Module 8: Endpoint Protection and Vulnerability Assessment

Module Objectives

Module Title: Endpoint Protection and Vulnerability Assessment

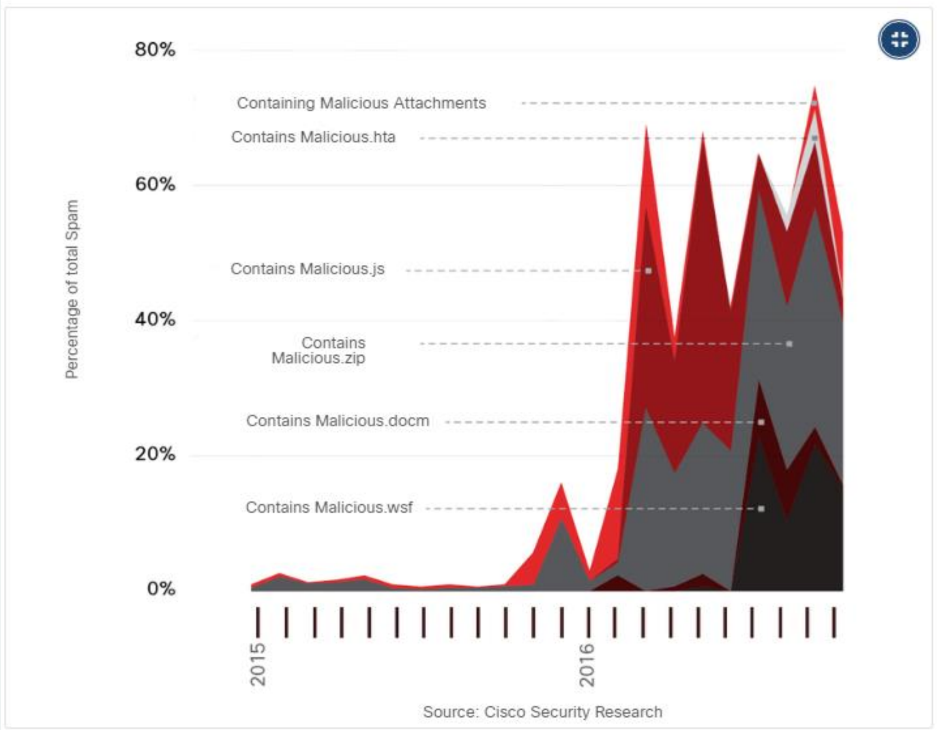
Module Objective: Explain how endpoint vulnerabilities are assessed and managed.

Topic Title	Topic Objective
Antimalware Protection	Explain methods of mitigating 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.
Secure Device Management	Explain how secure device management techniques are used to protect data and assets.
Information Security Management Systems	Explain how information security management systems are used to protect assets.

Endpoint Protection

Endpoint Threats

- Endpoints can be defined as hosts on the network that can access or be accessed by other hosts on the network.
- Each endpoint is potentially a way for malicious software to gain access to a network.
- Devices that remotely access networks through VPNs are also endpoints that could inject malware into the VPN network from the public network.
- Several common types of malware have been found to significantly change features in less than 24 hours in order to evade detection.



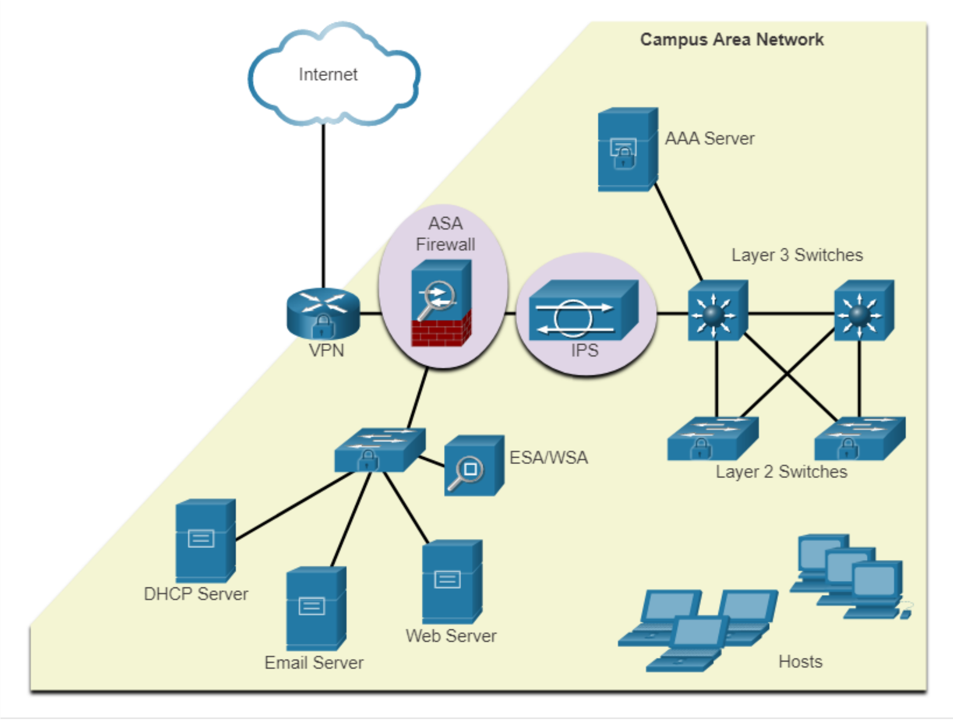
Source: Cisco Security Research

Malicious Spam Percentage

Endpoint Protection

Endpoint Security

- 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



Endpoint Protection

Host-Based Malware Protection

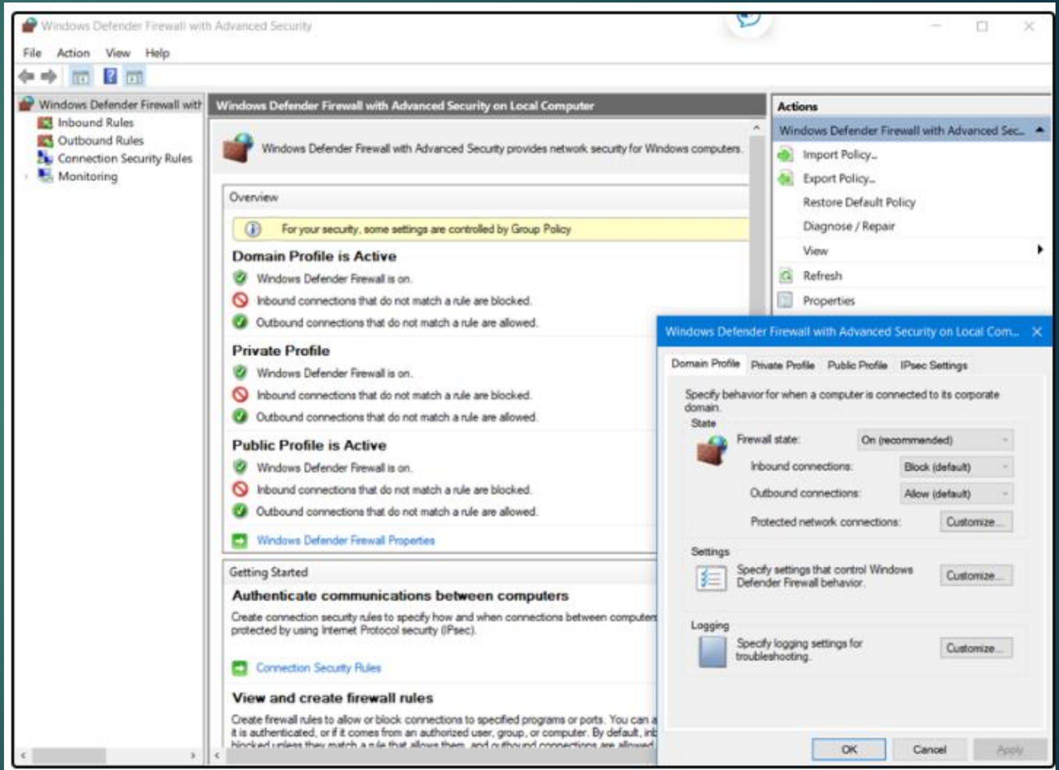
- Host-based antimalware/antivirus software and host-based firewalls are used to protect mobile devices using VPN.
- **Antivirus/Antimalware Software:** It is a software that is installed on a host to detect and mitigate viruses and malware. For example, Windows Defender Virus & Threat Protection, Cisco 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.

Endpoint Protection

Host-Based Malware Protection (Contd.)

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.



Windows Defender Firewall with Advanced Security on Local Computer

Windows Defender Firewall with Advanced Security provides network security for Windows computers.

Overview

For your security, some settings are controlled by Group Policy

Domain Profile is Active
- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Private Profile
- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Public Profile is Active
- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Windows Defender Firewall Properties

Getting Started

Authenticate communications between computers

Create connection security rules to specify how and when connections between computer protected by using Internet Protocol security (IPsec).

Connection Security Rules

View and create firewall rules

Create firewall rules to allow or block connections to specified programs or ports. You can a it is authenticated, or if it comes from an authorized user, group, or computer. By default, in blocked unless they match a rule that allows them, and outbound connections are allowed.

Windows Defender Firewall with Advanced Security on Local Com...

Domain Profile | Private Profile | Public Profile | IPsec Settings

Specify behavior for when a computer is connected to its corporate domain.

State
- Firewall state: On (recommended)
- Inbound connections: Block (default)
- Outbound connections: Allow (default)
- Protected network connections: Customize...

Settings
- Specify settings that control Windows Defender Firewall behavior. Customize...

Logging
- Specify logging settings for troubleshooting. Customize...

Endpoint Protection

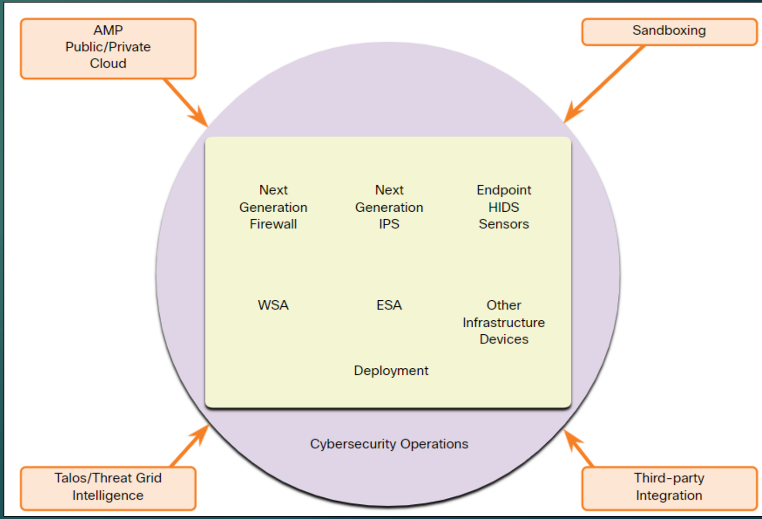
Host-Based Malware Protection (Contd.)

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.
- AV-TEST | Antivirus & Security Software & AntiMalware Reviews

Network-Based Malware Protection (Contd.)

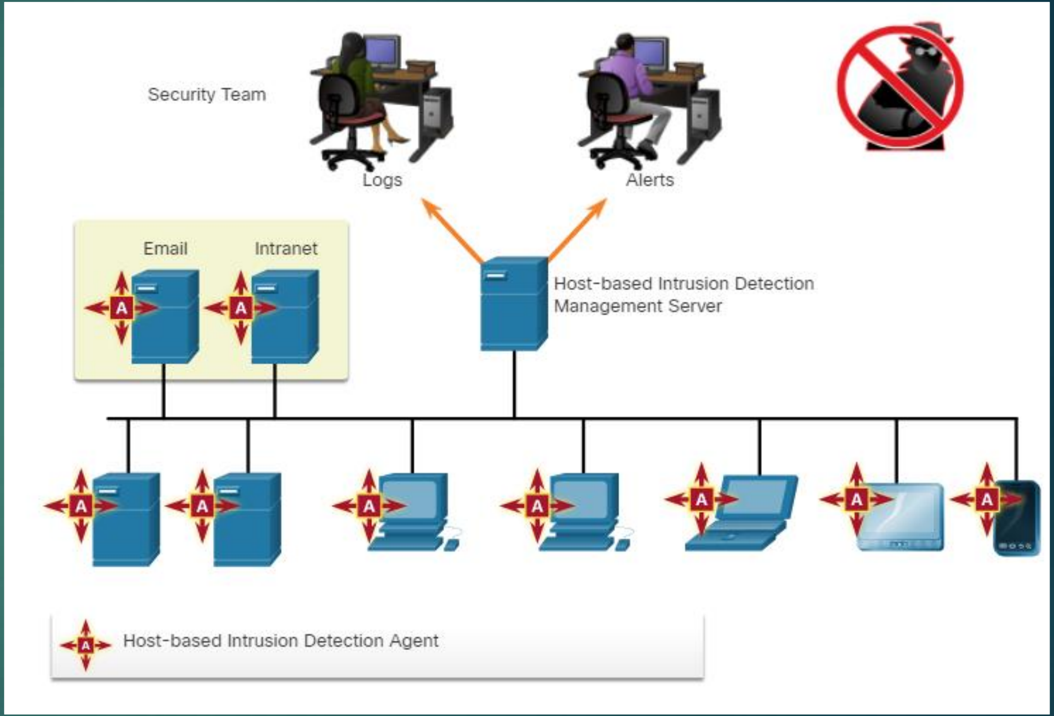
- Network-based malware prevention devices are capable of sharing information among themselves to make better informed decisions.
- Protecting endpoints in a borderless network can be accomplished using network-based, as well as host-based techniques.
- Some examples of devices and techniques that implement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


Security Team
Logs
Alerts
Email
Intranet
Host-based Intrusion Detection Management Server
A
Host-based Intrusion Detection Agent

Host-based Intrusion Detection Architecture

Host-Based Intrusion Protection

HIDS Operation

- 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.
- 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.

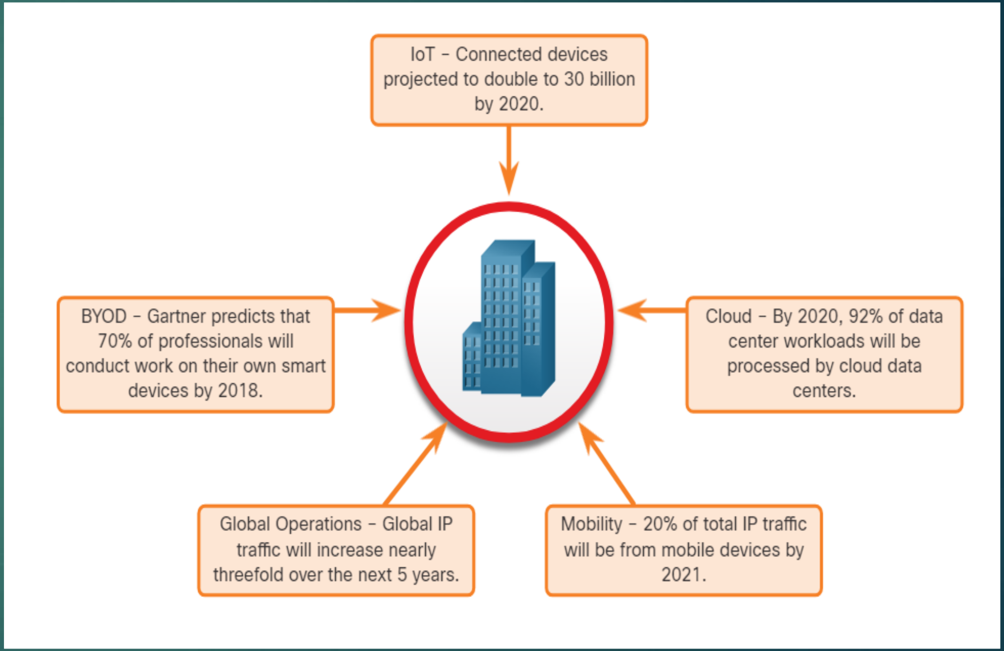
Host-Based Intrusion Protection

HIDS Products

- Most of the HIDS utilize software on the host and some sort of centralized security management functionality that allows integration with network security monitoring services and threat intelligence.
- Some examples are Cisco AMP, AlienVault USM, Tripwire, and Open Source HIDS SECurity (OSSEC).
- OSSEC uses a central manager server and agents that are installed on individual hosts.
- The OSSEC server, or Manager, can also receive and analyze alerts from a variety of network devices and firewalls over syslog.
- OSSEC monitors system logs on hosts and also conducts file integrity checking.
- OSSEC - World's Most Widely Used Host Intrusion Detection System - HIDS

Attack Surface

- **An attack surface** is the total sum of the vulnerabilities in a given 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.



IoT – Connected devices projected to double to 30 billion by 2020.

BYOD – Gartner predicts that 70% of professionals will conduct work on their own smart devices by 2018.

Cloud – By 2020, 92% of data center workloads will be processed by cloud data centers.

Global Operations – Global IP traffic will increase nearly threefold over the next 5 years.

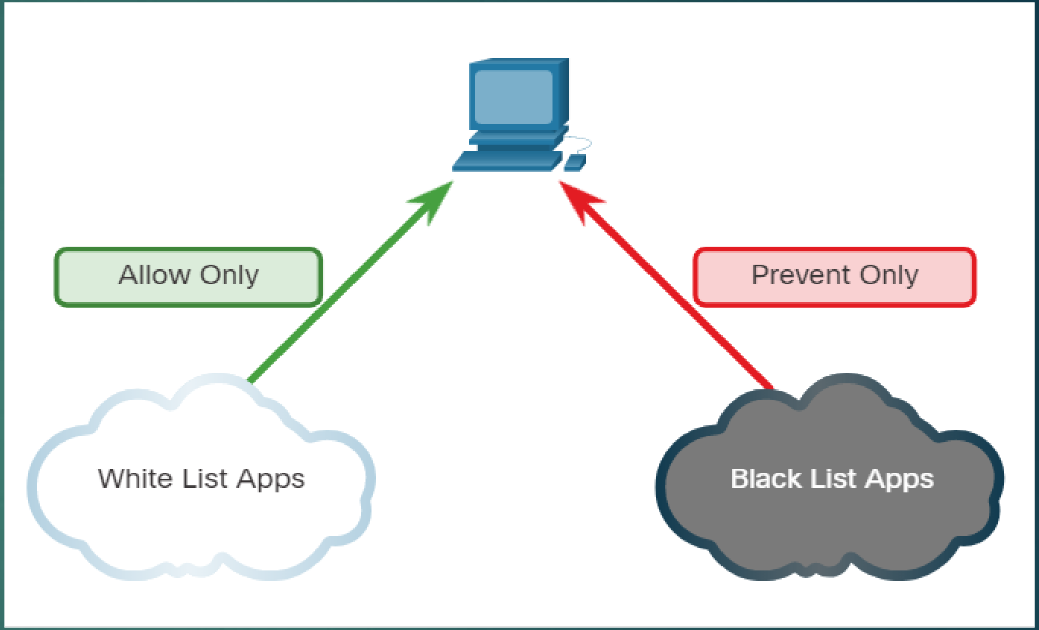
Mobility – 20% of total IP traffic will be from mobile devices by 2021.

An Expanding Attack Surface

Application Security

Application Blacklisting and Whitelisting

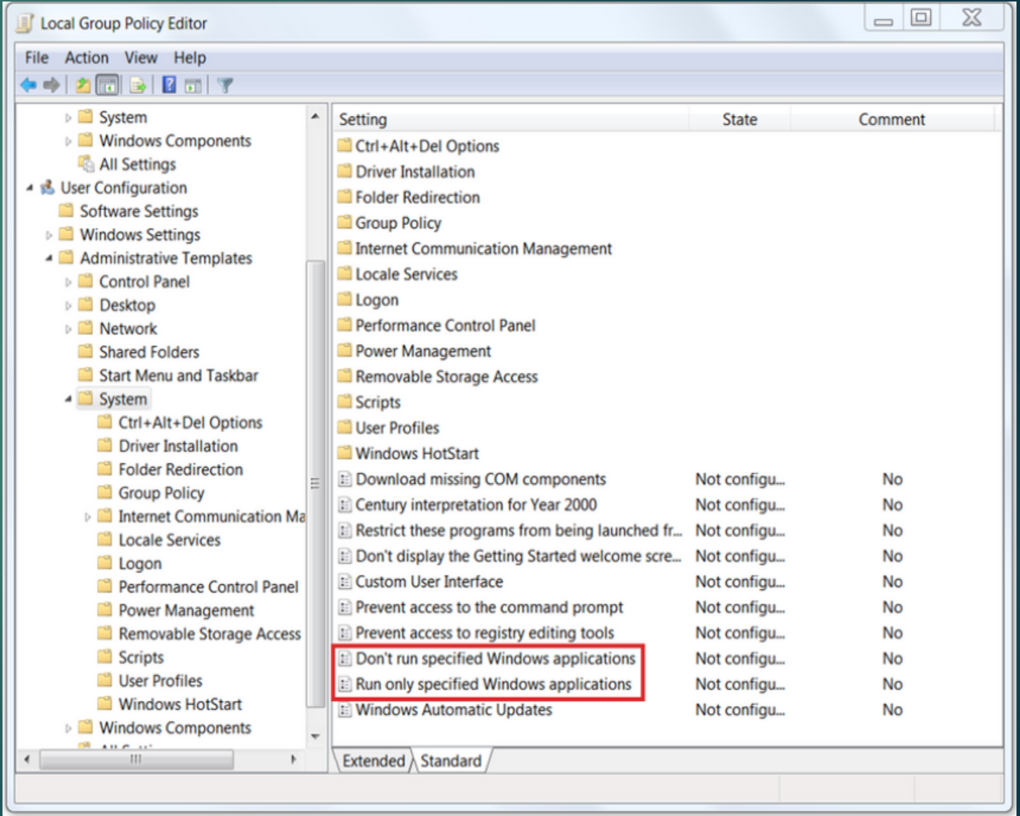
- Limiting access to potential threats by creating lists of prohibited applications is known as blacklisting.
- Application blacklists can dictate which user applications are not permitted to run on a computer.
- Whitelists specify which programs are allowed to run.
- In this way, known vulnerable applications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



Application Blacklisting and Whitelisting

Application Blacklisting and Whitelisting (Contd.)

- 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.
- Spamhaus is the world leader in supplying realtime highly accurate threat intelligence to the Internet's major networks.
- The Spamhaus Project

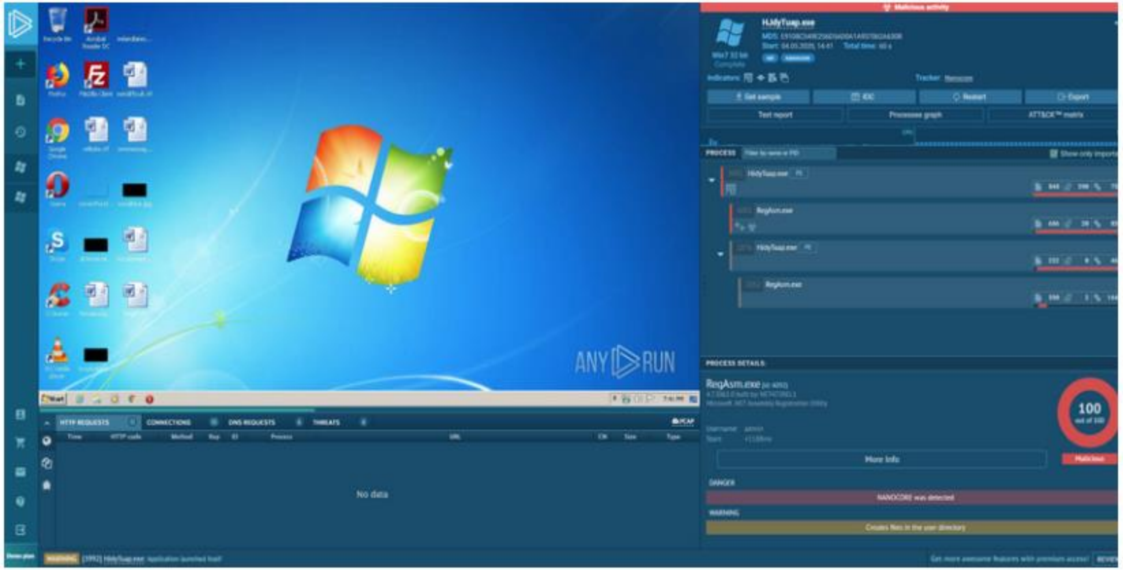


Setting	State	Comment
Ctrl+Alt+Del Options		
Driver Installation		
Folder Redirection		
Group Policy		
Internet Communication Management		
Locale Services		
Logon		
Performance Control Panel		
Power Management		
Removable Storage Access		
Scripts		
User Profiles		
Windows HotStart		
Download missing COM components	Not configu...	No
Century interpretation for Year 2000	Not configu...	No
Restrict these programs from being launched fr...	Not configu...	No
Don't display the Getting Started welcome scre...	Not configu...	No
Custom User Interface	Not configu...	No
Prevent access to the command prompt	Not configu...	No
Prevent access to registry editing tools	Not configu...	No
Don't run specified Windows applications	Not configu...	No
Run only specified Windows applications	Not configu...	No
Windows Automatic Updates	Not configu...	No

Application Security

System-Based Sandboxing

- 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.
- Cuckoo Sandbox - Automated Malware Analysis
- ANY.RUN is an online tool that offers the ability to upload a malware sample for analysis like any online sandbox.
- ANY.RUN - Interactive Online Malware Sandbox



Application Security

Video - Using a Sandbox to Launch Malware

- Play the video to view a demonstration of using sandbox environment to launch and analyze a malware attack.

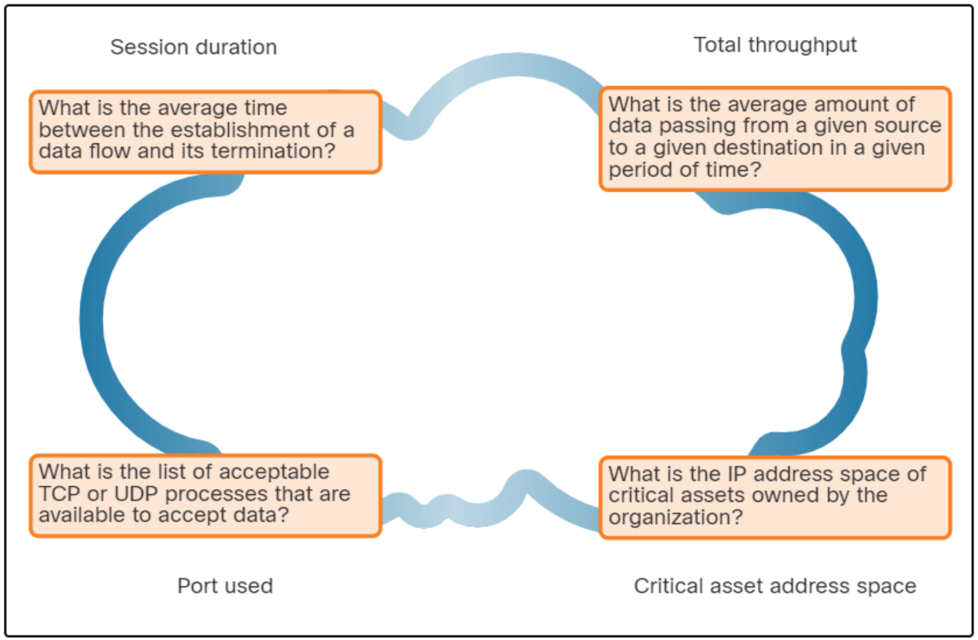
Malware Detected

Windows Security is taking action to clean detected malware.

Network and Server Profiling

Network 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

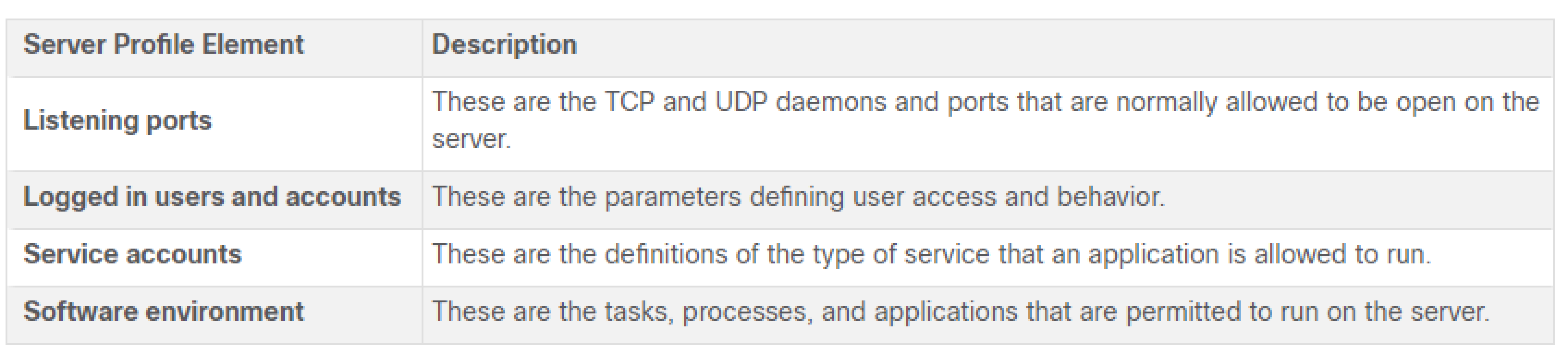


Session duration
What is the average time between the establishment of a data flow and its termination?
Total throughput
What is the average amount of data passing from a given source to a given destination in a given period of time?
What is the list of acceptable TCP or UDP processes that are available to accept data?
What is the IP address space of critical assets owned by the organization?
Port used
Critical asset address space

Elements of a Network Profile

Server Profiling

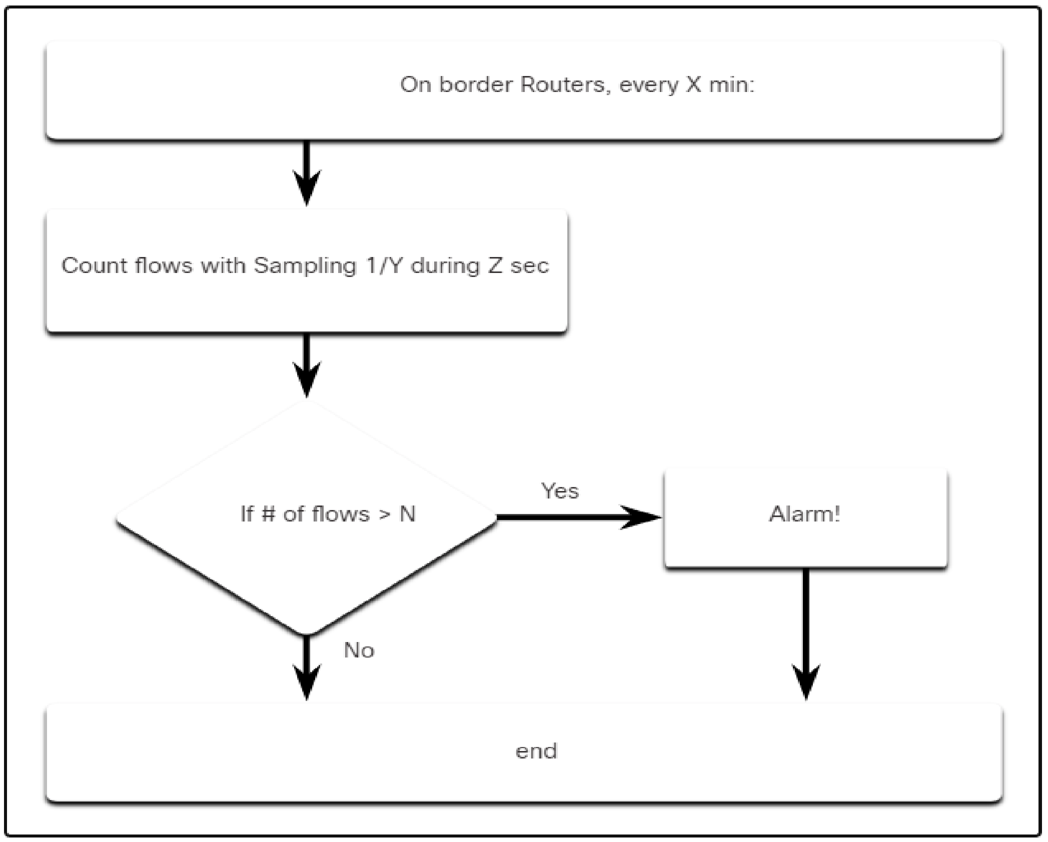
- A server profile is a security baseline for a given server.
- Server profiling is used to establish the accepted operating state of servers.
- The server profile elements are as follows:



Server Profile Element	Description
Listening ports	These are the TCP and UDP daemons and ports that are normally allowed to be open on the server.
Logged in users and accounts	These are the parameters defining user access and behavior.
Service accounts	These are the definitions of the type of service that an application is allowed to run.
Software environment	These are the tasks, processes, and applications that are permitted to run on the server.

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.
- 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.


On border Routers, every X min:
Count flows with Sampling 1/Y during Z sec
If # of flows > N
Yes
Alarm!
No
end

Network and Server Profiling

Network Vulnerability Testing

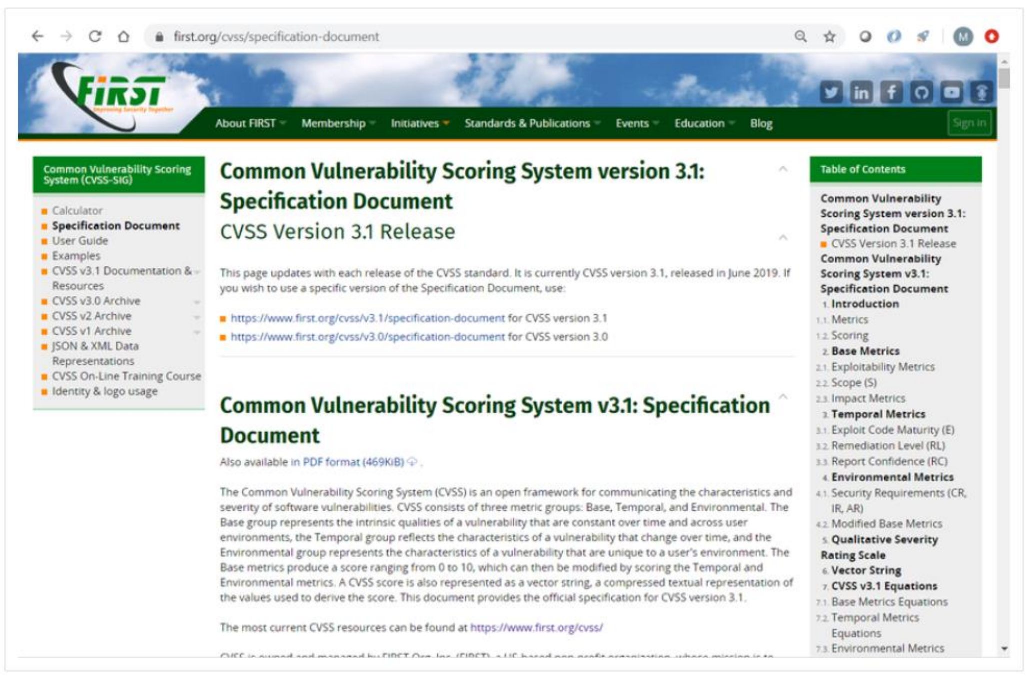
- Network Vulnerability Testing includes Risk Analysis, Vulnerability Assessment and Penetration Testing.
- The table lists examples of activities and tools that are used in vulnerability testing:

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)

CVSS Overview

- 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.
- Common Vulnerability Scoring System SIG (first.org)



Common Vulnerability Scoring System version 3.1: Specification Document

CVSS Version 3.1 Release

This page updates with each release of the CVSS standard. It is currently CVSS version 3.1, released in June 2019. If you wish to use a specific version of the Specification Document, use:

- https://www.first.org/cvss/v3.1/specification-document for CVSS version 3.1
- https://www.first.org/cvss/v3.0/specification-document for CVSS version 3.0

Common Vulnerability Scoring System v3.1: Specification Document

Also available in PDF format (469KiB).

The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base group represents the intrinsic qualities of a vulnerability that are constant over time and across user environments, the Temporal group reflects the characteristics of a vulnerability that change over time, and the Environmental group represents the characteristics of a vulnerability that are unique to a user's environment. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score. This document provides the official specification for CVSS version 3.1.

The most current CVSS resources can be found at https://www.first.org/cvss/

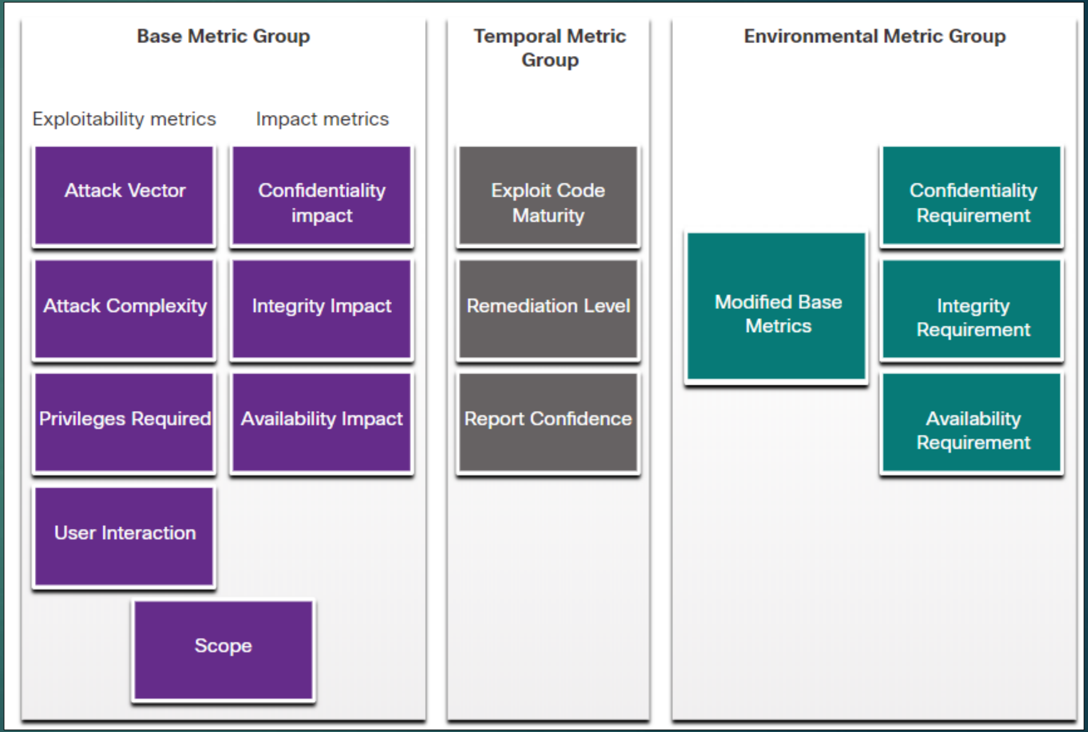
CVSS is owned and managed by FIRST.Org, Inc. (FIRST), a US-based non-profit organization, whose mission is to

Table of Contents

Common Vulnerability Scoring System (CVSS)

CVSS Metric Groups

- 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.



Base Metric Group

Exploitability metrics

Attack Vector

Attack Complexity

Privileges Required

User Interaction

Impact metrics

Confidentiality impact

Integrity Impact

Availability Impact

Scope

Temporal Metric Group

Exploit Code Maturity

Remediation Level

Report Confidence

Environmental Metric Group

Modified Base Metrics

Confidentiality Requirement

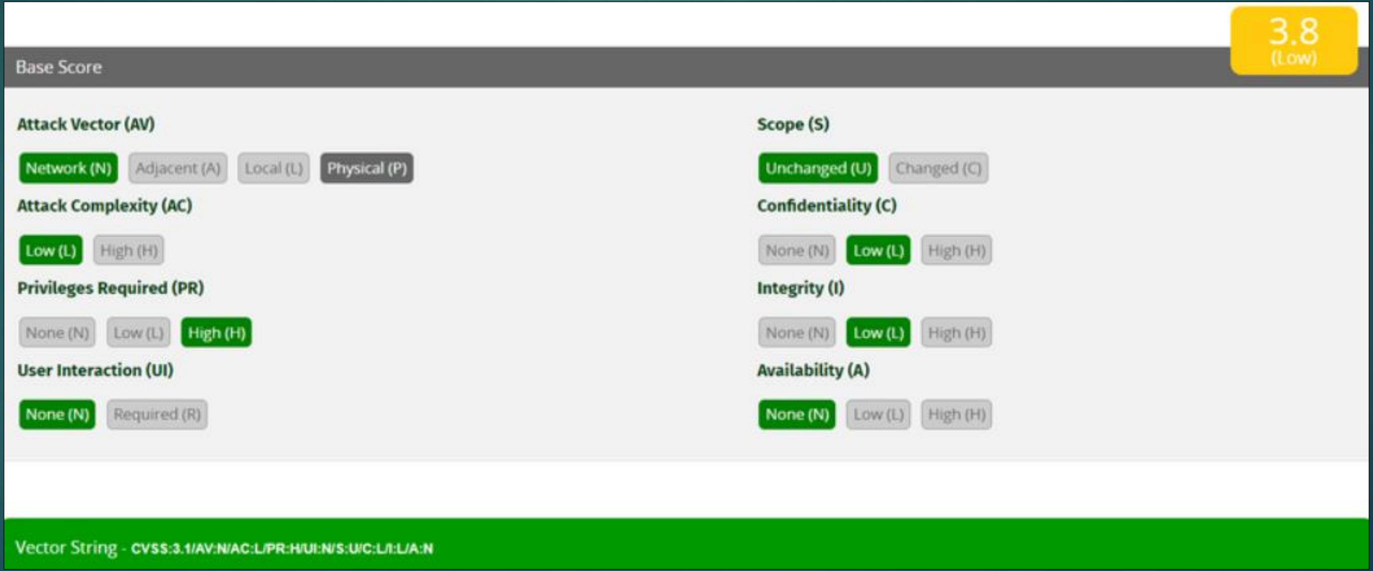
Integrity Requirement

Availability Requirement

Common Vulnerability Scoring System (CVSS)

The CVSS Process

- 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.



3.8
(Low)

Base Score

Attack Vector (AV)
[✓ Network (N)] Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC)
[✓ Low (L)] High (H)

Privileges Required (PR)
None (N) Low (L) [✓ High (H)]

User Interaction (UI)
[✓ None (N)] Required (R)

Scope (S)
[✓ Unchanged (U)] Changed (C)

Confidentiality (C)
None (N) [✓ Low (L)] High (H)

Integrity (I)
None (N) [✓ Low (L)] High (H)

Availability (A)
[✓ None (N)] Low (L) High (H)

Vector String - CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N

Common Vulnerability Scoring System (CVSS)

CVSS Reports

- 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:

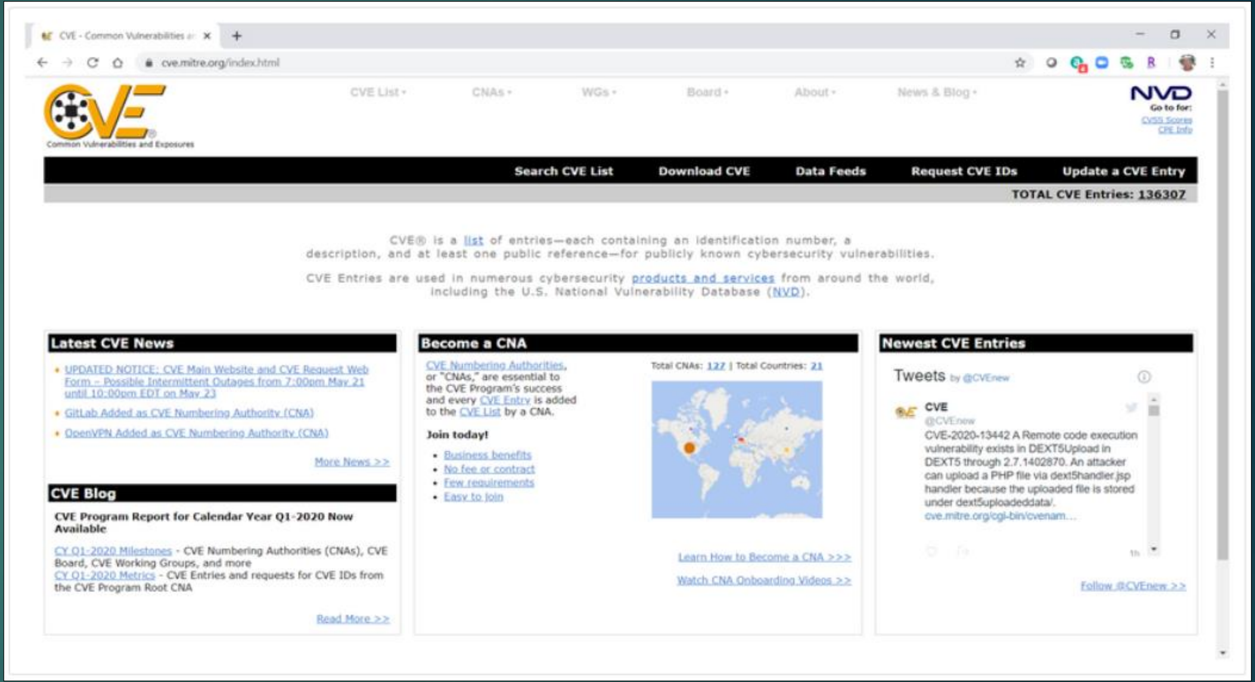
Rating	CVSS Score
None	0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

Common Vulnerability Scoring System (CVSS)

Other Vulnerability Information Sources

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.



TOTAL CVE Entries: 136307

CVE® is a list of entries—each containing an identification number, a description, and at least one public reference—for publicly known cybersecurity vulnerabilities.

CVE Entries are used in numerous cybersecurity products and services from around the world, including the U.S. National Vulnerability Database (NVD).

Latest CVE News

- UPDATED NOTICE: CVE Main Website and CVE Request Web Form – Possible Intermittent Outages from 7:00pm May 21 until 10:00pm EDT on May 23
- GitLab Added as CVE Numbering Authority (CNA)
- OpenVPN Added as CVE Numbering Authority (CNA)

More News >>

CVE Blog

CVE Program Report for Calendar Year Q1-2020 Now Available

CY Q1-2020 Milestones - CVE Numbering Authorities (CNAs), CVE Board, CVE Working Groups, and more
CY Q1-2020 Metrics - CVE Entries and requests for CVE IDs from the CVE Program Root CNA

Read More >>

Become a CNA

CVE Numbering Authorities, or "CNAs," are essential to the CVE Program's success and every CVE Entry is added to the CVE List by a CNA.

Join today!

- Business benefits
- No fee or contract
- Few requirements
- Easy to join

Total CNAs: 127 | Total Countries: 21

Learn How to Become a CNA >>>

Watch CNA Onboarding Videos >>

Newest CVE Entries

Tweets by @CVEnew

CVE
@CVEnew
CVE-2020-13442 A Remote code execution vulnerability exists in DEXT5Upload in DEXT5 through 2.7.1402870. An attacker can upload a PHP file via dext5handler.jsp handler because the uploaded file is stored under dext5uploadeddata/.
cve.mitre.org/cgi-bin/cvenam...
1h

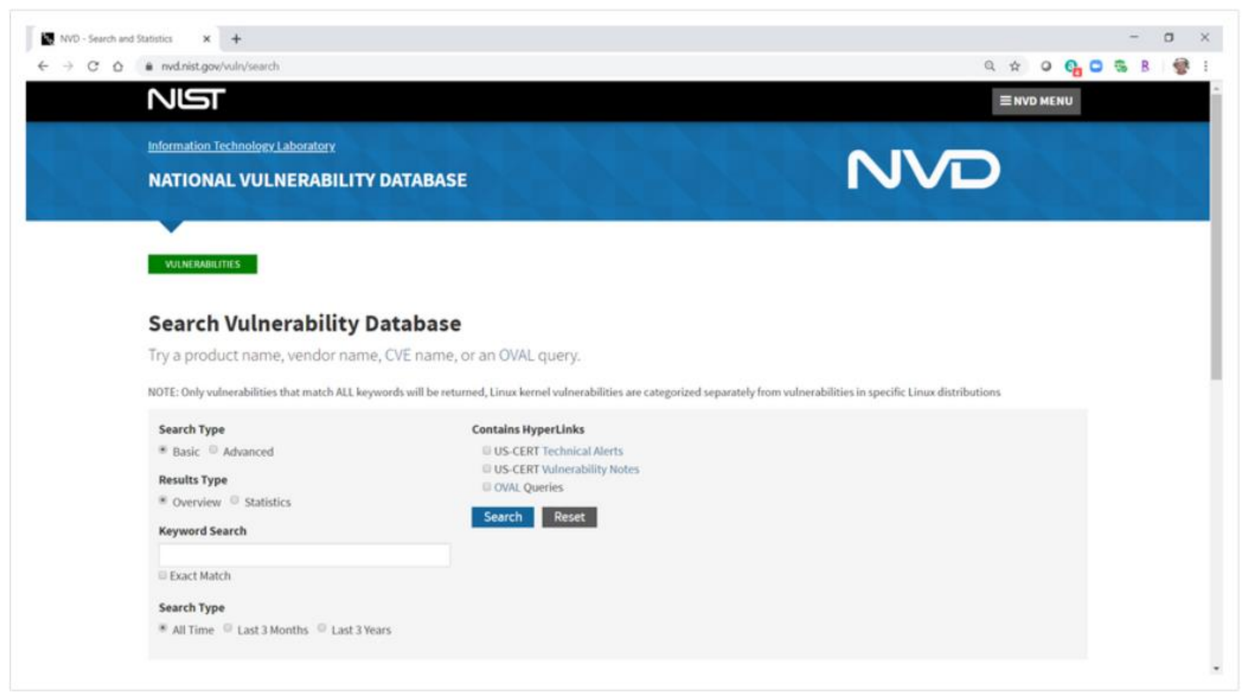
Follow @CVEnew >>

Common Vulnerability Scoring System (CVSS)

Other Vulnerability Information Sources (Contd.)

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.


NVD - Search and Statistics
nvd.nist.gov/vuln/search
NIST
☰ NVD MENU
Information Technology Laboratory
NATIONAL VULNERABILITY DATABASE
NVD
VULNERABILITIES

Search Vulnerability Database

Try a product name, vendor name, CVE name, or an OVAL query.

NOTE: Only vulnerabilities that match ALL keywords will be returned, Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions

Search Type
● Basic ○ Advanced

Results Type
● Overview ○ Statistics

Keyword Search

□ Exact Match

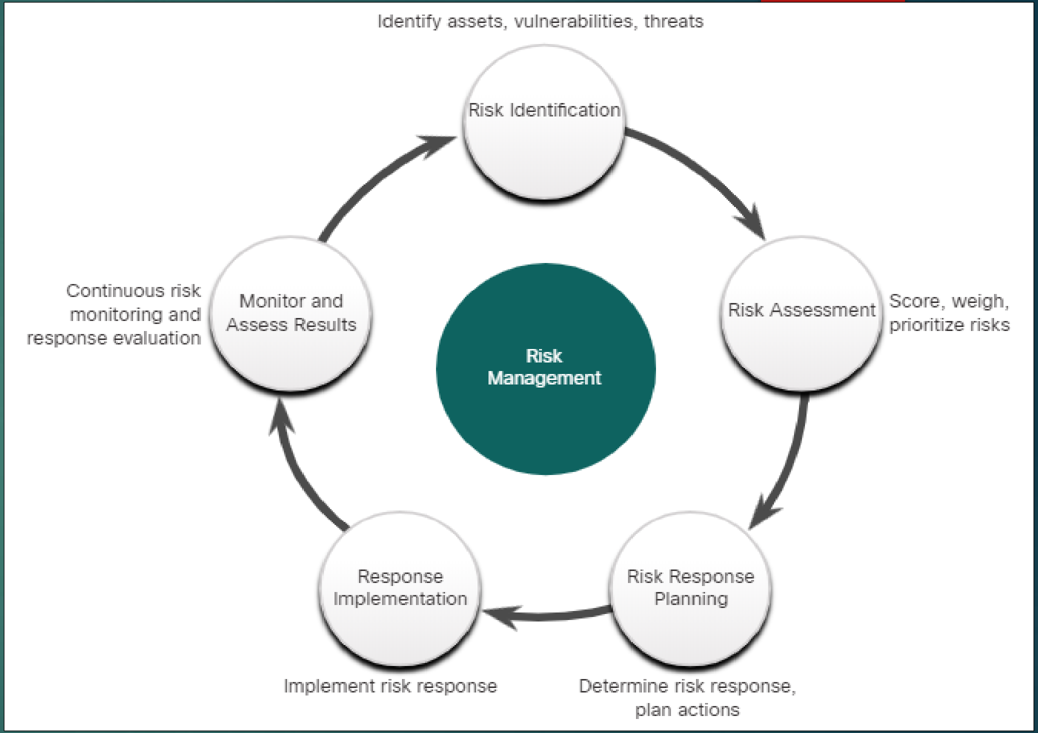
Search Type
● All Time ○ Last 3 Months ○ Last 3 Years

Contains HyperLinks
□ US-CERT Technical Alerts
□ US-CERT Vulnerability Notes
□ OVAL Queries

Search Reset

Risk Management

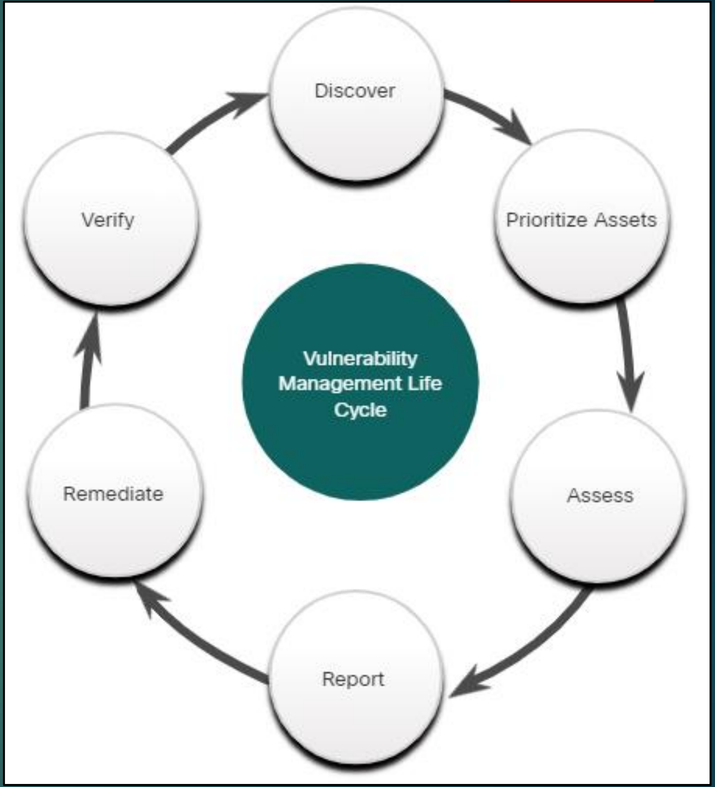
- Risk management involves the selection and specification of security controls for an organization.
- A mandatory activity in risk assessment is to identify threats and vulnerabilities.
- Ways to respond to identified risks:
  - **Risk avoidance** - Stop performing the activities that create risk.
  - **Risk reduction** - Take measures to reduce vulnerability.
  - **Risk sharing** - Shift some risk to other parties.
  - **Risk retention** - Accept the risk and its consequences.


Identify assets, vulnerabilities, threats
Risk Identification
Risk Assessment
Score, weigh, prioritize risks
Risk Management
Risk Response Planning
Determine risk response, plan actions
Response Implementation
Implement risk response
Monitor and Assess Results
Continuous risk monitoring and response evaluation

Secure Device Management

Vulnerability Management

- Vulnerability management is a security practice designed to proactively prevent the exploitation of IT vulnerabilities.
- The steps in the Vulnerability Management Life Cycle:
  - **Discover** - Develop a network baseline. Identify security vulnerabilities on a regular automated schedule.
  - **Prioritize Assets** - Categorize assets into groups or business units, and assign a business value based on their criticality to business operations.
  - **Assess** - Determine a baseline risk profile to eliminate risks based on asset criticality, vulnerability, threats, and asset classification.
  - **Report** - Measure the level of business risk associated with your assets according to your security policies. Document a security plan, monitor suspicious activity, and describe known vulnerabilities.
  - **Remediate** - Prioritize according to business risk and address vulnerabilities in order of risk.
  - **Verify** - Verify that threats have been eliminated through follow-up audits.

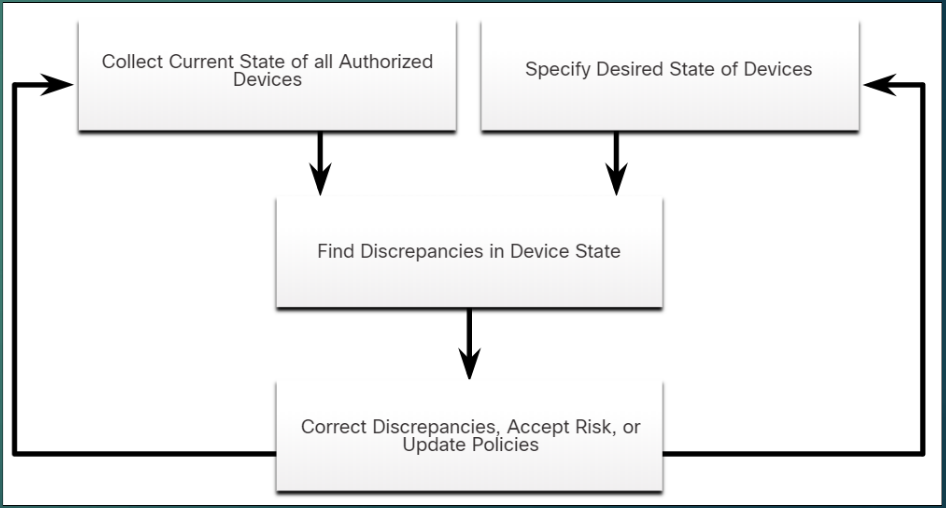


Secure Device Management

Asset Management

- Asset management involves the implementation of systems that track the location and configuration of networked devices and software across an enterprise.

- Tools and Techniques for Asset management:
  - Automated discovery and inventory of the actual state of devices
  - Articulation of the desired state for those devices using policies, plans, and procedures in the organization’s information security plan
  - Identification of non-compliant authorized assets
  - Remediation or acceptance of device state, possible iteration of desired state definition
  - Repeat the process at regular or ongoing intervals


Collect Current State of all Authorized Devices

Specify Desired State of Devices

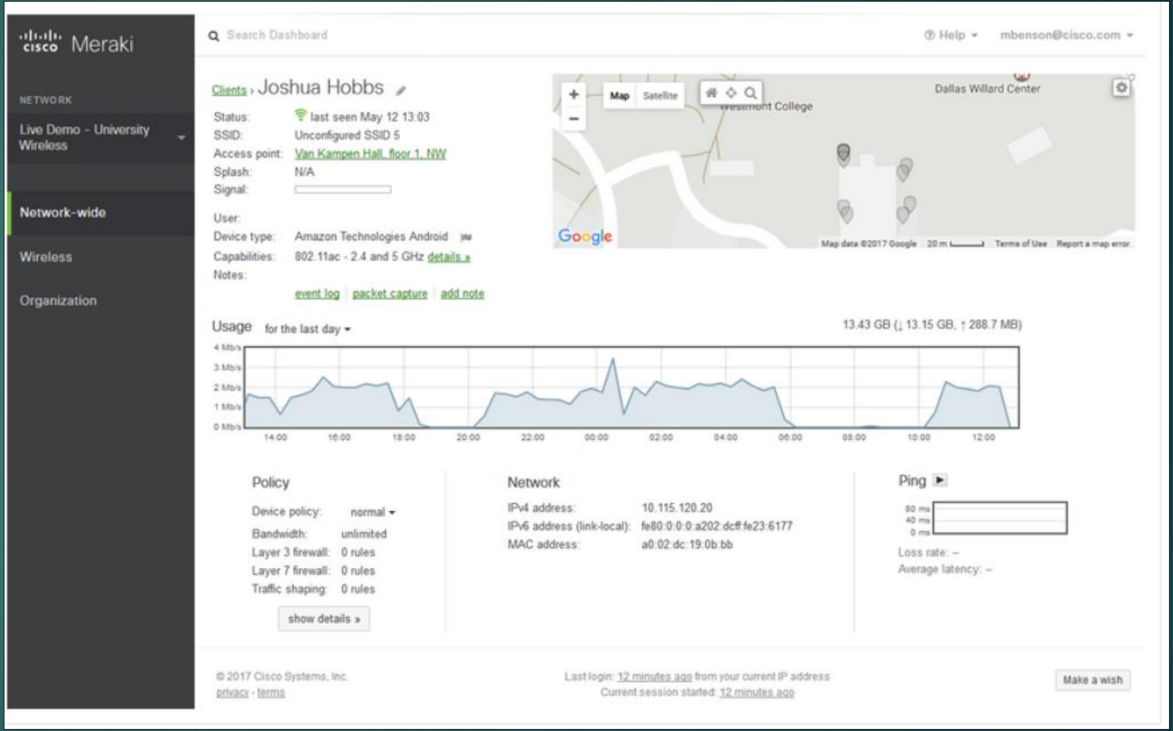
Find Discrepancies in Device State

Correct Discrepancies, Accept Risk, or Update Policies

Secure Device Management

Mobile Device Management

- Mobile devices cannot be physically controlled on the premises of an organization.
- MDM systems, such as Cisco Meraki Systems Manager, allows the security personnel to configure, monitor and update a very diverse set of mobile clients from the cloud.



Clients › Joshua Hobbs

Status: last seen May 12 13:03
SSID: Unconfigured SSID 5
Access point: Van Kampen Hall, floor 1, NW
Splash: N/A
Signal:

User:
Device type: Amazon Technologies Android
Capabilities: 802.11ac - 2.4 and 5 GHz details »
Notes:

event log | packet capture | add note

Usage for the last day

13.43 GB (↓ 13.15 GB, ↑ 288.7 MB)

Policy

Device policy: normal
Bandwidth: unlimited
Layer 3 firewall: 0 rules
Layer 7 firewall: 0 rules
Traffic shaping: 0 rules

Network

IPv4 address: 10.115.120.20
IPv6 address (link-local): fe80:0:0:0:a202:dcff:fe23:6177
MAC address: a0:02:dc:19:0b:bb

Ping

Loss rate: –
Average latency: –

© 2017 Cisco Systems, Inc.
privacy - terms

Last login: 12 minutes ago from your current IP address
Current session started: 12 minutes ago

Secure Device Management

Configuration Management

- **Configuration Management**: As defined by NIST, configuration management:

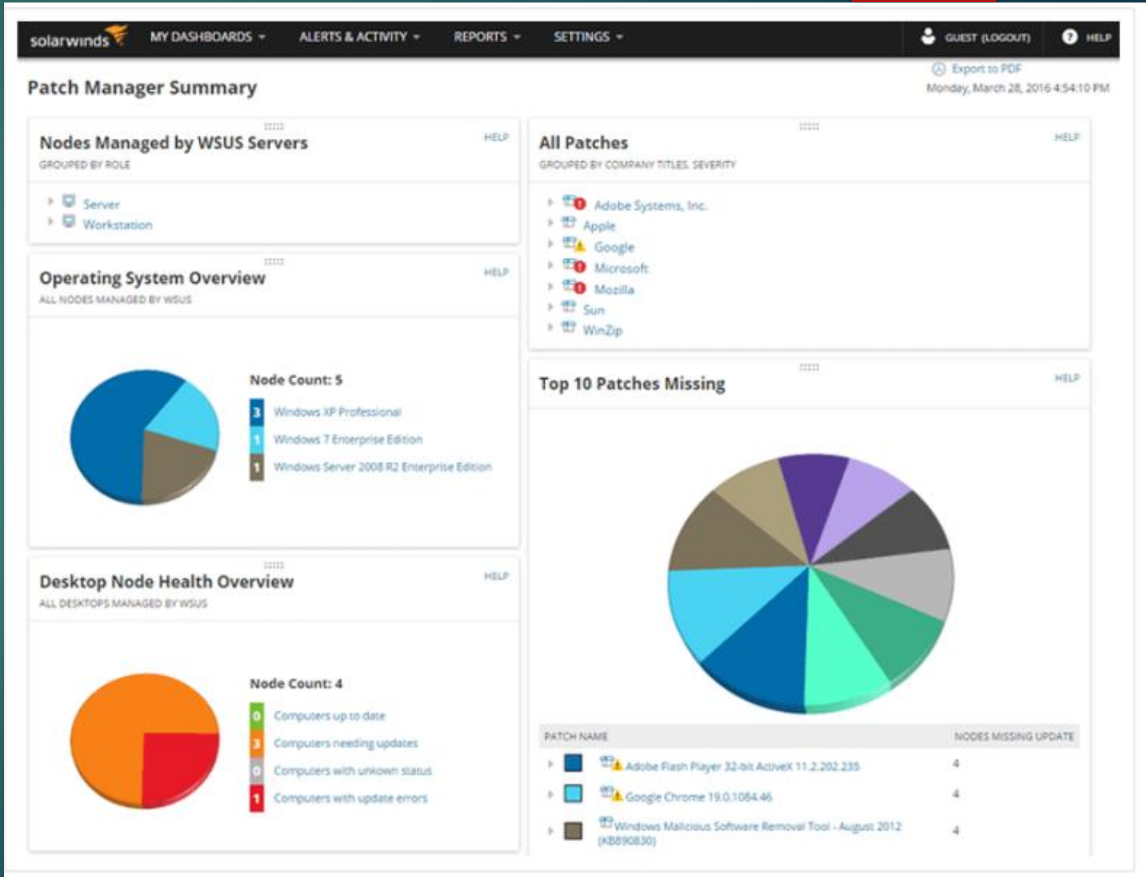
  Comprises a collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configurations of those products and systems.

- For internetworking devices, software tools are available that will backup configurations, detect changes in configuration files, and enable bulk change of configurations across a number of devices.
- With the advent of cloud data centers and virtualization, management of numerous servers presents special challenges. Tools like Puppet, Chef, Ansible, and SaltStack enable efficient management of servers that are used in cloud-based computing.

Secure Device Management

Enterprise Patch Management

- Patch management involves all aspects of software patching, including identifying required patches, acquiring, distributing, installing, and verifying.
- Patch management is required by some compliance regulations such as Sarbanes Oxley (SOX) and the Health Insurance Portability and Accountability Act (HIPAA).



Patch Manager Summary

Monday, March 28, 2016 4:54:10 PM

Nodes Managed by WSUS Servers

GROUPED BY ROLE

- Server
- Workstation

Operating System Overview

ALL NODES MANAGED BY WSUS

Node Count: 5

3	Windows XP Professional
1	Windows 7 Enterprise Edition
1	Windows Server 2008 R2 Enterprise Edition

Desktop Node Health Overview

ALL DESKTOPS MANAGED BY WSUS

Node Count: 4

0	Computers up to date
3	Computers needing updates
0	Computers with unkown status
1	Computers with update errors

All Patches

GROUPED BY COMPANY TITLES, SEVERITY

- Adobe Systems, Inc.
- Apple
- Google
- Microsoft
- Mozilla
- Sun
- WinZip

Top 10 Patches Missing

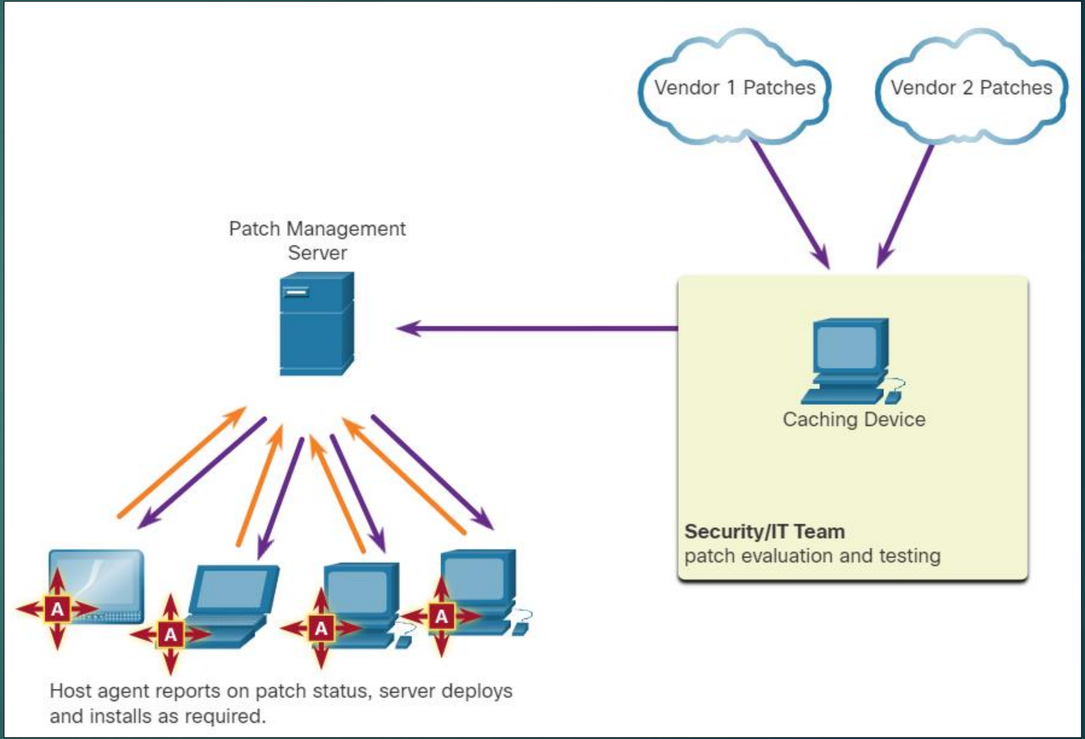
PATCH NAME	NODES MISSING UPDATE
Adobe Flash Player 32-bit ActiveX 11.2.202.235	4
Google Chrome 19.0.1084.46	4
Windows Malicious Software Removal Tool - August 2012 (KB890830)	4

Secure Device Management

Patch Management Techniques

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 and determines if patches exist that require installation, and installs the patches.
- Agent-based approaches are the preferred means of patching mobile devices.



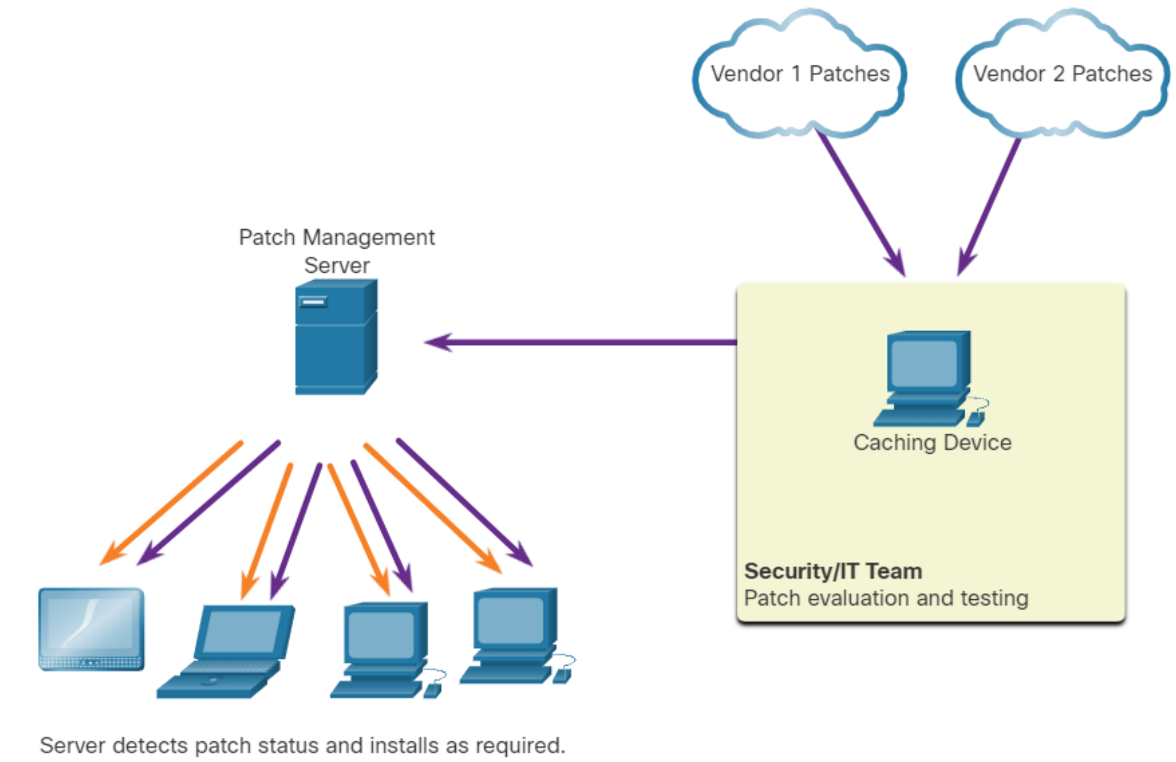
Host agent reports on patch status, server deploys and installs as required.

Secure Device Management

Patch Management Techniques

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, which can be a problem for mobile devices.

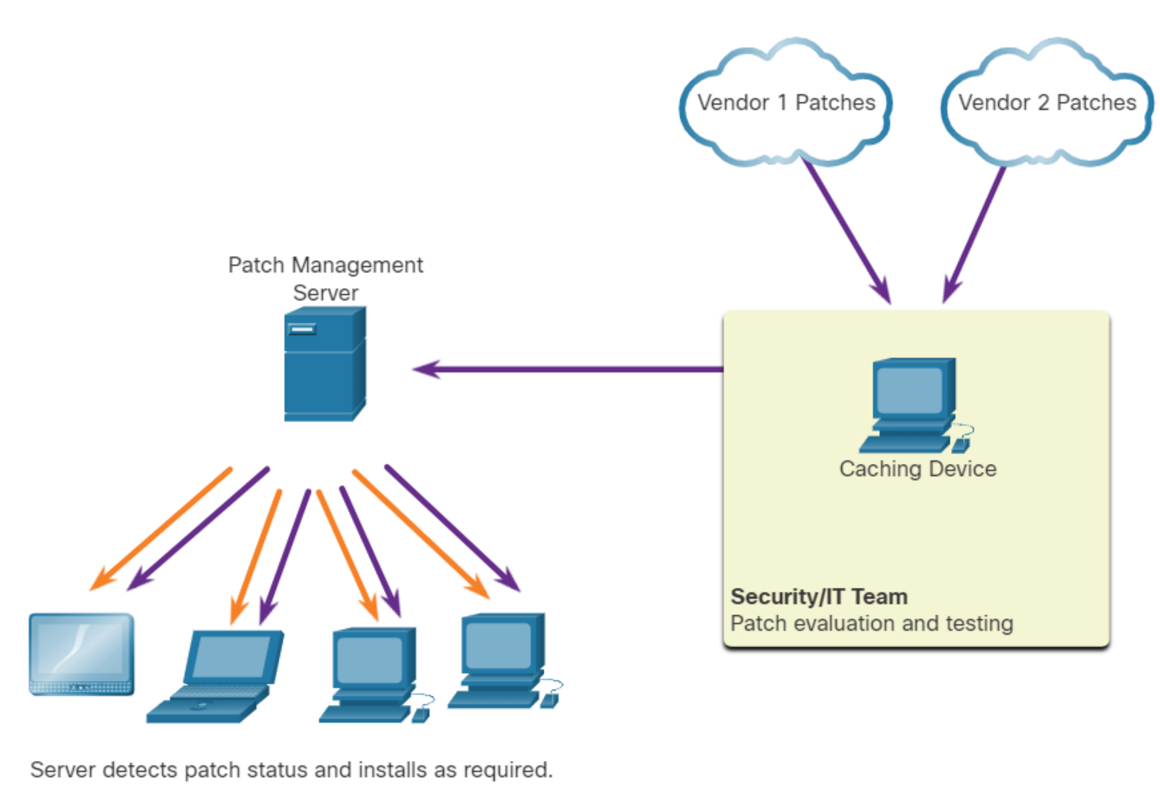


Server detects patch status and installs as required.

Patch Management Techniques

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.



Server detects patch status and installs as required.

Endpoint Protection Summary

What Did I Learn in this Module?

- Endpoints are defined as hosts on the network that can access or be accessed by other hosts on the network.
- There are two internal LAN elements to secure: Endpoints and Network Infrastructure.
- Antivirus/Antimalware Software is installed on a host to detect and mitigate viruses and malware.
- Host-based firewalls may use a set of predefined policies, or profiles, to control packets entering and leaving a computer.
- Some examples of host-based firewalls include Windows Defender Firewall, iptables, nftables, and TCP Wrappers.
- HIDS protects hosts against known and unknown malware.
- An attack surface is the total sum of the vulnerabilities in a given system that is accessible to an attacker.
- Application blacklists dictate which user applications are not permitted to run on a computer and whitelists specify which programs are allowed to run.

Endpoint Vulnerability Assessment

What Did I Learn in this Module?

- Network and device profiling provides statistical baseline information that can serve as a reference point for normal network and device performance.
- Network security can be evaluated using a variety of tools and services.
- Vulnerability assessment uses software to scan Internet-facing servers and internal networks for various types of vulnerabilities.
- 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.
- Vulnerabilities are rated according to the attack vector, attack complexity, privileges required, user interaction, and scope.
- Risk management involves the selection and specification of security controls for an organization.
- Vulnerability management is a security practice that is designed to proactively prevent the exploitation of IT vulnerabilities that exist within an organization.