze malware
Network and Server Profiling	Explain the value of network and server profiling.
Common Vulnerability Scoring System (CVSS)	Explain how CVSS reports are used to describe security vulnerabilities.



Antimalware Protection



- As many attacks originate from inside the network, securing an internal LAN is nearly as important as securing the outside network perimeter.
- After an internal host is infiltrated, it can become a starting point for an attacker to gain access to critical system devices, such as servers and sensitive information.
- There are two internal LAN elements to secure:
 - **Endpoints** - Hosts are susceptible to malware-related attacks.
 - **Network infrastructure** - LAN infrastructure devices interconnect endpoints



Host-Based Malware Protection

- Host-based antimalware/antivirus software and host-based firewalls are used to protect mobile devices using VPN.

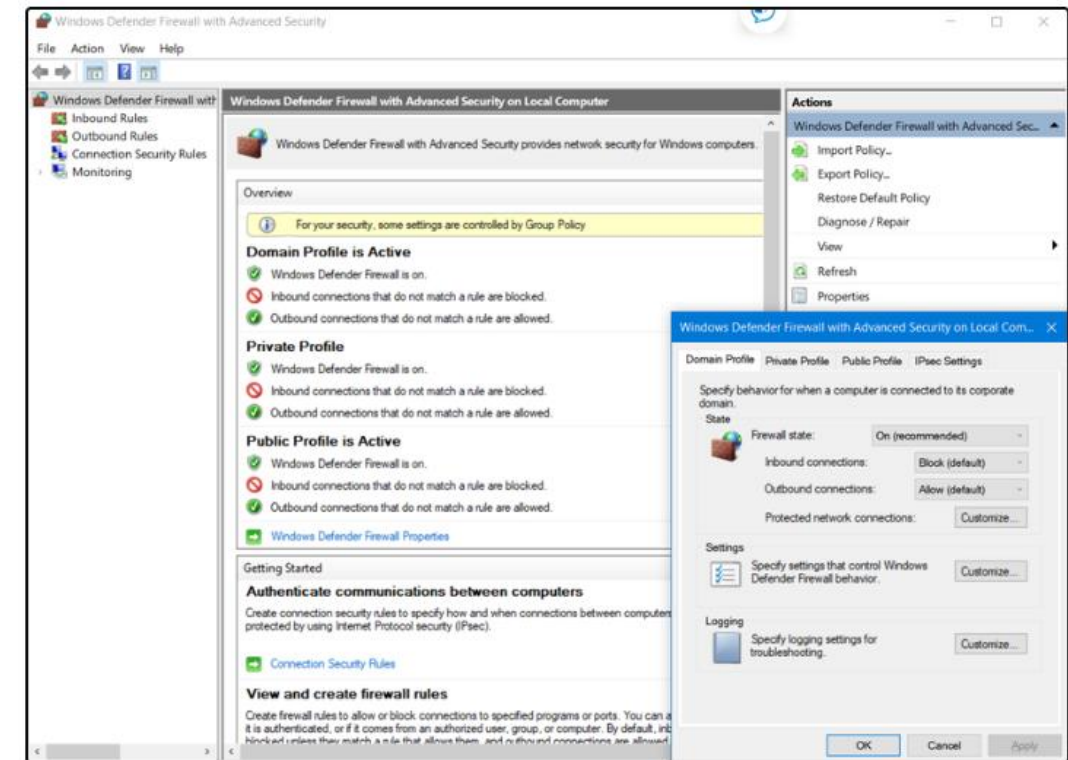
Antivirus/Antimalware Software

- It is a software that is installed on a host to detect and mitigate viruses and malware. For example, Windows Defender Virus & Threat Protection, Cisco AMP for Endpoints, Norton Security, McAfee, Trend Micro, and others.
- Antimalware programs may detect viruses using three different approaches:
 - **Signature-based:** Recognizes various characteristics of known malware files
 - **Heuristics-based:** Recognizes general features shared by various types of malware
 - **Behavior-based:** Employs analysis of suspicious behavior
- Host-based antivirus protection, also known as agent-based, runs on every protected machine.



Host-based Firewall

- This software is installed on a host.
- It restricts incoming and outgoing connections to connections initiated by that host only.
- Some firewall software can prevent a host from becoming infected and stop infected hosts from spreading malware to other hosts. This function is included in some operating systems.
- For example, Windows includes Windows Defender Firewall with Advanced Security.

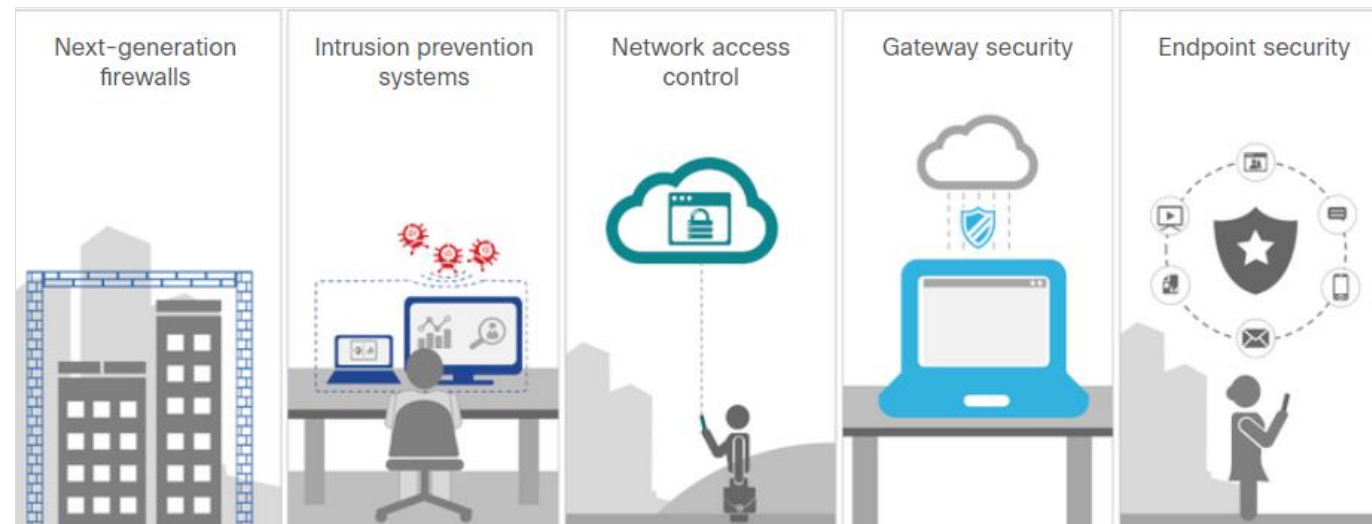


Host-based Security Suites

- It is recommended to install a host-based suite of security products on home and business networks to provide a layered defense that will protect against most common threats.
- These include **antivirus, anti-phishing, safe browsing, Host-based intrusion prevention system, and firewall capabilities.**
- Host-based security products also provide telemetry function.
- Most host-based security software includes robust logging functionality that is essential to cyber security operations.
- The independent testing laboratory AV-TEST provides high-quality reviews of host-based protections, as well as information about many other security products.

Network-Based Malware Protection

- Network-based malware prevention devices are capable of sharing information among themselves to make better informed decisions.
- Protecting endpoints in a borderless network can be accomplished using network-based, as well as host-based techniques.

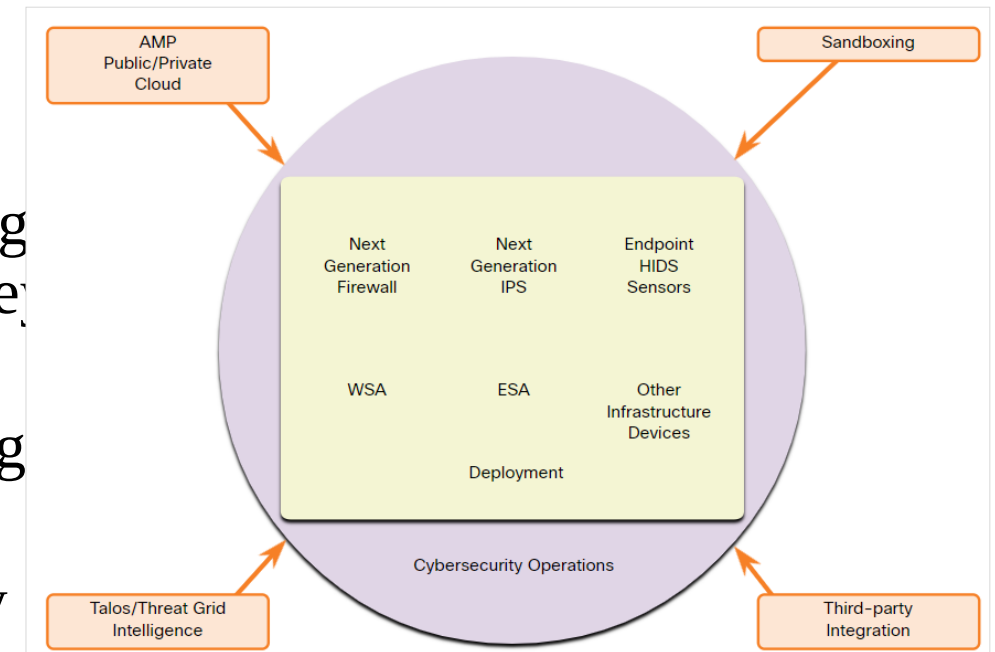


Advanced Malware Protection Everywhere

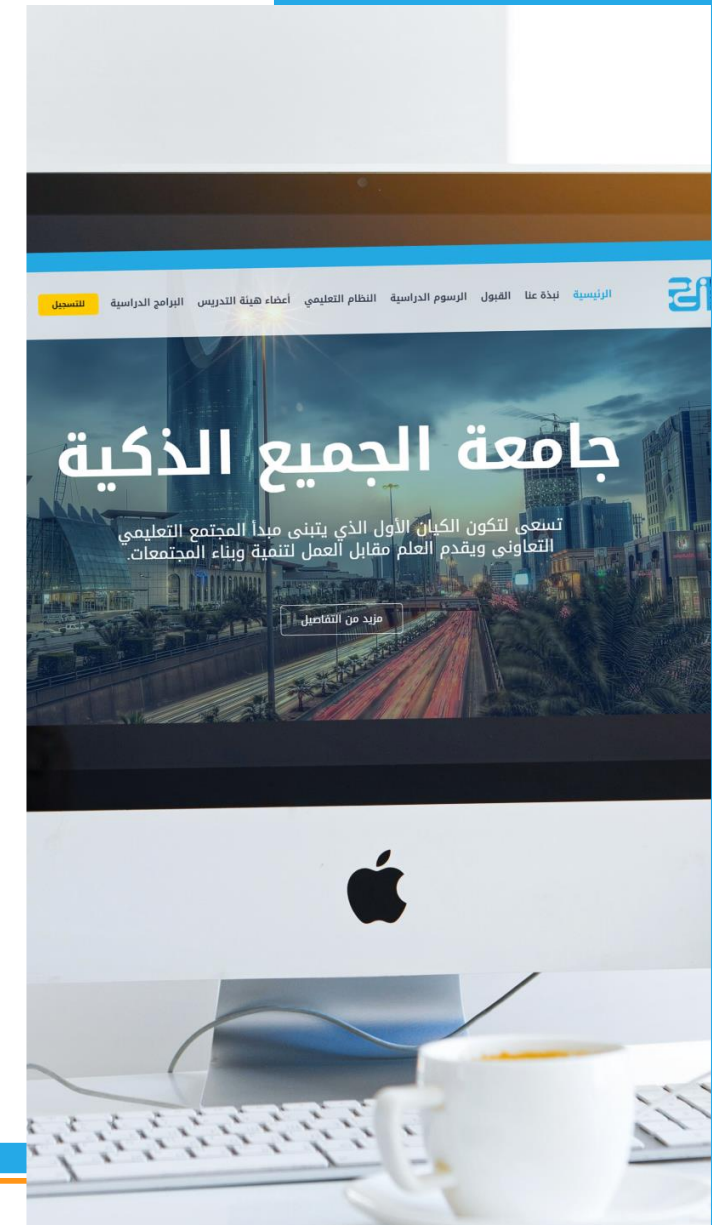
Network-Based Malware Protection (Cont.)

Some examples of devices and techniques that implement host protections at the network level:

- **Advanced Malware Protection (AMP)** - Provides endpoint protection from viruses and malware.
- **Email Security Appliance (ESA)** - Provides filtering of SPAM and potentially malicious emails before they reach the endpoint.
- **Web Security Appliance (WSA)** - Provides filtering of websites and blacklisting
- **Network Admission Control (NAC)** - Permits only authorized and compliant systems to connect to the network.



Host-Based Intrusion Protection

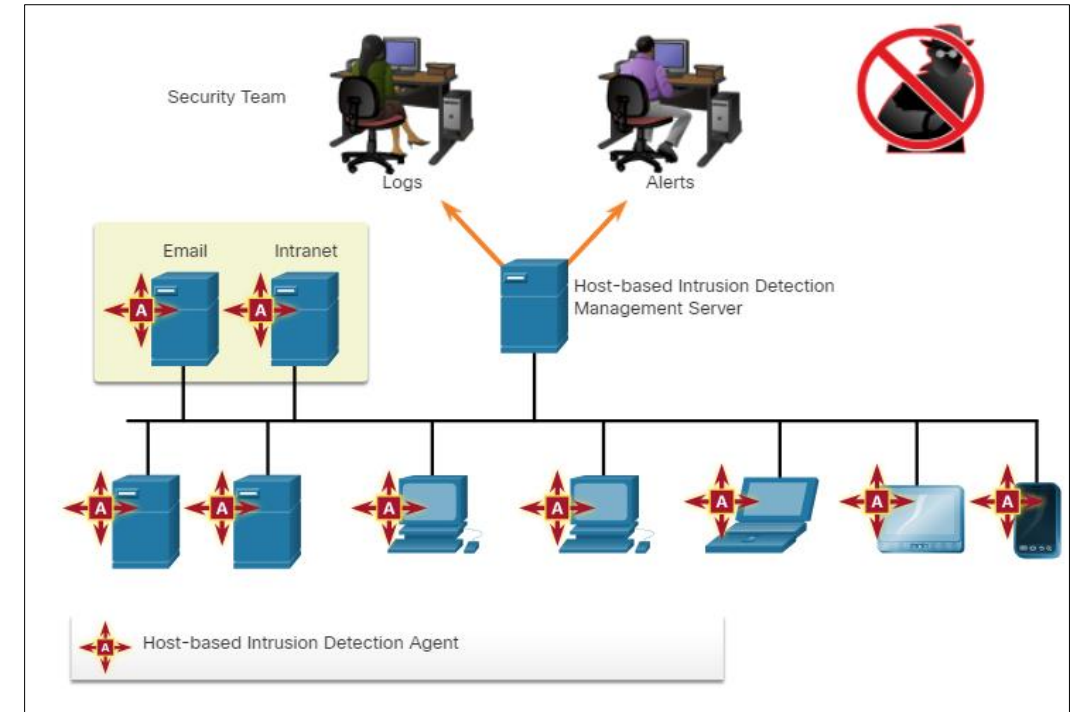


- Host-based personal firewalls are standalone software programs that control traffic entering or leaving a computer.
- Host-based firewall applications can also be configured to issue alerts to users if suspicious behavior is detected.
- **Some examples of host-based firewalls:**
 - **Windows Defender Firewall** – First included with Windows XP, Windows Firewall (now Windows Defender Firewall) uses a profile-based approach to firewall functionality.
 - **iptables** – This is an application that allows Linux system administrators to configure network access rules that are part of the Linux kernel Netfilter modules.
 - **nftables** – The successor to iptables, nftables is a Linux firewall application that uses a simple virtual machine in the Linux kernel.
 - **TCP Wrappers** – This is a rule-based access control and logging system for Linux.



Host-Based Intrusion Detection

- A Host-based Intrusion Detection System (HIDS) is designed to protect hosts against known and unknown malware.
- A HIDS can perform detailed monitoring and reporting on the system configuration and application activity.
- HIDS is a comprehensive security application that combines the functionalities of antimalware applications with firewall functionality.
- As HIDS must run directly on the host, it is considered as an agent-based system.

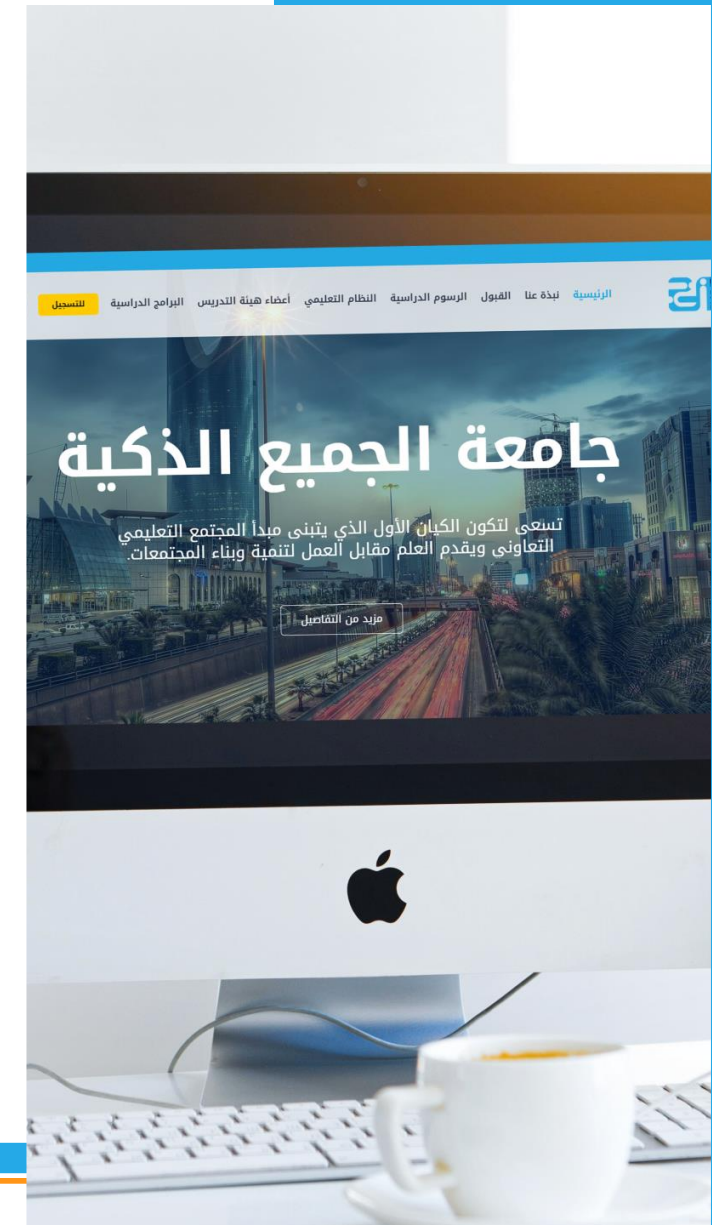


Host-based Intrusion Detection Architecture

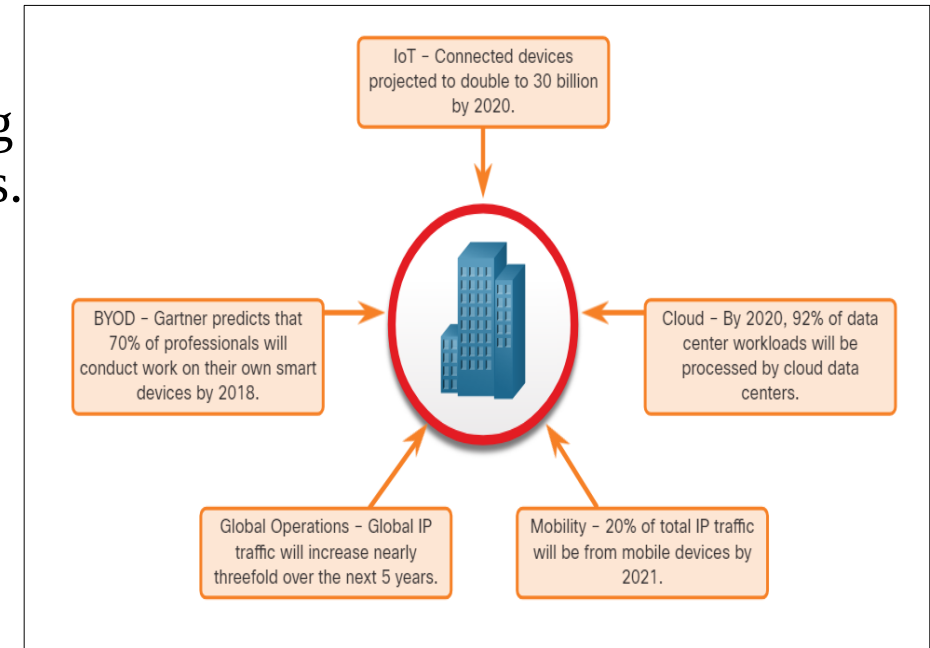
- A HIDS can prevent intrusion because it uses signatures to detect known malware and prevent it from infecting a system.
- Some malware families exhibit **polymorphism** (many shapes).
- **An additional set of strategies** are used to detect the possibility of successful intrusions by malware that evades signature detection:
 - **Anomaly based** - Host system behavior is compared to a learned baseline model of normal behavior. If an intrusion is detected, the HIDS can log details of the intrusion, send alerts to security management systems, and take action to prevent the attack.
 - **Policy based** - Normal system behavior is described by rules, or the violation of rules, that are predefined. Violation of these policies will result in action by the HIDS, such as shut down of software processes.



Application Security



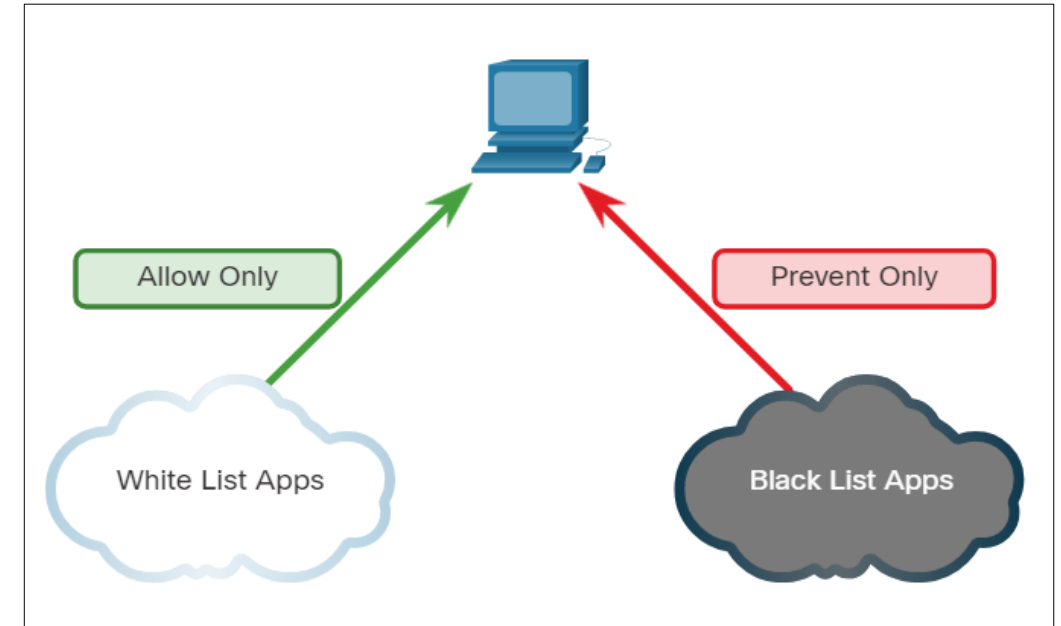
- An attack surface is the total sum of the vulnerabilities in each system that is accessible to an attacker.
- It can consist of open ports on servers or hosts, software running on internet-facing servers, wireless network protocols, and users.
- Components of the Attack Surface:
 - **Network Attack Surface:** Exploits vulnerabilities in networks.
 - **Software Attack Surface:** Delivered through exploitation of vulnerabilities in web, cloud, or host-based software applications.
 - **Human Attack Surface:** Exploits weaknesses in user behavior.



An Expanding Attack Surface

Application Blacklisting and Whitelisting

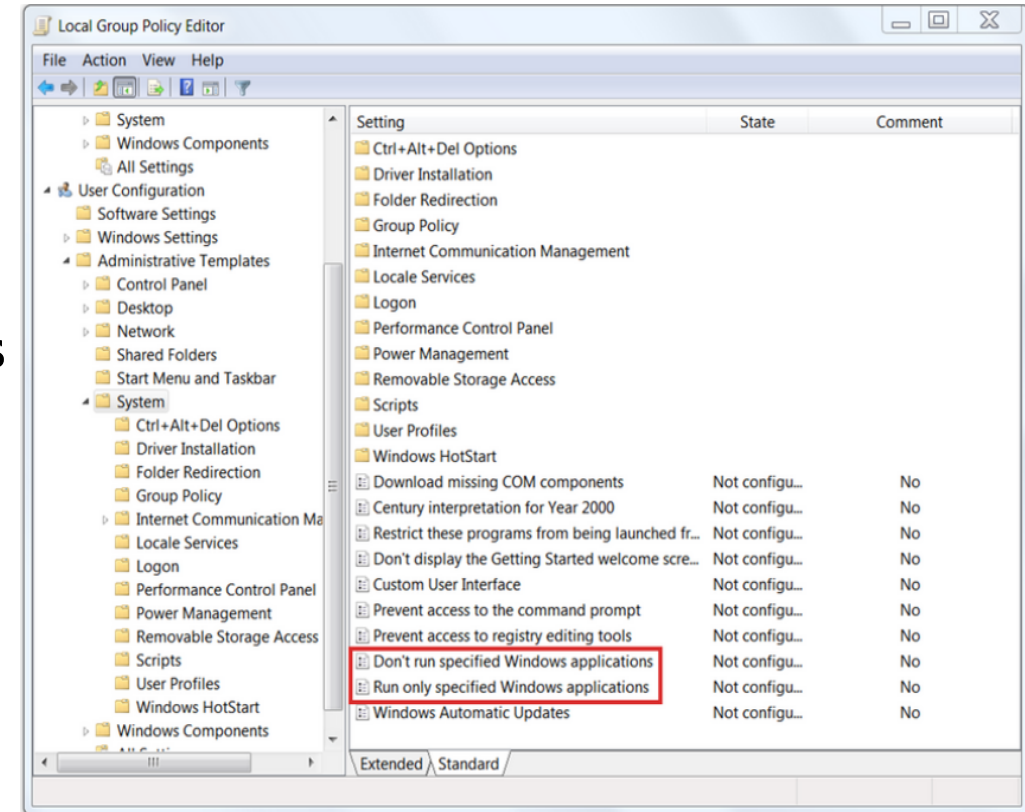
- Limiting access to potential threats by creating lists of prohibited applications is known as blacklisting.
- Application blacklists can dictate which user applications are not permitted to run on a computer.
- Whitelists specify which programs are allowed to run.
- In this way, known vulnerable applications can be prevented from creating vulnerabilities on network hosts.



Application Blacklisting and Whitelisting



- Websites can also be whitelisted and blacklisted.
- These blacklists can be manually created, or they can be obtained from various security services.
- Blacklists can be continuously updated by security services and distributed to firewalls and other security systems that use them.
- Cisco's Firepower security management system is an example of a system that can access the Cisco Talos security intelligence service to obtain blacklists.



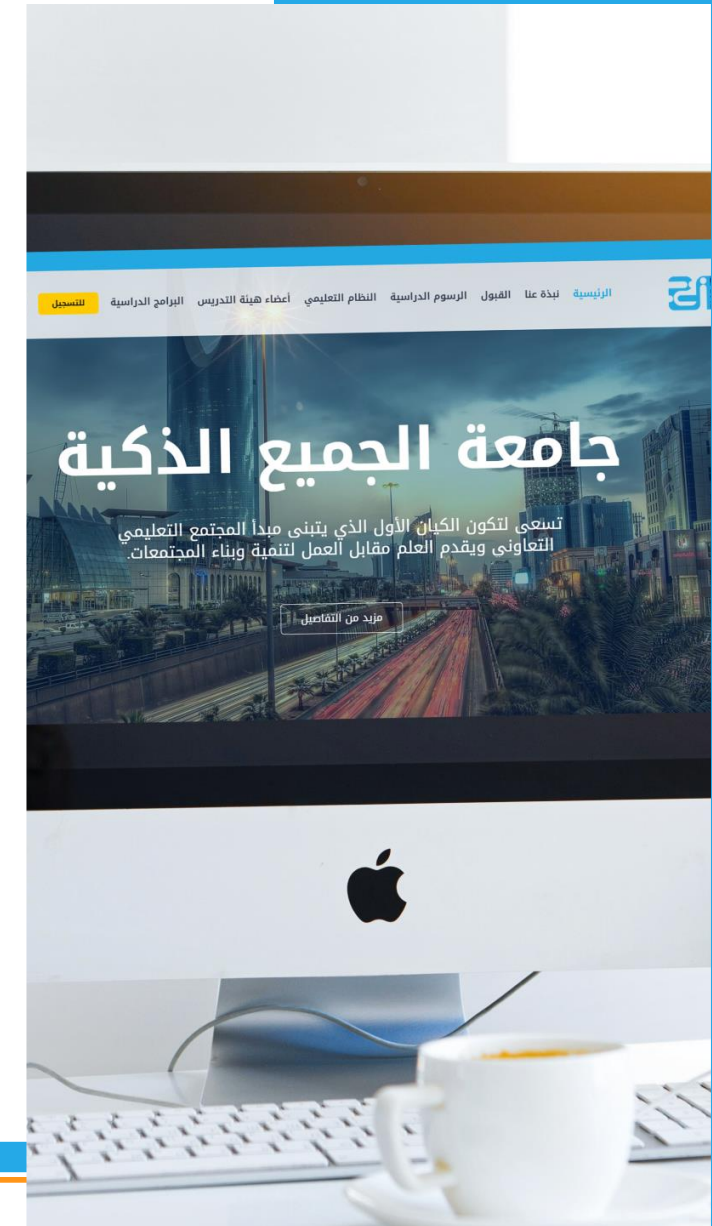
- Sandboxing is a technique that allows suspicious files to be executed and analyzed in a safe environment.
- **Cuckoo Sandbox** is a popular free malware analysis system sandbox. It can be run locally and have malware samples submitted to it for analysis.
- **ANY.RUN** is an online tool that offers the ability to upload a malware sample for analysis like any online sandbox.



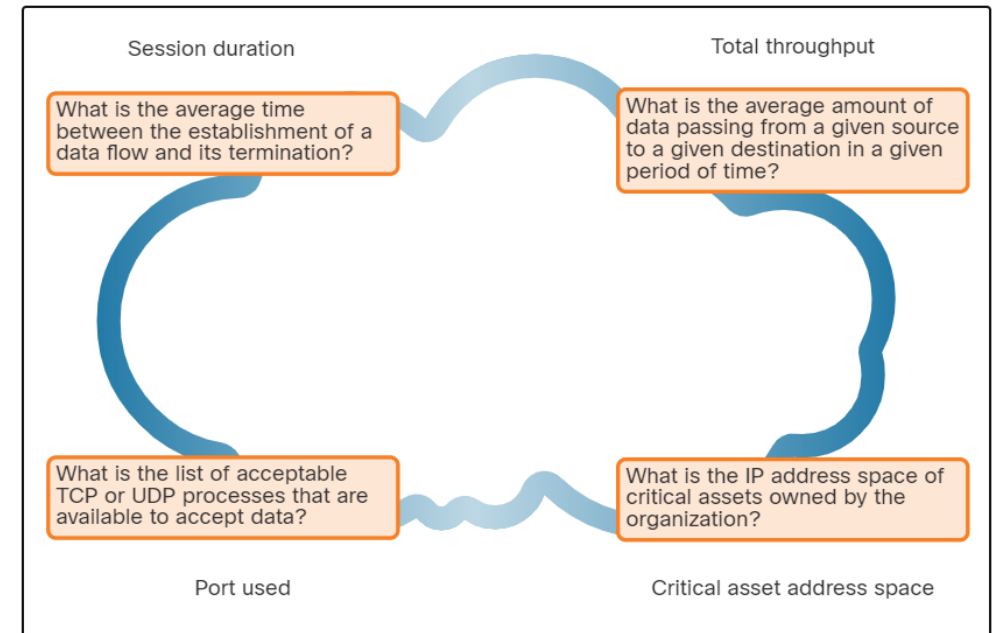
- Sandboxing is a technique that allows suspicious files to be executed and analyzed in a safe environment.
- **Cuckoo Sandbox** is a popular free malware analysis system sandbox. It can be run locally and have malware samples submitted to it for analysis.
- **ANY.RUN** is an online tool that offers the ability to upload a malware sample for analysis like any online sandbox.



Network and Server Profiling

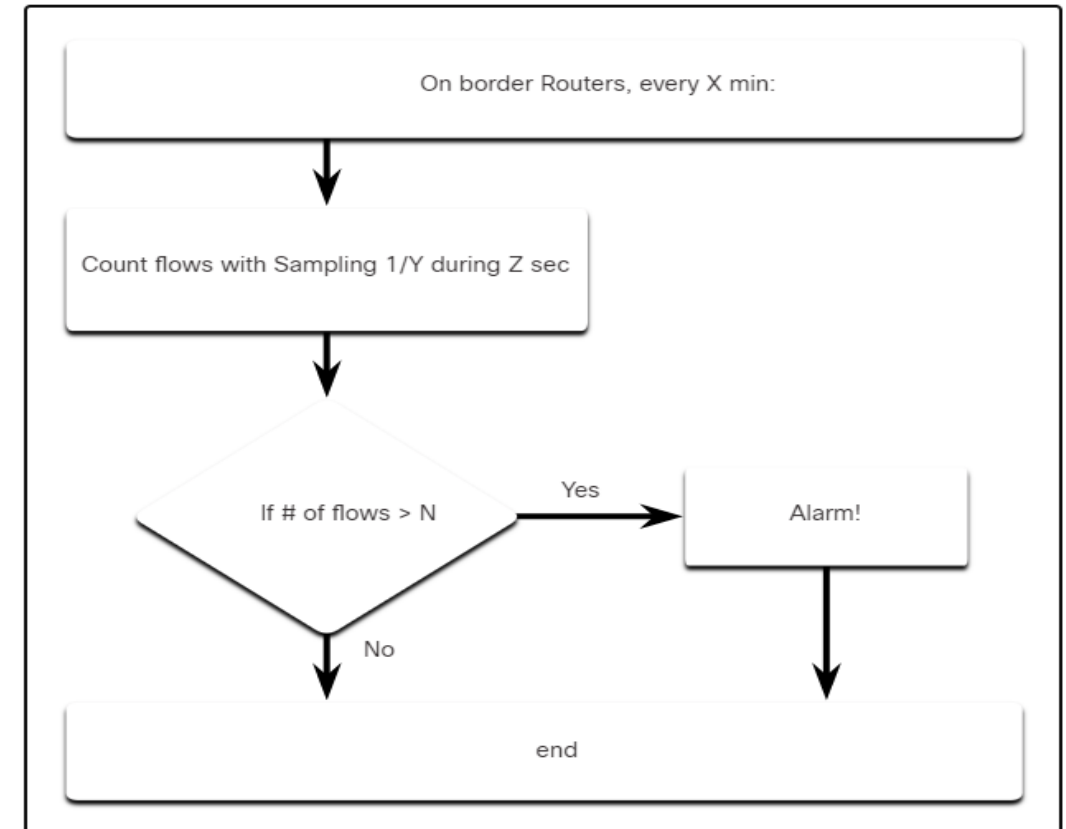


- **Network and device profiling** provides statistical baseline information that can serve as a reference point for normal network and device performance.
- Elements of network profile:
 - Session duration
 - Total throughput
 - Critical asset address space
 - Typical traffic type



- **A server profile** is a security baseline for a given server.
- Server profiling is used to establish the accepted operating state of servers.
- The **server profile elements** are as follows:
 - Listening ports
 - Logged in users and accounts
 - Service accounts
 - Software environment

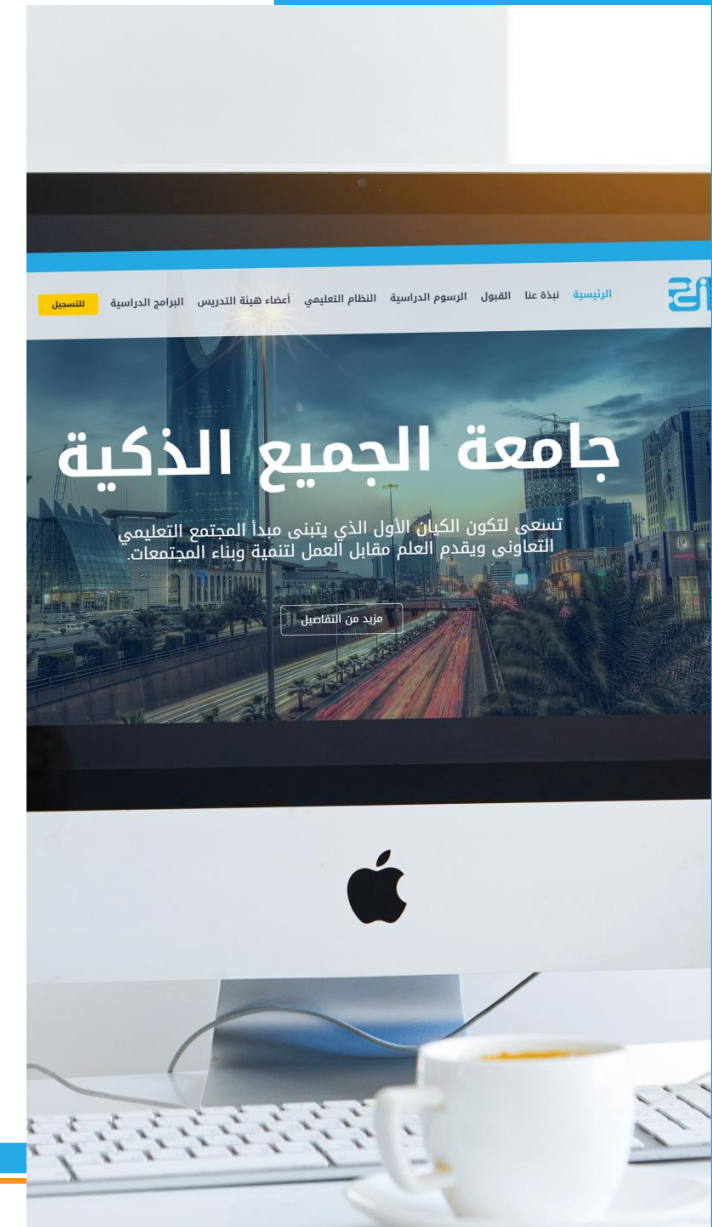
- Network behavior is described by a large amount of diverse data such as the features of packet flow, features of the packets themselves, and telemetry from multiple sources.
- **Big Data analytics techniques** can be used to analyze this data and detect variations from the baseline.
- **Anomaly detection** can 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.



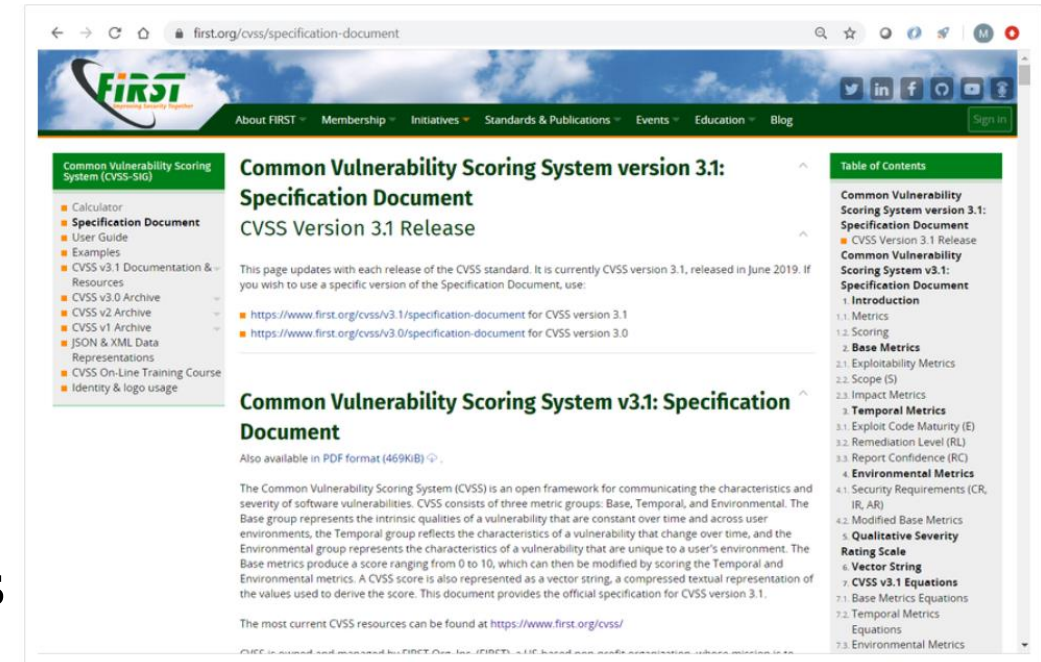
- Network Vulnerability Testing includes Risk Analysis, Vulnerability Assessment and Penetration Testing.
- The table lists examples of activities and tools that are used in vulnerability testing:

Activity	Description	Tools
Risk analysis	Individuals conduct comprehensive analysis of impacts of attacks on core company assets and functioning	Internal or external consultants, risk management frameworks
Vulnerability Assessment	Patch management, host scans, port scanning, other vulnerability scans and services	OpenVas, Microsoft Baseline Analyzer, Nessus, Qualys, Nmap
Penetration Testing	Use of hacking techniques and tools to penetrate network defenses and identify depth of potential penetration	Metasploit, CORE Impact, ethical hackers

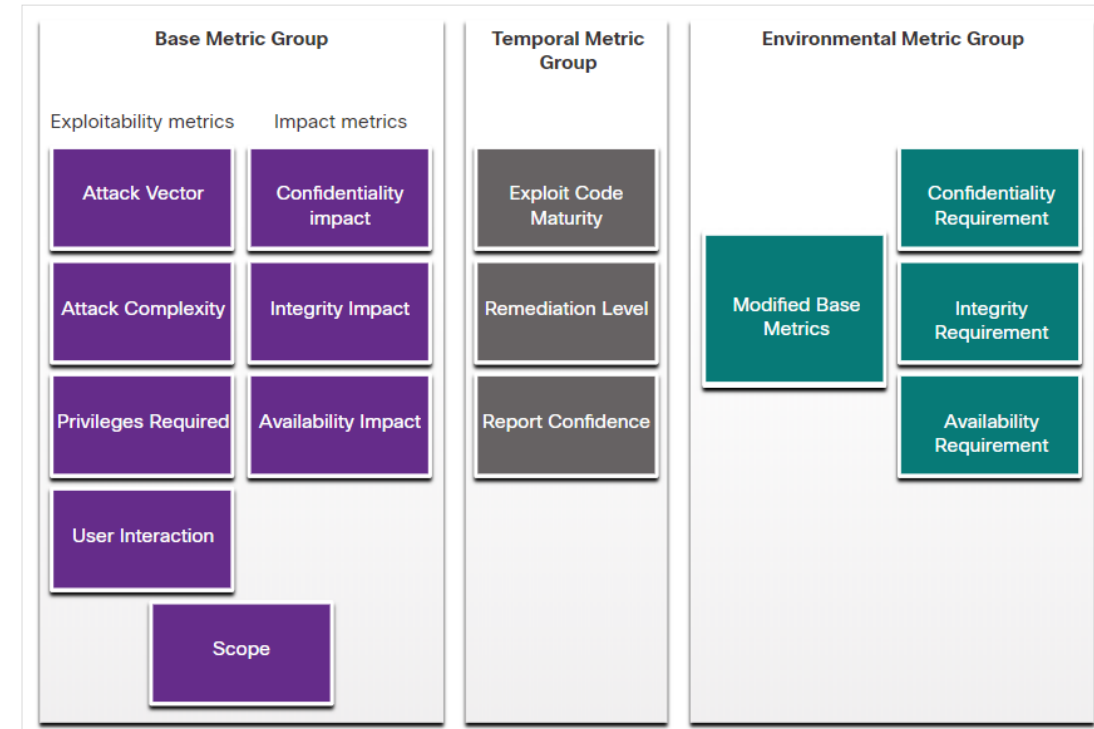
Common Vulnerability Scoring System (CVSS)



- **The Common Vulnerability Scoring System (CVSS)** is a risk assessment tool designed to convey the common attributes and severity of vulnerabilities in computer hardware and software systems.
- CVSS provides standardized vulnerability scores.
- It provides an open framework with metrics to all users.
- CVSS helps prioritize risk.
- The Forum of Incident Response and Security Teams (FIRST) has been designated as the custodian of the CVSS to promote its adoption globally.



- The CVSS uses three groups of metrics to assess vulnerability.
- **Base Metric Group:** Represents the characteristics of a vulnerability that are constant over time and across contexts.
- **Temporal Metric Group:** Measures the characteristics of a vulnerability that may change over time, but not across user environments.
- **Environmental Metric Group:** Measures the aspects of a vulnerability that are rooted in a specific organization's environment.



These are features of the exploit

- Base Metric Group Exploitability metrics include the following criteria:
 - Attack vector
 - Attack complexity Threat actors close to your network (inside your network) or remote.
 - Privileges required the number of components, software, hardware, or networks, that are beyond the attacker's control
 - User interaction the level of access that is required for a successful exploit
 - Scope the presence or absence of the requirement for user interaction
 - Scope whether multiple authorities must be involved in an exploit
- Impact metric components include:
 - Confidentiality Impact
 - Integrity Impact
 - Availability Impact

The impacts of the exploit are rooted in the CIA

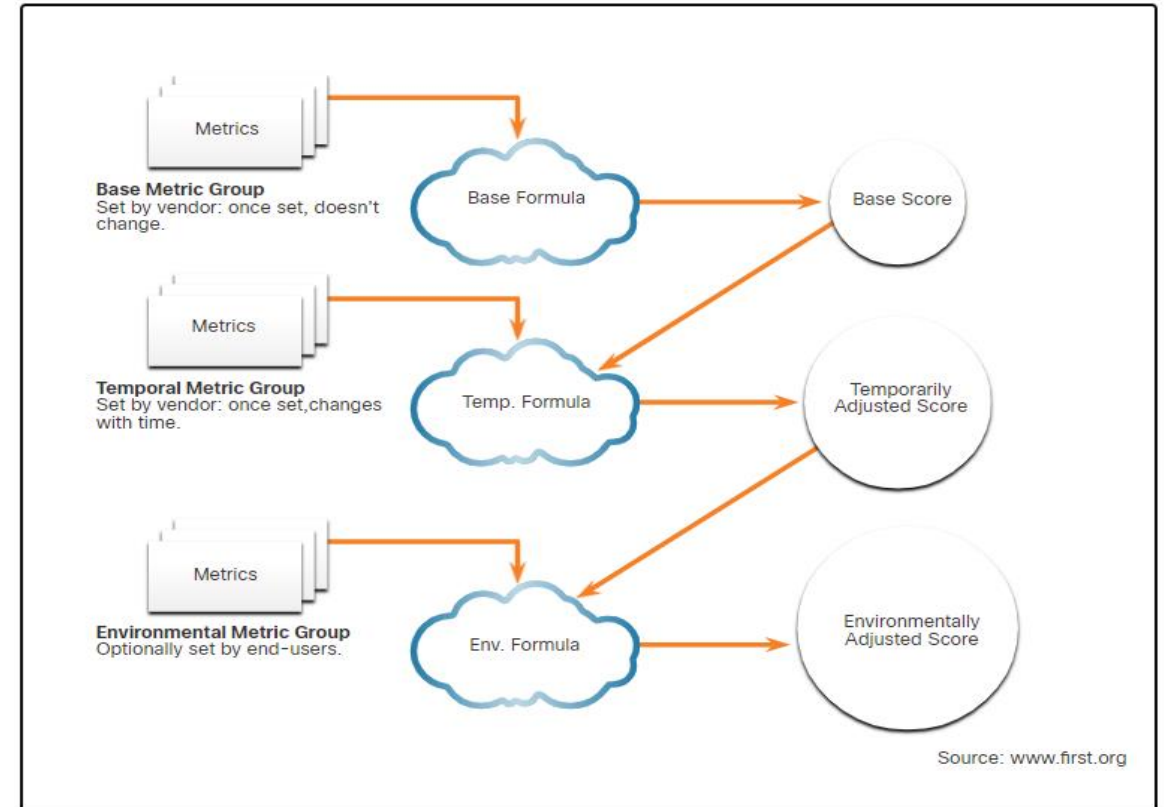


the impact to (CIA) due to a successfully exploited vulnerability.

- The CVSS process uses a tool called **the CVSS v3.1 Calculator**.
- The calculator is like a questionnaire in which the choices are made that describe the vulnerability for each metric group.
- Later, a score is generated, and numeric severity rating is displayed.

The screenshot displays the CVSS v3.1 Calculator interface. At the top right, a yellow box shows the **Base Score** as **3.8 (Low)**. The interface is divided into two columns of metrics, each with a title and a set of radio buttons. The left column includes: **Attack Vector (AV)** with options Network (N), Adjacent (A), Local (L), and Physical (P); **Attack Complexity (AC)** with Low (L) and High (H); **Privileges Required (PR)** with None (N), Low (L), and High (H); and **User Interaction (UI)** with None (N) and Required (R). The right column includes: **Scope (S)** with Unchanged (U) and Changed (C); **Confidentiality (C)** with None (N), Low (L), and High (H); **Integrity (I)** with None (N), Low (L), and High (H); and **Availability (A)** with None (N), Low (L), and High (H). At the bottom, a green bar displays the **Vector String** as **CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N**.

- After the Base Metric group is completed, the Temporal and Environmental metric values modify the Base Metric results to provide an overall score.



- The higher the severity rating, the greater the potential impact of an exploit and the greater the urgency in addressing the vulnerability.
- Any vulnerability that exceeds 3.9 should be addressed.
- The ranges of scores and the corresponding qualitative meaning is shown in the table:

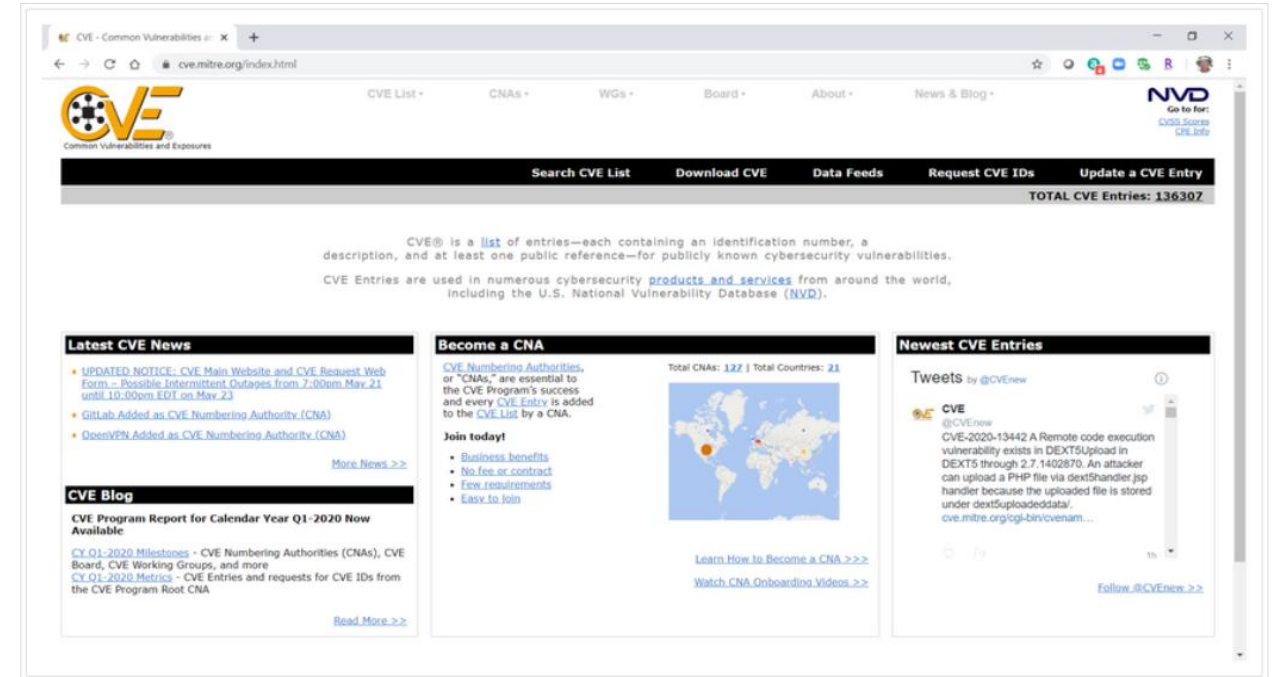
Rating	CVSS Score
None	0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

- The higher the severity rating, the greater the potential impact of an exploit and the greater the urgency in addressing the vulnerability.
- Any vulnerability that exceeds 3.9 should be addressed.
- The ranges of scores and the corresponding qualitative meaning is shown in the table:

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

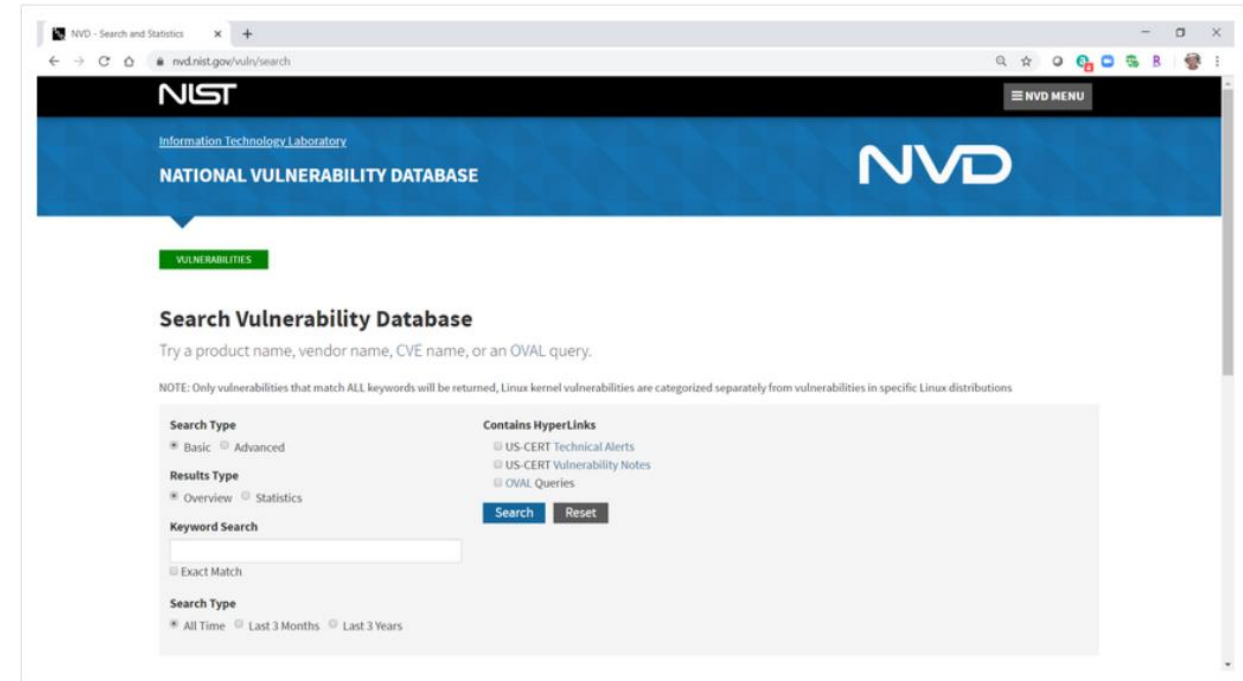
Common Vulnerabilities and Exposures (CVE):

- CVE identifier provides a standard way to research a reference to vulnerabilities.
- **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.



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.



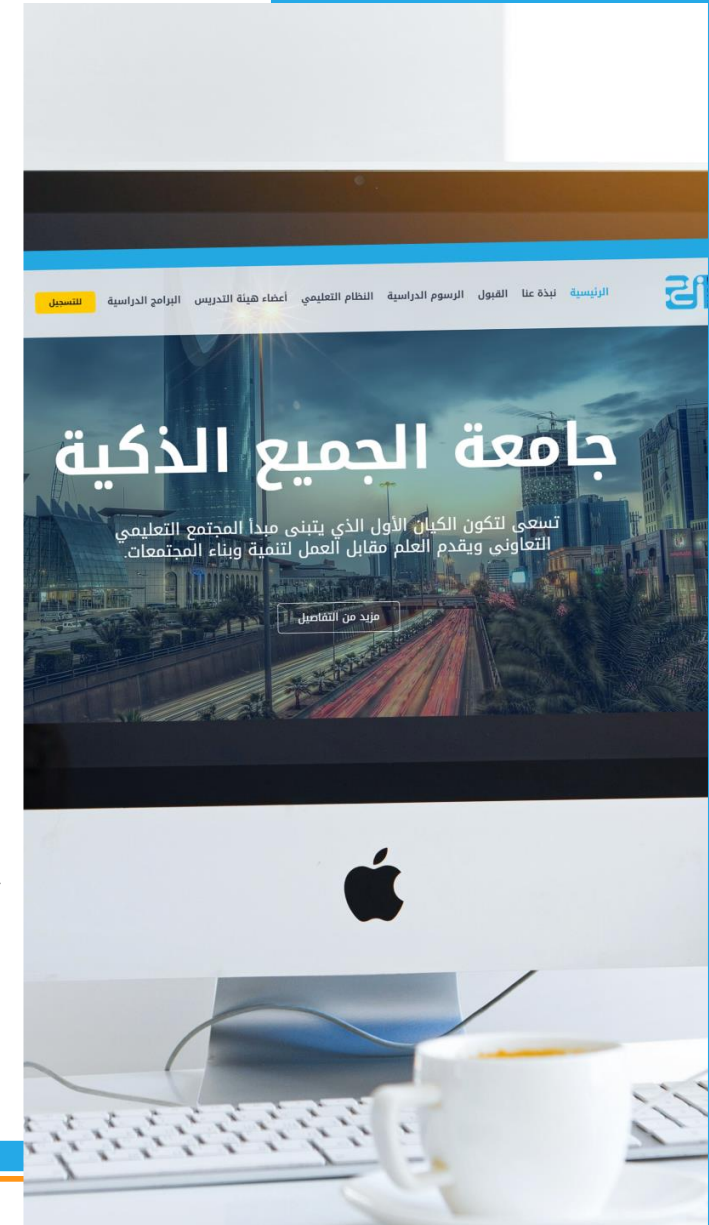
Lecture – 5

Activity

Snort and Firewall Rules

In this lab, you will complete the following objectives:

- Perform live monitoring of IDS and events.
- Configure your own customized firewall rule to stop internal hosts from contacting a malware-hosting server.
- Craft a malicious packet and launch it against an internal target.
- Create a customized IDS rule to detect the customized attack and issue an alert based on it.



Thanks

