5.1 VULNERABILITY SCANNING

- Vulnerability Scans
- Vulnerability Scanning Tools
- Scanner Output and Reports

ABOUT VULNERABILITIES

- A weakness that might be exploitable
- Can occur anywhere in the network:
  - People
  - Processes
  - Technology
- You can have vulnerabilities that you are not aware of
- You can have known vulnerabilities that no one has yet created an exploit for

VULNERABILITY CLASSIFICATIONS

- Misconfigurations
  - Not applying secure settings or configuring per best practices
  - No firewall, no anti-virus, etc.
- Leaving defaults in place
  - Configurations
  - Passwords
  - Services
- Buffer overflows
  - Not patching against known code weaknesses
- Unpatched systems
  - Not applying security updates from the vendor

VULNERABILITY CLASSIFICATIONS (CONT'D)

- Design flaws
  - Software that had a hurried development process with insufficient built-in security
- OS flaws
  - Vulnerabilities discovered in the operating system
- Application flaws
  - Vulnerabilities discovered in an application, or services that ship with an OS
- Open services
  - Services that freely permit client connections with no authentication or security controls
- User-based vulnerabilities
  - User susceptibility to social engineering, lack of training or awareness
- Process-based vulnerabilities
  - Security gaps in a business process that might allow exploitation by an attacker

VULNERABILITY SCANNING

- You can scan for vulnerabilities and/or compliance
- Should include both physical and virtual systems (VMs, containers)
- Tools are typically automated and include host discovery and port scanning as part of the scan
- Some tools only "rattle the door knob" to see if the vulnerability exists
  - They do not attempt to actually exploit the vulnerability
- Some tools also attempt to exploit the vulnerability and provide proof
  - Such as a stolen file, obtaining a shell (command prompt), etc.
- Most tools refer to discovered vulnerabilities by CVE number
  - They provide links to additional information and recommendations
- Most tools have reporting capabilities
- Some tools use standardized output that you can import into another tool for additional validation

VULNERABILITY SCANNING APPROACHES

- Passive scanning
  - Observation
  - Passive sniffing
- Active scanning
  - Send probes and specially crafted requests to targets
    - Host discovery – see what hosts are live
    - Port scan and service enumeration – see what open ports, services, and versions exist on the hosts
    - "Rattle the doorknob"
    - See if the OS or service responds in a way that suggests it is susceptible to a specific attack
    - Need not include actually launching the attack and compromising the device
      - That is usually done in a penetration test
- Credentialed scans
  - You provide the scanner with authentication credentials for the various systems it will scan
    - The scanner logs into the systems to retrieve their configuration information and log data
  - Uncredentialed scans are generally unable to detect many vulnerabilities on a device
    - The rely on external resources for configuration settings that can be altered or incorrect

VULNERABILITY SCANNING TOOL TYPES

- Host-based
  - OS
  - Services
  - Apps
  - Versions
  - Patch levels
  - Defaults and misconfigurations
- Network-based
  - Protocols
  - Ports
  - ACLs / firewall rules / IDS/IPS
- Cloud-based
  - Comprehensive solutions
  - Emulated attacks
  - Good for DevSecOps
  - Often use AI for advanced analysis
- Depth assessment
  - Fuzzers
  - Look for previously unknown vulnerabilities

CHARACTERISTICS OF A GOOD VULNERABILITY SCANNER

- Follows an inference-based approach
  - Assess vulnerabilities depending on the inventory of protocols in the environment
- Inventories protocols
- Detects open ports
- Identifies services behind the ports
- Checks for vulnerabilities
- Validates vulnerabilities
- Can be automated
- Signature database regularly updated
- Supports different network/host types
- Suggests proper remedies and workarounds
- Imitates outside attackers
- Creates actionable, customizable reports
- Includes trends and categorizes by severity

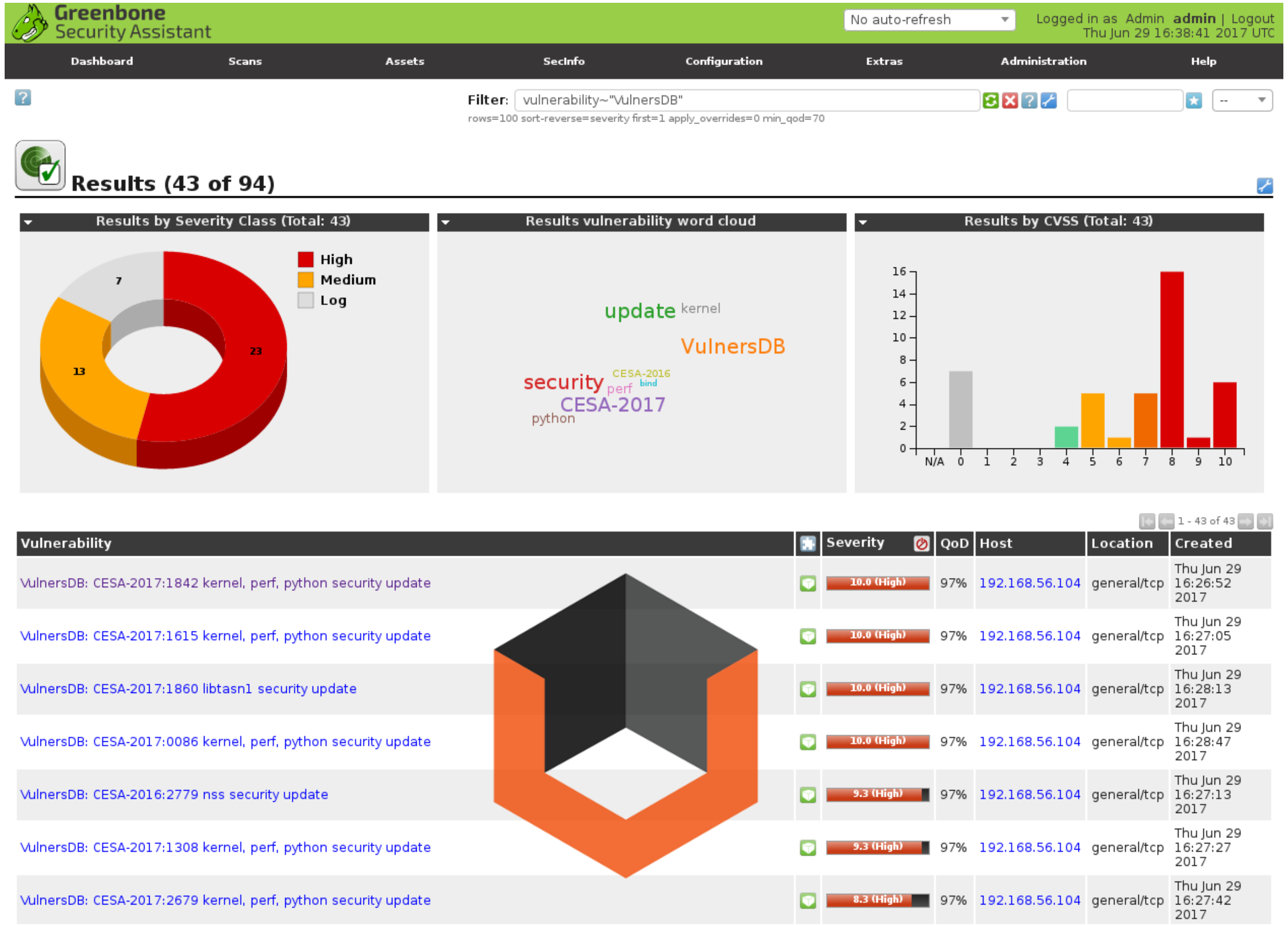
LIMITS OF VULNERABILITY SCANNERS

- Just a start
  - Only one part of a larger penetration test
- Tools only look for known signatures
- Automated tools can produce a lot of false positives
- Automated tools focus on technology
  - You will need a skilled pentester to also evaluate vulnerabilities in people and processes
- Requires a pen test to determine if the system can truly be compromised
- Can destabilize fragile systems/interfere with normal operations
- Likely to be incomplete if uncredentialed

POPULAR VULNERABILITY SCANNERS

- OpenVAS
- Tripwire IP360
- Nessus
- Nexpose
- Comodo HackerProof
- Vulnerability Manager Plus
- Nikto
- Retina
- ImmuniWeb
- SolarWinds
- Intruder
- Core Impact
- SecPod SanerNow
- ManageEngine
- Paessler
- CrowdStrike Falcon
- Kiuwan Code Security
- Acunetix
- Invicti
- Hakware Archangel
- Runecast Analyzer
- Astra Pentest
- Qualsys
- Aqua

VULNERABILITY SCANNER EXAMPLE



Filter: vulnerability~"VulnersDB"

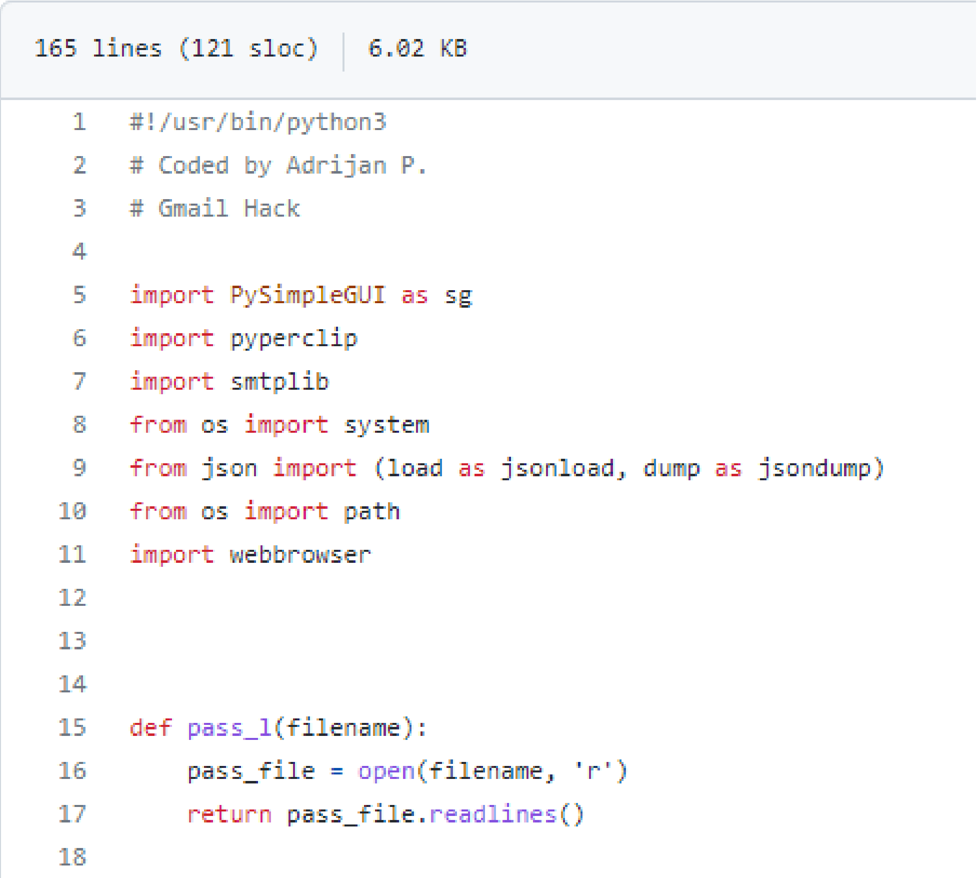
rows=100 sort-reverse=severity first=1 apply_overrides=0 min_qod=70

Results (43 of 94)

Vulnerability		Severity	QoD	Host	Location	Created
VulnersDB: CESA-2017:1842 kernel, perf, python security update		10.0 (High)	97%	192.168.56.104	general/tcp	Thu Jun 29 16:26:52 2017
VulnersDB: CESA-2017:1615 kernel, perf, python security update		10.0 (High)	97%	192.168.56.104	general/tcp	Thu Jun 29 16:27:05 2017
VulnersDB: CESA-2017:1860 libtasn1 security update		10.0 (High)	97%	192.168.56.104	general/tcp	Thu Jun 29 16:28:13 2017
VulnersDB: CESA-2017:0086 kernel, perf, python security update		10.0 (High)	97%	192.168.56.104	general/tcp	Thu Jun 29 16:28:47 2017
VulnersDB: CESA-2016:2779 nss security update		9.3 (High)	97%	192.168.56.104	general/tcp	Thu Jun 29 16:27:13 2017
VulnersDB: CESA-2017:1308 kernel, perf, python security update		9.3 (High)	97%	192.168.56.104	general/tcp	Thu Jun 29 16:27:27 2017
VulnersDB: CESA-2017:2679 kernel, perf, python security update		8.3 (High)	97%	192.168.56.104	general/tcp	Thu Jun 29 16:27:42 2017

PYTHON

- A popular scripting language
- Can be installed on any platform
  - Including Linux, Windows, macOS iOS and Android
- You can write a script to:
  - Perform customized vulnerability scanning
  - Automate tasks
  - Parse results
- Used in some commercial scanning tools
- GitHub has many Python hacking tools that you can download



165 lines (121 sloc) | 6.02 KB

```python
#!/usr/bin/python3
# Coded by Adrijan P.
# Gmail Hack

import PySimpleGUI as sg
import pyperclip
import smtplib
from os import system
from json import (load as jsonload, dump as jsondump)
from os import path
import webbrowser



def pass_l(filename):
    pass_file = open(filename, 'r')
    return pass_file.readlines()

```

Python is only one example of a programming language that you can use to create your own hacking tools.

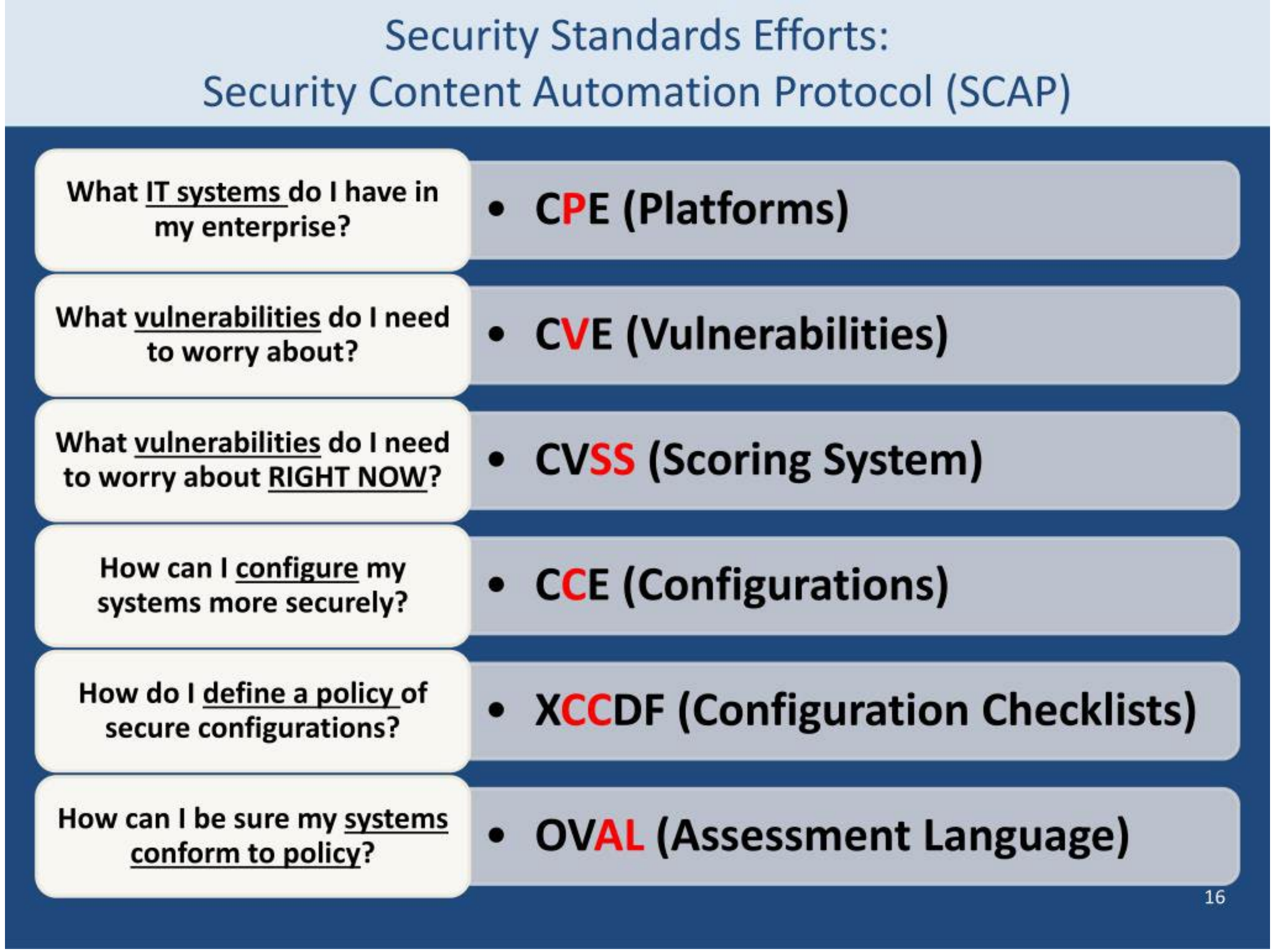
PYTHON PORT SCANNER EXAMPLE

```
from socket import *
import time
startTime = time.time()

if __name__ == '__main__':
    target = input('Enter the host to be scanned: ')
    t_IP = gethostbyname(target)
    print ('Starting scan on host: ', t_IP)

    for i in range(50, 500):
        s = socket(AF_INET, SOCK_STREAM)

        conn = s.connect_ex((t_IP, i))
        if(conn == 0) :
            print ('Port %d: OPEN' % (i,))
        s.close()
print('Time taken:', time.time() - startTime)
```

SECURITY CONTENT AUTOMATION PROTOCOL (SCAP)

- A multi-purpose framework of specifications supporting:
  - Automated configuration
  - Vulnerability and patch checking
  - Technical control compliance
  - Security measurement
- Used by the NVD
- SCAP is an industry standard
- SCAP scanners are typically used to test a system for compliance

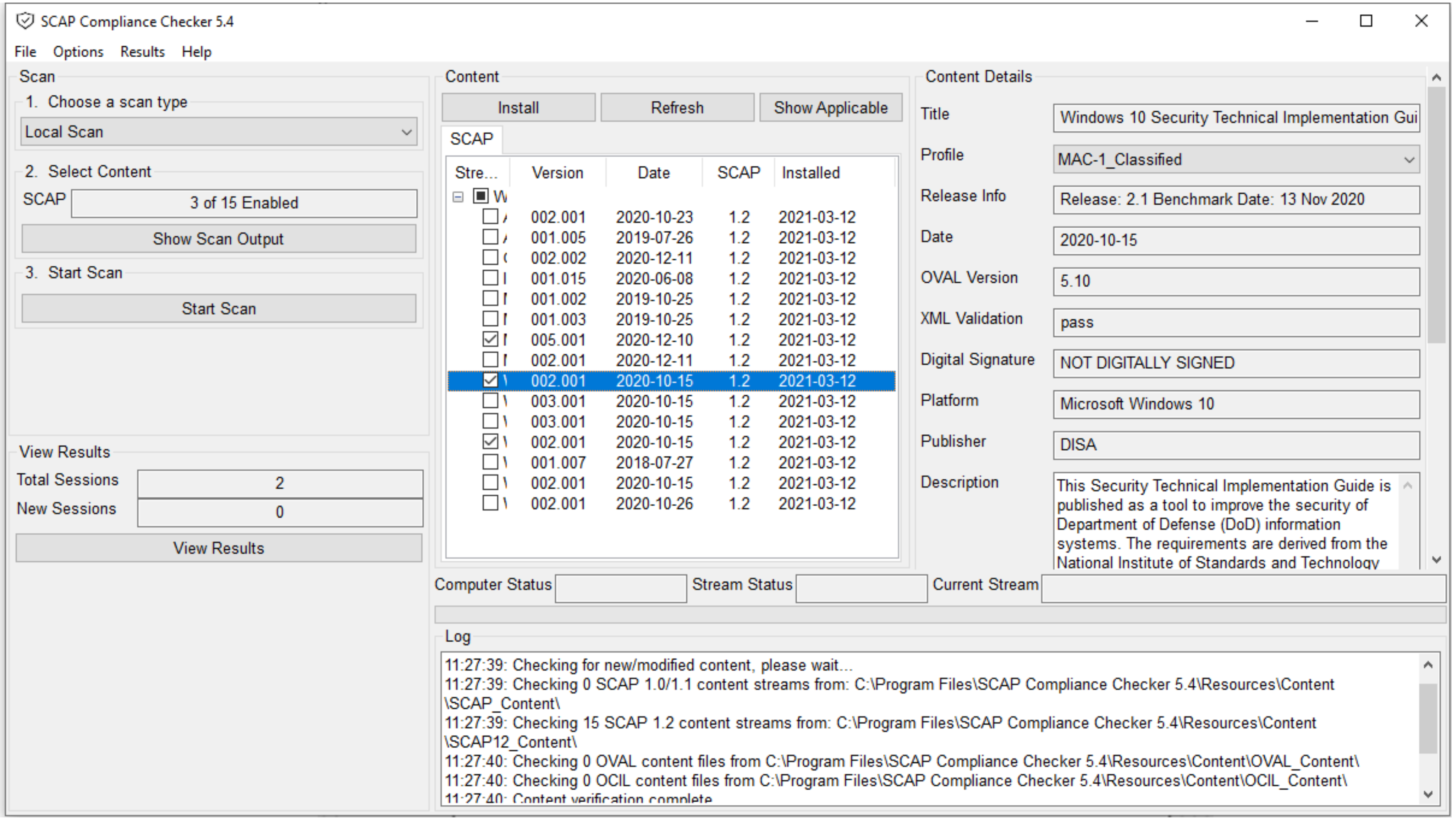
SCAP FRAMEWORK



Security Standards Efforts:
Security Content Automation Protocol (SCAP)

What IT systems do I have in my enterprise?	• CPE (Platforms)
What vulnerabilities do I need to worry about?	• CVE (Vulnerabilities)
What vulnerabilities do I need to worry about RIGHT NOW?	• CVSS (Scoring System)
How can I configure my systems more securely?	• CCE (Configurations)
How do I define a policy of secure configurations?	• XCCDF (Configuration Checklists)
How can I be sure my systems conform to policy?	• OVAL (Assessment Language)

SCAP COMPLIANCE CHECKER EXAMPLE



1. Choose a scan type: Local Scan

2. Select Content

SCAP: 3 of 15 Enabled

3. Start Scan

View Results

Total Sessions: 2

New Sessions: 0

Stre...	Version	Date	SCAP	Installed
⊟ ■ W				
☐ /	002.001	2020-10-23	1.2	2021-03-12
☐ /	001.005	2019-07-26	1.2	2021-03-12
☐ (	002.002	2020-12-11	1.2	2021-03-12
☐ I	001.015	2020-06-08	1.2	2021-03-12
☐ I	001.002	2019-10-25	1.2	2021-03-12
☐ I	001.003	2019-10-25	1.2	2021-03-12
☑ I	005.001	2020-12-10	1.2	2021-03-12
☐ I	002.001	2020-12-11	1.2	2021-03-12
☑ \	002.001	2020-10-15	1.2	2021-03-12
☐ \	003.001	2020-10-15	1.2	2021-03-12
☐ \	003.001	2020-10-15	1.2	2021-03-12
☑ \	002.001	2020-10-15	1.2	2021-03-12
☐ \	001.007	2018-07-27	1.2	2021-03-12
☐ \	002.001	2020-10-15	1.2	2021-03-12
☐ \	002.001	2020-10-26	1.2	2021-03-12

Content Details

Title	Windows 10 Security Technical Implementation Gui
Profile	MAC-1_Classified
Release Info	Release: 2.1 Benchmark Date: 13 Nov 2020
Date	2020-10-15
OVAL Version	5.10
XML Validation	pass
Digital Signature	NOT DIGITALLY SIGNED
Platform	Microsoft Windows 10
Publisher	DISA
Description	This Security Technical Implementation Guide is published as a tool to improve the security of Department of Defense (DoD) information systems. The requirements are derived from the National Institute of Standards and Technology

Computer Status

Stream Status

Current Stream

Log

```
11:27:39: Checking for new/modified content, please wait...
11:27:39: Checking 0 SCAP 1.0/1.1 content streams from: C:\Program Files\SCAP Compliance Checker 5.4\Resources\Content
\SCAP_Content\
11:27:39: Checking 15 SCAP 1.2 content streams from: C:\Program Files\SCAP Compliance Checker 5.4\Resources\Content
\SCAP12_Content\
11:27:40: Checking 0 OVAL content files from C:\Program Files\SCAP Compliance Checker 5.4\Resources\Content\OVAL_Content\
11:27:40: Checking 0 OCIL content files from C:\Program Files\SCAP Compliance Checker 5.4\Resources\Content\OCIL_Content\
11:27:40: Content verification complete
```

SCAP SCENARIO

- You are creating baseline system images
- The images will be used to remediate vulnerabilities found in different operating systems
- Before any of the images can be deployed, they must be scanned for malware and vulnerabilities
- You must ensure the configurations meet industry-standard benchmarks and that the baselining creation process can be repeated frequently
- Use an operating system SCAP plugin to check the OS against known good baselines

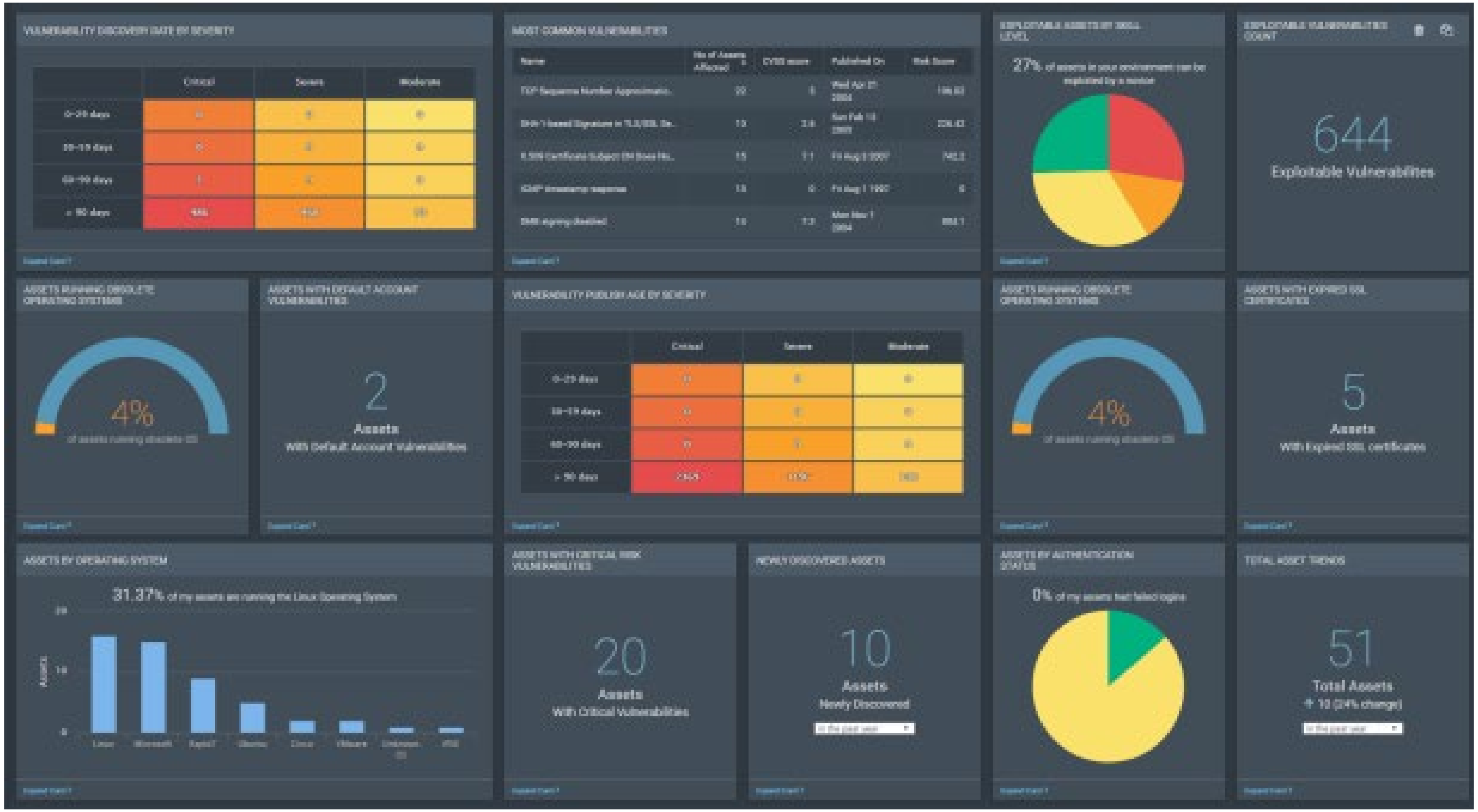
VULNERABILITY SCANNER OUTPUT

- Usually includes:
  - Dashboard with summaries
  - Details for each device
- Output for both physical and virtual hosts
- Device names, types, IP addresses, MAC addresses
- Device OS version
- Open TCP and UPD ports
- Installed applications and services
- Discovered vulnerabilities, insecure default settings and misconfigurations

VULNERABILITY SCANNER OUTPUT (CONT'D)

- Accounts with weak or default passwords
- Files and folders with weak permissions
- Technology- or device-specific issues
- Missing patches and hotfixes
- End-of-Life / End-of-Service software information
- Higher-end scanning tools will separate the report into:
  - Executive summary
  - Technical details
- May include CVE and CVSS references
- Should include recommendations to correct/mitigate discovered issues

VULNERABILITY SCANNER OUTPUT EXAMPLE



VULNERABILITY DISCOVERY DATE BY SEVERITY

	Critical	Severe	Moderate
0–29 days	0	0	0
30–59 days	0	0	0
60–90 days	1	0	0
> 90 days	[illegible]	[illegible]	[illegible]

Expand Card

MOST COMMON VULNERABILITIES

Name	No of Assets Affected	CVSS score	Published On	Risk Score
TCP Sequence Number Approximatio...	20	5	Wed Apr 21 2004	196.02
SHA-1-based Signature in TLS/SSL Se...	13	2.6	Sun Feb 15 2005	226.42
X.509 Certificate Subject DN Does No...	13	7.1	Fri Aug 3 2007	740.2
ICMP timestamp response	13	0	Fri Aug 1 1997	0
SMB signing disabled	13	7.3	Mon Nov 1 2004	868.1

Expand Card

EXPLOITABLE ASSETS BY SKILL LEVEL

27% of assets in your environment can be exploited by a novice

Expand Card

EXPLOITABLE VULNERABILITIES COUNT

644

Exploitable Vulnerabilities

ASSETS RUNNING OBSOLETE OPERATING SYSTEMS

4%

of assets running obsolete OS

Expand Card

ASSETS WITH DEFAULT ACCOUNT VULNERABILITIES

2

Assets

With Default Account Vulnerabilities

Expand Card

VULNERABILITY PUBLISH AGE BY SEVERITY

	Critical	Severe	Moderate
0–29 days	0	0	0
30–59 days	0	0	0
60–90 days	0	0	0
> 90 days	[illegible]	[illegible]	[illegible]

Expand Card

ASSETS RUNNING OBSOLETE OPERATING SYSTEMS

4%

of assets running obsolete OS

Expand Card

ASSETS WITH EXPIRED SSL CERTIFICATES

5

Assets

With Expired SSL certificates

Expand Card

ASSETS BY OPERATING SYSTEM

31.37% of my assets are running the Linux Operating System

Expand Card

ASSETS WITH CRITICAL RISK VULNERABILITIES

20

Assets

With Critical Vulnerabilities

Expand Card

NEWLY DISCOVERED ASSETS

10

Assets

Newly Discovered

in the past year ▾

Expand Card

ASSETS BY AUTHENTICATION STATUS

0% of my assets had failed logins

Expand Card

TOTAL ASSET TRENDS

51

Total Assets

↑ 10 (24% change)

in the past year ▾

Expand Card

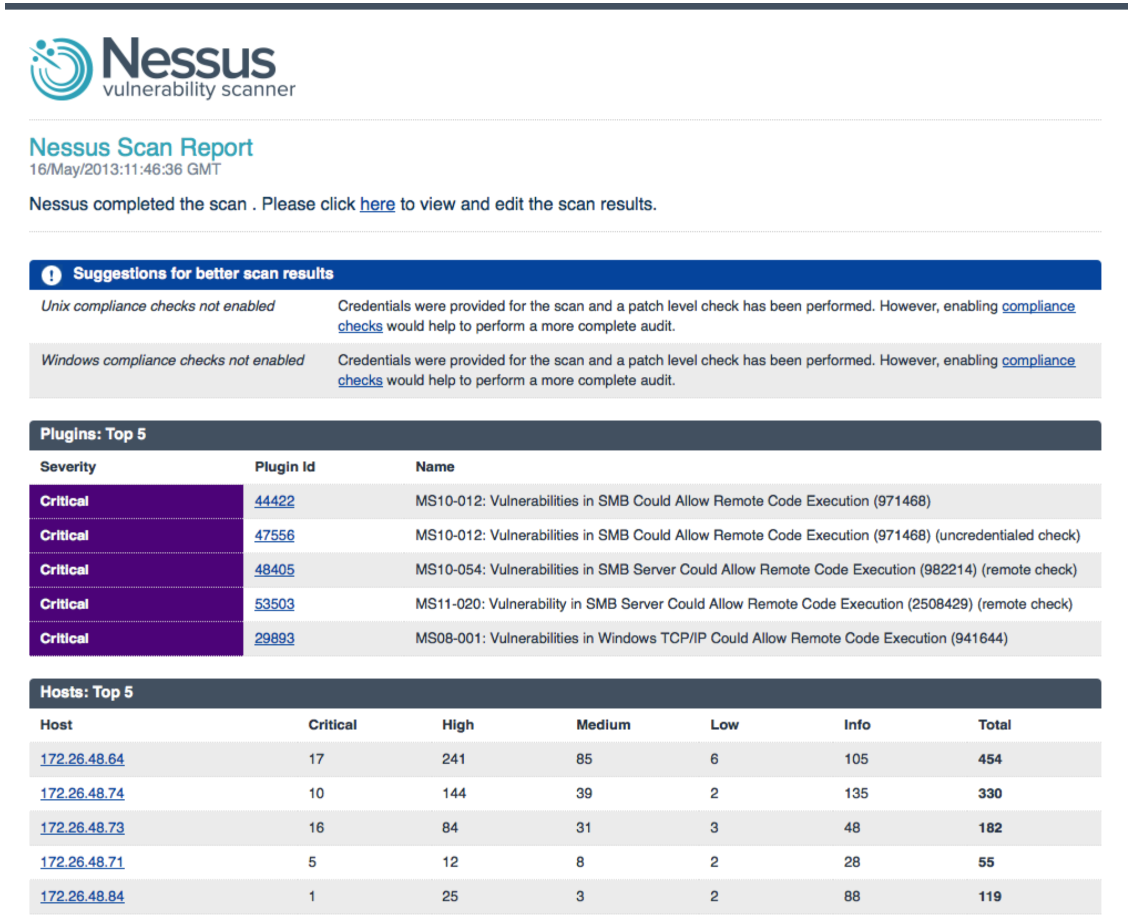
SCAN RESULT CATEGORIES

- **True Positive**
  - The scanner detects a vulnerability
  - The vulnerability actually exists on the scanned system
  - The scan did its job!
- **True Negative**
  - The scanner does not detect a vulnerability
  - The vulnerability really does not exist on the scanned system
  - This is our preferred result!
- **False Positive**
  - The scanner detects a vulnerability
  - But the vulnerability does not actually exist on the scanned system
  - Too many of these can be annoying!
- **False Negative**
  - The scanner does not detect a vulnerability
  - But the vulnerability actually exists on the scanned system
  - This is the worst result!

COMMON REPORT ELEMENTS

- Executive Summary
- Major findings
- Scan information (tools used, scope)
- Target information
- Results
- Target details
  - Node
  - OS
  - Services / ports
  - Date
  - Modules used
  - Outcomes
- Vulnerability Classification
  - Typically includes CVE references
- Threat Assessment
- Recommendations
- Summary

VULNERABILITY REPORT EXAMPLE



Nessus
vulnerability scanner

Nessus Scan Report

16/May/2013:11:46:36 GMT

Nessus completed the scan . Please click here to view and edit the scan results.

Suggestions for better scan results

Unix compliance checks not enabled	Credentials were provided for the scan and a patch level check has been performed. However, enabling compliance checks would help to perform a more complete audit.
Windows compliance checks not enabled	Credentials were provided for the scan and a patch level check has been performed. However, enabling compliance checks would help to perform a more complete audit.

Plugins: Top 5

Severity	Plugin Id	Name
Critical	44422	MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution (971468)
Critical	47556	MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution (971468) (uncredentialed check)
Critical	48405	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214) (remote check)
Critical	53503	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429) (remote check)
Critical	29893	MS08-001: Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (941644)

Hosts: Top 5

Host	Critical	High	Medium	Low	Info	Total
172.26.48.64	17	241	85	6	105	**454**
172.26.48.74	10	144	39	2	135	**330**
172.26.48.73	16	84	31	3	48	**182**
172.26.48.71	5	12	8	2	28	**55**
172.26.48.84	1	25	3	2	88	**119**

5.2 VULNERABILITY ASSESSMENT

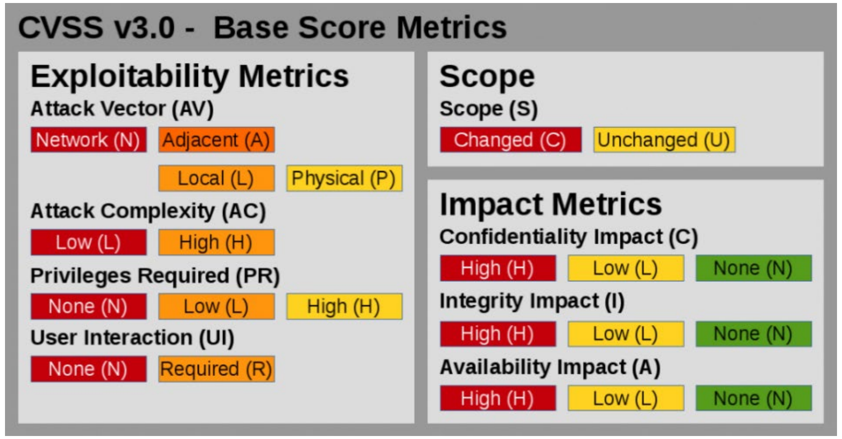
- Overview
- CVSS
- CVE
- Vulnerability Research

WHAT IS A VULNERABILITY ASSESSMENT?

- A comprehensive assessment of a system's ability to withstand attack
  - Includes the use of automated vulnerability scanning tools
  - Part of the overall security audit
- Should also assess non-technical vulnerabilities (people, processes)
- Should produce an actionable report

COMMON VULNERABILITY SCORING SYSTEM (CVSS)

- Open framework for communicating characteristics and impacts of IT vulnerabilities
- Uses three groups of metrics for measuring vulnerabilities:
  - Base metrics - inherent qualities of a vulnerability
  - Temporal metrics - features that keep changing during vulnerability lifetime
  - Environmental metrics - vulnerabilities based on a particular environment or implementation
- 1 (lowest) - 10 (most severe) scoring
- Recorded in National Vulnerability Database



CVSS v3.0 - Base Score Metrics

Exploitability Metrics

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

Scope (S)

Changed (C) | Unchanged (U)

Impact Metrics

Confidentiality Impact (C)

High (H) | Low (L) | None (N)

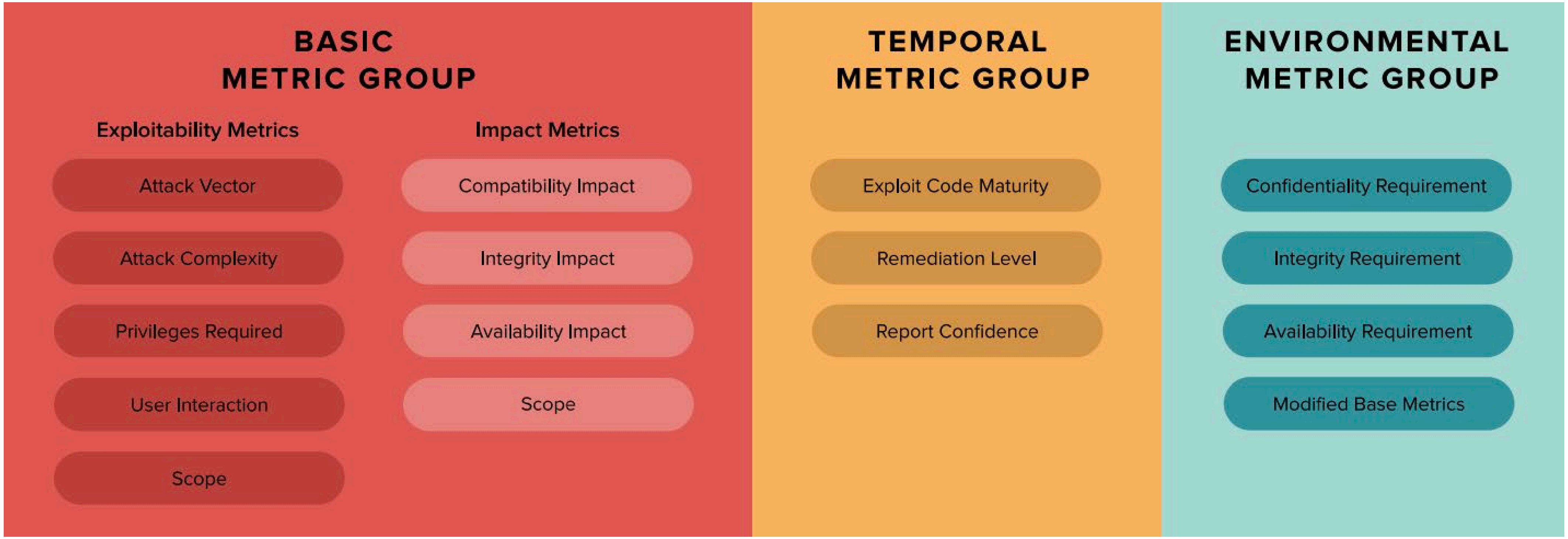
Integrity Impact (I)

High (H) | Low (L) | None (N)

Availability Impact (A)

High (H) | Low (L) | None (N)

CVSS METRIC GROUPS



BASIC METRIC GROUP

Exploitability Metrics

- Attack Vector
- Attack Complexity
- Privileges Required
- User Interaction
- Scope

Impact Metrics

- Compatibility Impact
- Integrity Impact
- Availability Impact
- Scope

TEMPORAL METRIC GROUP

- Exploit Code Maturity
- Remediation Level
- Report Confidence

ENVIRONMENTAL METRIC GROUP

- Confidentiality Requirement
- Integrity Requirement
- Availability Requirement
- Modified Base Metrics

CVSS ATTACK VECTOR METRICS

The Attack Vector metric is scored in one of four levels:

- Network (N)
  - Vulnerabilities with this rating are remotely exploitable, from one or more hops away, up to, and including, remote exploitation over the Internet
- Adjacent (A)
  - A vulnerability with this rating requires network adjacency for exploitation
  - The attack must be launched from the same physical or logical network
  - The attacker must have access to the local network that the system is connected to
- Local (L)
  - Vulnerabilities with this rating are not exploitable over a network
  - The attacker must access the system locally, remotely (via protocol like SSH or RDP)
  - Or requires use of social engineering or other techniques to trick an unsuspecting user to help initiate the exploit
- Physical (P)
  - In this type of attack, the adversary must physically interact with the target system

CVSS ATTACK COMPLEXITY METRICS

- The Attack Complexity metric indicates conditions beyond the attacker's control
  - These conditions must exist in order to exploit the vulnerability
  - Most commonly, this refers to either required user interaction, or specific configurations of the target system
- The Attack Complexity metric is scored as either Low or High:
  - Low (L)
    - There are no specific pre-conditions required for exploitation
  - High (H)
    - There are conditions beyond the attackers control for successful attack
    - For this type of attack, the attacker must complete some number of preparatory steps in order to get access
    - This might include gather reconnaissance data, overcoming mitigations, or becoming a man-in-the-middle

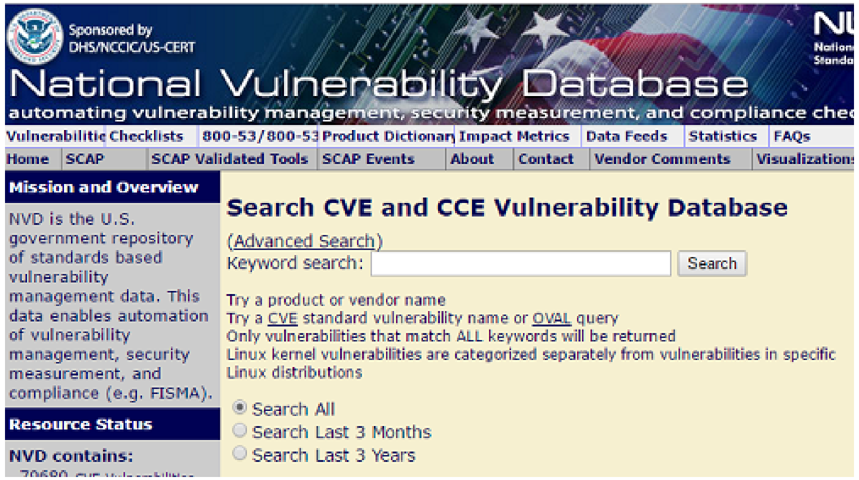
CVSS PRIVILEGES REQUIRED METRIC

- This metric is exactly as it sounds, describing the level of privileges, or access, an attacker must have before successful exploit
- Privileges requires falls under three ratings:
  - None (N)
    - There is no privilege or special access required to conduct the attack
  - Low (L)
    - The attacker requires basic, "user" level privileges to leverage the exploit
  - High (H)
    - Administrative or similar access privileges are required for successful attack

For additional information on CVSS metrics see
https://www.balbix.com/insights/base-cvss-scores/

NATIONAL VULNERABILITY DATABASE (NVD)

- nvd.nist.gov
- US government repository of standards-based vulnerability management data
- Uses Security Content Automation Protocol (SCAP)
  - Suite of specifications for automatically exchanging security content between systems
- Enables automation of vulnerability management
- Aggregates data to produce:
  - CVSS
  - Common Weakness Enumeration (CWE)
  - Common Platform Enumeration (CPE)
- Does not perform the actual tests



NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

NVD contains:

Search CVE and CCE Vulnerability Database

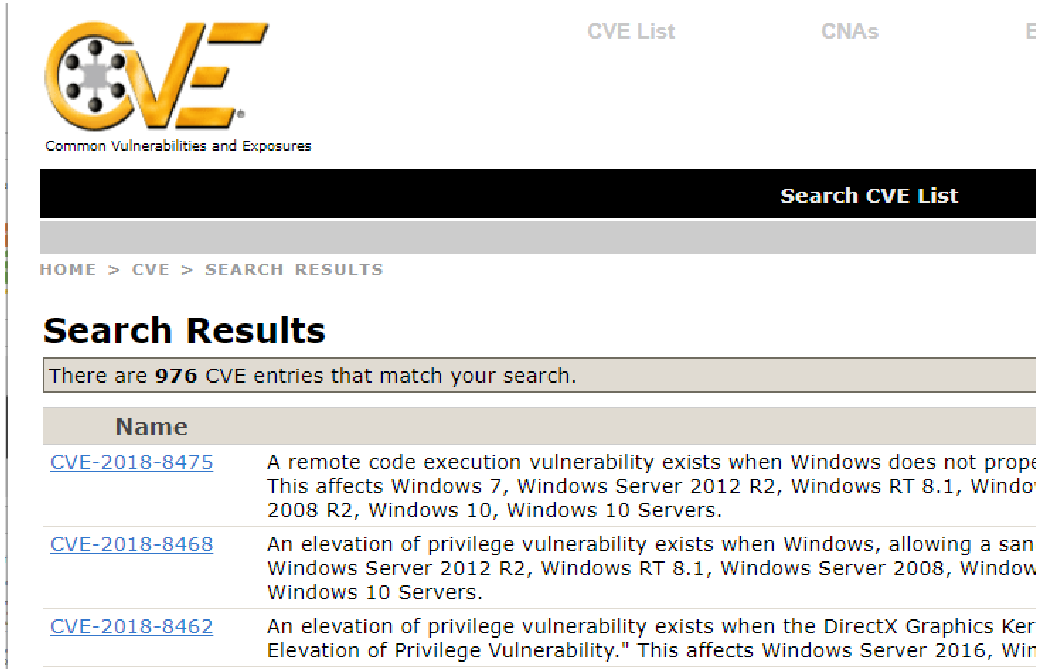
Keyword search:

Try a product or vendor name
Try a CVE standard vulnerability name or OVAL query
Only vulnerabilities that match ALL keywords will be returned
Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions

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

COMMON VULNERABILITIES AND EXPOSURES (CVE)

- ID system to precisely identify a vulnerability
- Used by both malicious and ethical hackers
- cve.mitre.org


CVE
Common Vulnerabilities and Exposures
CVE List
CNAs
E
Search CVE List
HOME > CVE > SEARCH RESULTS

Search Results

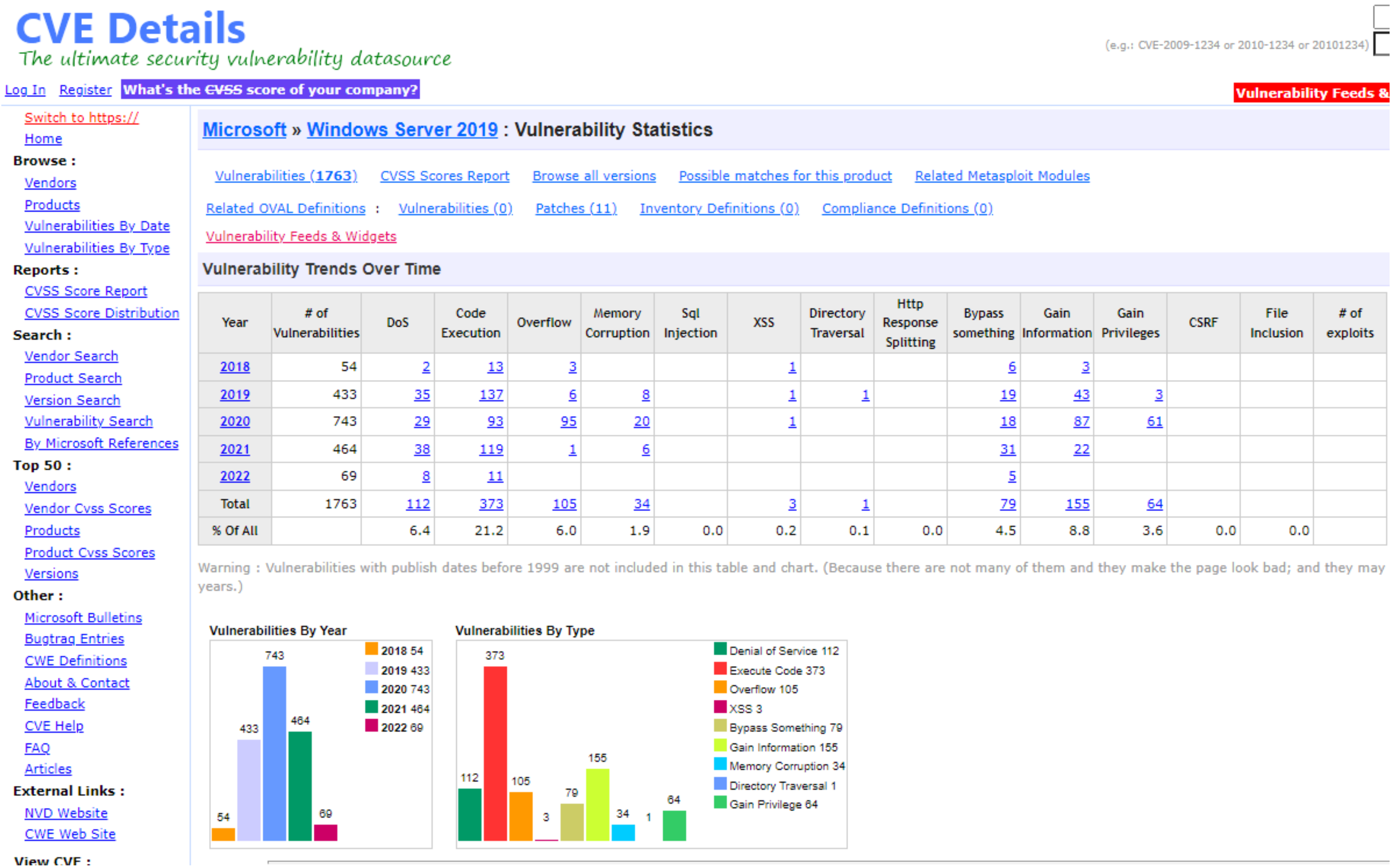
There are **976** CVE entries that match your search.

Name	
CVE-2018-8475	A remote code execution vulnerability exists when Windows does not prope This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windo 2008 R2, Windows 10, Windows 10 Servers.
CVE-2018-8468	An elevation of privilege vulnerability exists when Windows, allowing a san Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Window Windows 10 Servers.
CVE-2018-8462	An elevation of privilege vulnerability exists when the DirectX Graphics Ker Elevation of Privilege Vulnerability." This affects Windows Server 2016, Wir

RESEARCHING VULNERABILITIES

- Gather information about security trends, threats and attacks
- Discover system design faults and find weaknesses before an attack
- Learn how to recover from a network attack
- Classify vulnerabilities by:
  - Priority
  - Severity
  - Scope
- Stay updated about new products, technologies, and exploits
- Check underground hacking web sites (Deep and Dark Web sites) for newly discovered vulnerabilities and exploits
- Check for news releases on security innovations and product improvements

VULNERABILITY RESEARCH EXAMPLE



CVE Details

The ultimate security vulnerability datasource

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Log In Register What's the ~~CVSS~~ score of your company?

Vulnerability Feeds &

Switch to https://
Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact
Feedback
CVE Help
FAQ
Articles
External Links :
NVD Website
CWE Web Site
View CVE :

Microsoft » Windows Server 2019 : Vulnerability Statistics

Vulnerabilities (1763) CVSS Scores Report Browse all versions Possible matches for this product Related Metasploit Modules

Related OVAL Definitions : Vulnerabilities (0) Patches (11) Inventory Definitions (0) Compliance Definitions (0)

Vulnerability Feeds & Widgets

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2018	54	2	13	3			1			6	3				
2019	433	35	137	6	8		1	1		19	43	3			
2020	743	29	93	95	20		1			18	87	61			
2021	464	38	119	1	6					31	22				
2022	69	8	11							5					
Total	1763	112	373	105	34		3	1		79	155	64			
% Of All		6.4	21.2	6.0	1.9	0.0	0.2	0.1	0.0	4.5	8.8	3.6	0.0	0.0	

Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them and they make the page look bad; and they may years.)

Vulnerabilities By Year

Vulnerabilities By Type

RESOURCES FOR VULNERABILITY RESEARCH

- SANS (https://sans.org)
- CISA (https://cisa.gov)
- CVE Details (https://www.cvedetails.com)
- OWASP (https://www.owasp.org)
- Microsoft Vulnerability Research (MSVR) (https://www.microsoft.com)
- Dark Reading (https://www.darkreading.com)
- SecurityTracker (https://securitytracker.com)
- Trend Micro (https://www.trendmicro.com)
- Security Magazine (https://www.securitymagazine.com)
- PenTest Magazine (https://pentestmag.com)
- SC Magazine (https://www.scmagazine.com)

RESOURCES FOR VULNERABILITY RESEARCH (CONT'D)

- Exploit Database (https://www.exploit-db.com)
- Rapid7 (https://www.rapid7.com)
- Security Focus (https://www.securityfocus.com)
- Help Net Security (https://www.helpnetsecurity.com)
- HackerStorm (http://www.hackerstorm.co.uk)
- Computerworld (https://www.computerworld.com)
- WindowsSecurity (http://www.windowsecurity.com)
- D'Crypt (https://www.d-crypt.com)
- Sophos (https://www.sophos.com)

5.3 VULNERABILITY ANALYSIS REVIEW

- Review

VULNERABILITY ANALYSIS REVIEW

- You can perform vulnerability scans to identify weaknesses or lack of compliance
- Scanning can be passive or active
- Vulnerability scanning tools can focus on hosts, network devices, cloud services, or applications
- Credentialed scans typically provide more information than uncredentialed scans
- SCAP scans are used to test a system for compliance

- Scan results can return four different types of results:
  - True positive – there really is a vulnerability
  - True negative – there really is no vulnerability
  - False positive – the scanner reports vulnerabilities that do not actually exist
  - False negative – the scanner fails to report vulnerabilities that actually exist

VULNERABILITY ANALYSIS REVIEW

- Vulnerability assessment should include both technical and non-technical targets (people, processes)
- A vulnerability assessment should produce an actionable report
- Common Vulnerability Scoring System (CVSS) ranks vulnerability severity on a scale of 1-10
- CVSS identifies four attack vectors: network, adjacent, local, physical

- The National Vulnerability Database is a central repository of vulnerability information
- Common Vulnerabilities and Exposures (CVE) is an identification system used to precisely identify a specific vulnerability
- CVEs are used by both malicious and ethical hackers
- Vulnerability research should be an ongoing process
- There are many sites and services dedicated to providing the latest vulnerability information