Phase 3. Identify Vulnerabilities

Goal: Identify the tools and techniques to be used to scan for vulnerabilities.

Procedure: List out the tools you plan on using to perform vulnerability scanning and how you will use them. Include both Tenable Nessus and OpenVAS. Remember to include tools designed to look for vulnerabilities within specific technologies or platforms, such as Cisco devices, remote access services, and web applications (e.g., Burp Suite). Follow the same documentation procedure you performed in the previous step. Include screenshots of such tools showing configuration options and settings. Finally, list the pros and cons of each tool.

Deliverable: Provide a minimum 2-page description of the tools you plan on using for the vulnerability scans, how you will use them, screenshots of the tools with configuration options and settings, and the pros and cons of each tool. Deliverable should cover at least 5 tools.

Time estimate: 2 hours

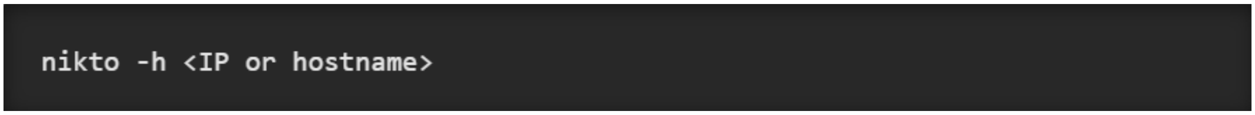
DELIVERABLES

In cybersecurity terms, a vulnerability is a weakness or loophole left in software code that allows attackers to infiltrate and run malicious code or install malware. Such an intrusion, when successful, can allow bad actors to steal or destroy data, take over systems and accounts, and execute unauthorized actions on behalf of the compromised user. A vulnerability scanner is an automated tool that identifies and creates an inventory of all IT assets (including servers, desktops, laptops, virtual machines, containers, firewalls, switches, and printers) connected to a network. For each asset, it also attempts to identify operational details such as the operating system it runs and the software installed on it, along with other attributes such as open ports and user accounts. A vulnerability scanner enables organizations to monitor their networks, systems, and applications for security vulnerabilities. This report will detail tools and techniques used for vulnerability scans

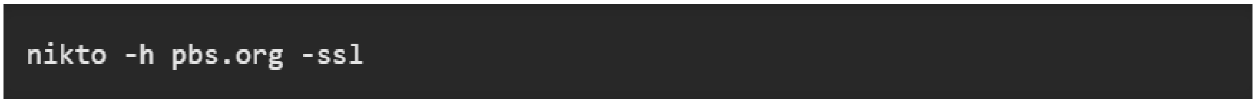
Nikto

Nikto is an open source web server and web application scanner. Nikto can perform comprehensive tests against web servers for multiple security threats, including over 6700 potentially dangerous files/programs. Nikto can also perform checks for outdated web servers software, and version-specific problems. Here are some of the cool things that Nikto can do:

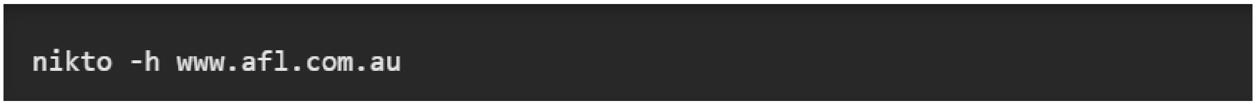
- Find SQL injection, XSS, and other common vulnerabilities, Identify installed software (via headers, favicons, and files), Guess subdomains, Includes support for SSL (HTTPS) websites, Saves reports in plain text, XML, HTML or CSV, “Fish” for content on web servers, Report unusual headers, Check for server configuration items like multiple index files, HTTP server options, Has full HTTP proxy support, Guess credentials for authorization (including many default username/password combinations), Is configured with a template engine to easily customize reports, Exports to Metasploit.



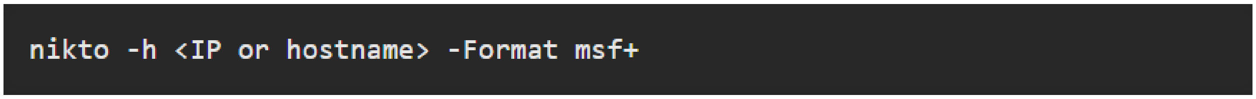
```
nikto -h <IP or hostname>
```



```
nikto -h pbs.org -ssl
```



```
nikto -h www.afl.com.au
```



```
nikto -h <IP or hostname> -Format msf+
```

Pros:

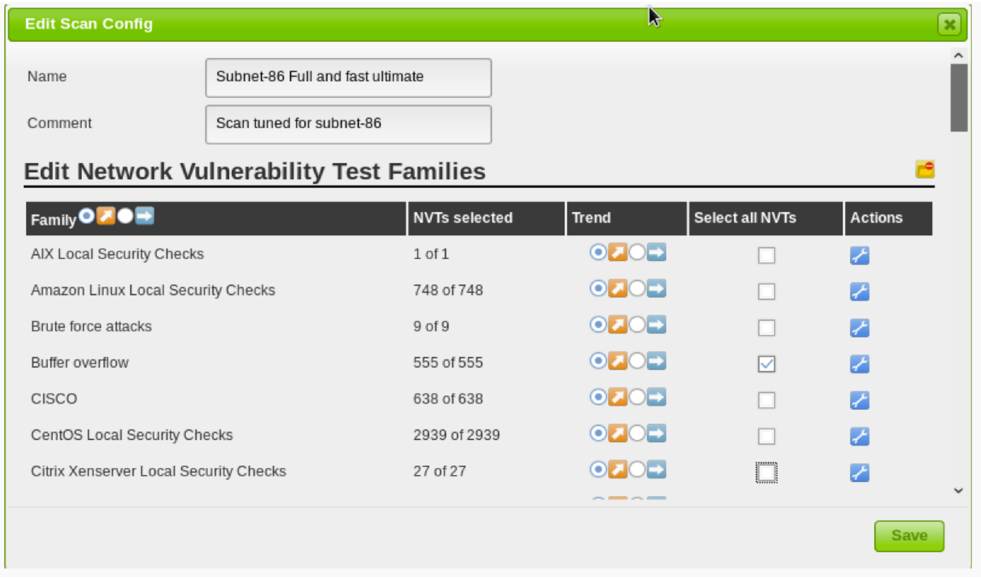
- A free base program
- Thorough checks with the number of exploits in the standard scan match that sought by paid vulnerability managers
- External checks for Web applications
- Included in Kali Linux

Cons:

- No GUI interface
- No development and support team
- No community forum
- Won't work without a paid vulnerability list

OpenVAS

OpenVAS is a system vulnerability scanner that checks visible ports, services it can access for known exploits, and high level web threats (like cross-site script vulnerabilities and improper file access). The primary reason to use this scan type is to perform comprehensive security testing of an IP address. It will initially conduct a port scan of an IP address to find open services. Once listening services are discovered, they are tested for known vulnerabilities and misconfiguration using a large database (more than 53000 NVT checks). The results are compiled into a report, including detailed information regarding each vulnerability and notable issues discovered. Vulnerability scans performed from externally hosted servers give you the same perspective as an attacker. This has the advantage of understanding exactly what is exposed on external facing services.



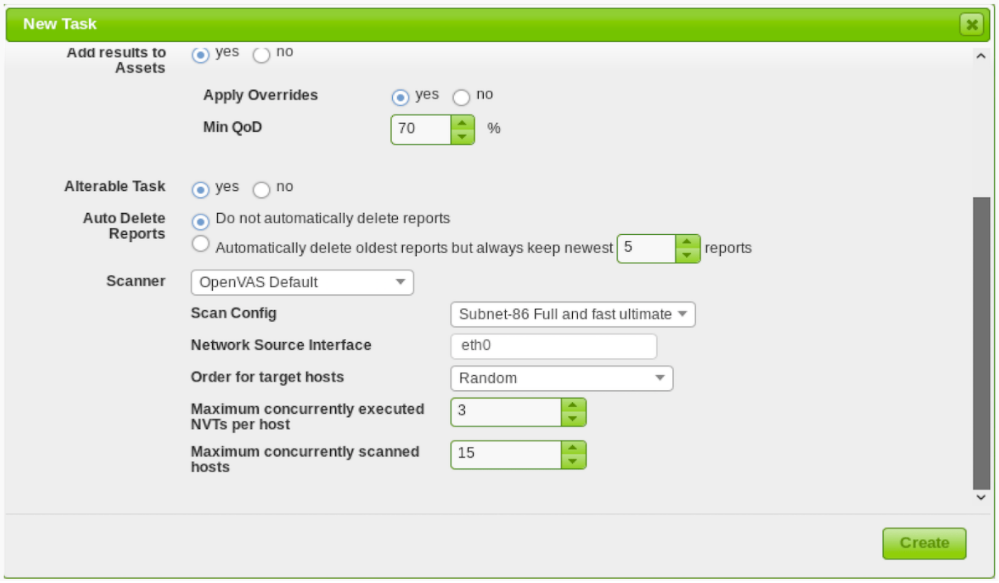
Edit Scan Config

Name: Subnet-86 Full and fast ultimate

Comment: Scan tuned for subnet-86

Edit Network Vulnerability Test Families

Family ◉ ↗ ○ ➡	NVTs selected	Trend	Select all NVTs	Actions
AIX Local Security Checks	1 of 1	◉ ↗ ○ ➡	□	🔧
Amazon Linux Local Security Checks	748 of 748	◉ ↗ ○ ➡	□	🔧
Brute force attacks	9 of 9	◉ ↗ ○ ➡	□	🔧
Buffer overflow	555 of 555	◉ ↗ ○ ➡	☑	🔧
CISCO	638 of 638	◉ ↗ ○ ➡	□	🔧
CentOS Local Security Checks	2939 of 2939	◉ ↗ ○ ➡	□	🔧
Citrix Xenserver Local Security Checks	27 of 27	◉ ↗ ○ ➡	□	🔧


New Task

Add results to Assets ● yes ○ no

Apply Overrides ● yes ○ no

Min QoD 70 %

Alterable Task ● yes ○ no

Auto Delete Reports ● Do not automatically delete reports
○ Automatically delete oldest reports but always keep newest 5 reports

Scanner OpenVAS Default

Scan Config Subnet-86 Full and fast ultimate

Network Source Interface eth0

Order for target hosts Random

Maximum concurrently executed NVTs per host 3

Maximum concurrently scanned hosts 15

Pros

- OpenVAS is a free open-source vulnerability assessment tool that is maintained by Greenbone Networks.
- Common vulnerabilities and exposure (CVE) coverage of around 26,000
- Popular and useful among SME's
- Built to be an all-in-one scanner
- The scan engine of OpenVAS is updated on a regular basis
- Greenbone provides thorough tutorials for the usage of this tool

Cons

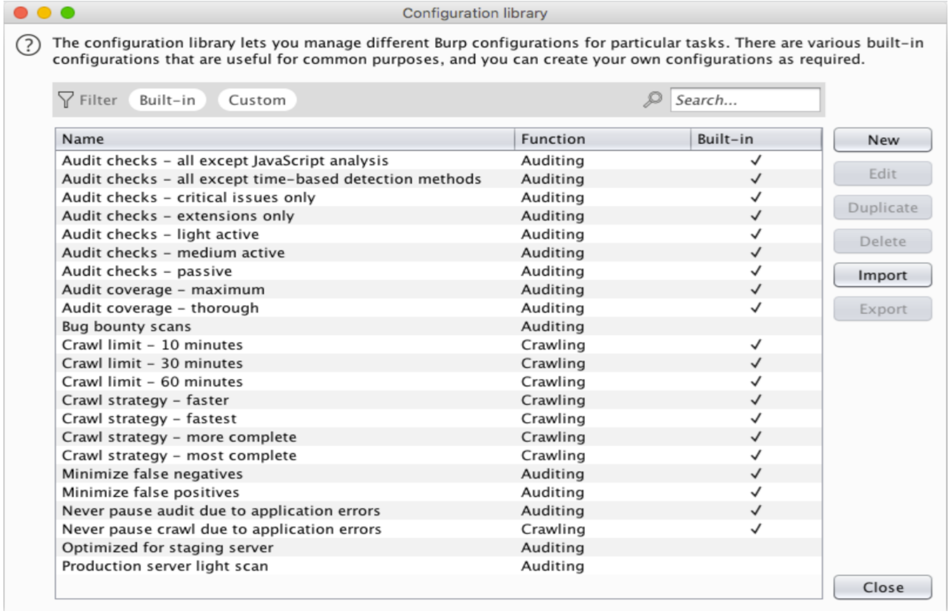
- Covers fewer CVEs as compared to Nessus
- Less operating system supportability
- Does not offer policy management

Burp Suite

Burp Suite software is the best toolbox for web security testing. In web security testing, the incursion also protects engineer grace. Used to find and exploit search flaws. Burp Suite is therefore designed to be used by point-and-click. Understanding how systems are attacked is essential for everyone working in security, whether they are developers or security professionals. Burp Suite is an integrated platform/graphical tool for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

Burp Suite is a proxy program that enables us to track, examine, and alter requests made by our browsers before they are forwarded to a distant server.

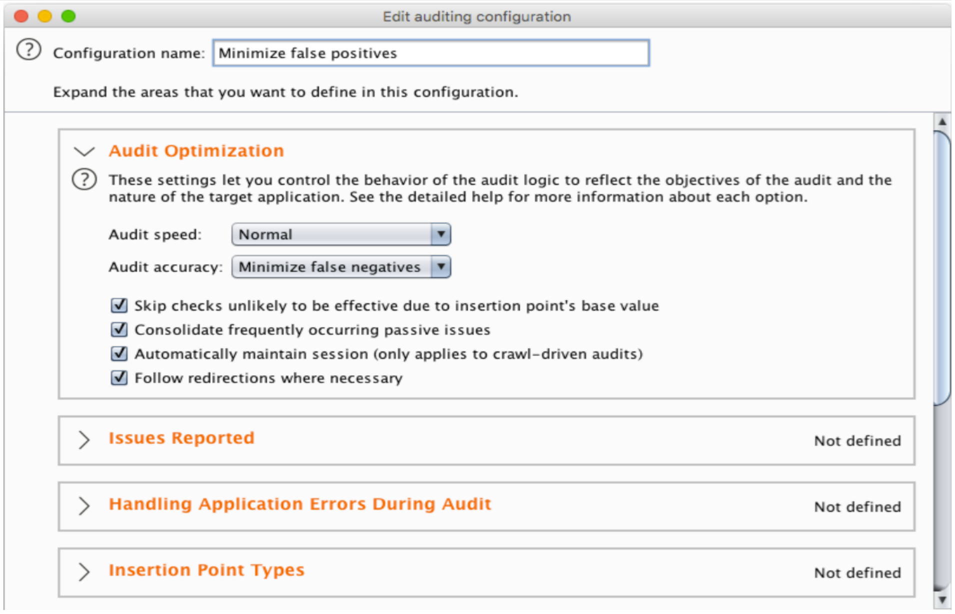
Burp Suite is a prominent web application security solution. It gives us the ability to manually test for vulnerabilities, intercepts HTTP messages, and change a message's body and header.



Configuration library

The configuration library lets you manage different Burp configurations for particular tasks. There are various built-in configurations that are useful for common purposes, and you can create your own configurations as required.

Name	Function	Built-in
Audit checks – all except JavaScript analysis	Auditing	✓
Audit checks – all except time-based detection methods	Auditing	✓
Audit checks – critical issues only	Auditing	✓
Audit checks – extensions only	Auditing	✓
Audit checks – light active	Auditing	✓
Audit checks – medium active	Auditing	✓
Audit checks – passive	Auditing	✓
Audit coverage – maximum	Auditing	✓
Audit coverage – thorough	Auditing	✓
Bug bounty scans	Auditing	
Crawl limit – 10 minutes	Crawling	✓
Crawl limit – 30 minutes	Crawling	✓
Crawl limit – 60 minutes	Crawling	✓
Crawl strategy – faster	Crawling	✓
Crawl strategy – fastest	Crawling	✓
Crawl strategy – more complete	Crawling	✓
Crawl strategy – most complete	Crawling	✓
Minimize false negatives	Auditing	✓
Minimize false positives	Auditing	✓
Never pause audit due to application errors	Auditing	✓
Never pause crawl due to application errors	Crawling	✓
Optimized for staging server	Auditing	
Production server light scan	Auditing	



Edit auditing configuration

Configuration name: Minimize false positives

Expand the areas that you want to define in this configuration.

Audit Optimization

These settings let you control the behavior of the audit logic to reflect the objectives of the audit and the nature of the target application. See the detailed help for more information about each option.

Audit speed: Normal

Audit accuracy: Minimize false negatives

☑ Skip checks unlikely to be effective due to insertion point's base value

☑ Consolidate frequently occurring passive issues

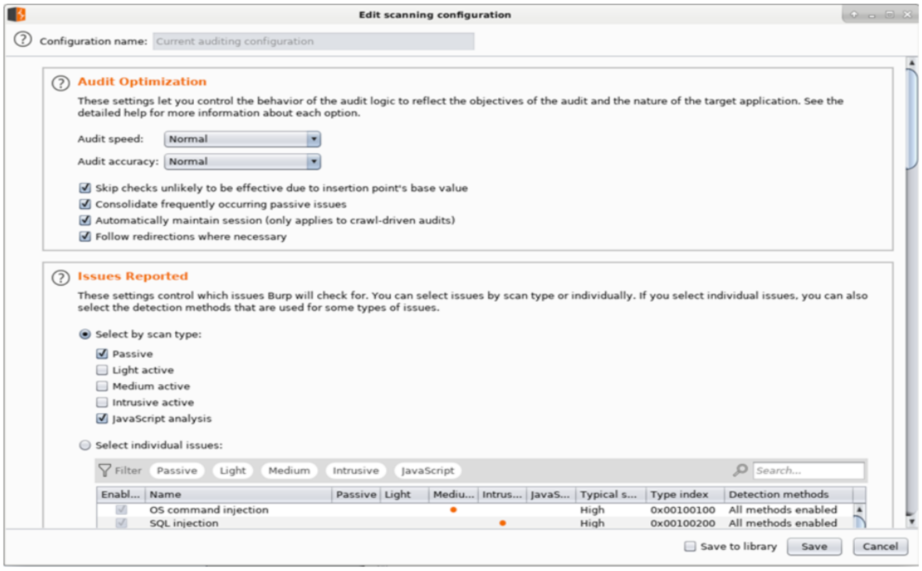
☑ Automatically maintain session (only applies to crawl-driven audits)

☑ Follow redirections where necessary

Issues Reported — Not defined

Handling Application Errors During Audit — Not defined

Insertion Point Types — Not defined



Edit scanning configuration

Configuration name: Current auditing configuration

Audit Optimization

These settings let you control the behavior of the audit logic to reflect the objectives of the audit and the nature of the target application. See the detailed help for more information about each option.

Audit speed: Normal

Audit accuracy: Normal

☑ Skip checks unlikely to be effective due to insertion point's base value
☑ Consolidate frequently occurring passive issues
☑ Automatically maintain session (only applies to crawl-driven audits)
☑ Follow redirections where necessary

Issues Reported

These settings control which issues Burp will check for. You can select issues by scan type or individually. If you select individual issues, you can also select the detection methods that are used for some types of issues.

● Select by scan type:

☑ Passive
□ Light active
□ Medium active
□ Intrusive active
☑ JavaScript analysis

○ Select individual issues:

Filter: Passive Light Medium Intrusive JavaScript   Search...

Enabl...	Name	Passive	Light	Mediu...	Intrus...	JavaS...	Typical s...	Type index	Detection methods
✓	OS command injection			●			High	0x00100100	All methods enabled
✓	SQL injection				●		High	0x00100200	All methods enabled

□ Save to library Save Cancel

Pros

There are various advantages of using the this tool. Some of the most prominent advantages of using this tool are:

- The burp suite comprises a set of tools that ensure thorough security testing.
- The tool allows users to perform fully customized scans per their requirements.
- By using the this tool, users can prevent a lot of cyber attacks, such as phishing, malware, etc.
- The tool helps you maintain the users’ trust by protecting their sensitive information.
- This tool also allows its users to perform active scans, which involves sending more data to the server; hence, vulnerability to DoS attacks can be checked.

Cons

Being one of the most popular penetration testing tools, there are only a few disadvantages to using this tool, such as:

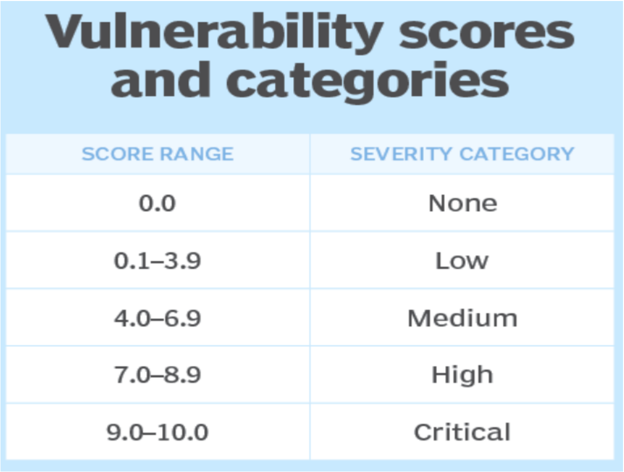
- The graphical interface of this tool is not user-friendly.
- The free version of this tool lacks a lot of features that are present in the pro version.

- As the tool consists of various other tools, it is difficult to use for first-time or new users with little information.

Nessus

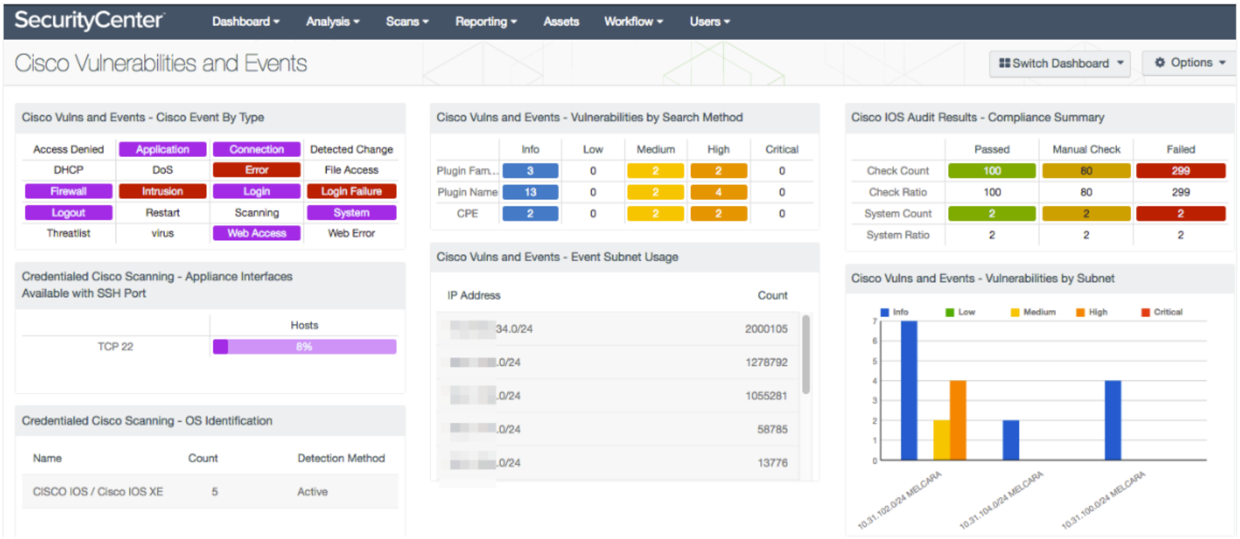
Nessus is a platform developed by Tenable that scans for security vulnerabilities in devices, applications, operating systems, cloud services and other network resources. Nessus identifies software flaws, missing patches, malware, denial-of-service vulnerabilities, default passwords and misconfiguration errors, among other potential flaws. When Nessus discovers vulnerabilities, it issues an alert that IT teams can then investigate and determine what, if any, further action is required.

Nessus contains a feature called Predictive Prioritization, which uses algorithms to categorize vulnerabilities by their severity to aid IT teams in determining which threats are most urgent to address. Each vulnerability is assigned a Vulnerability Priority Rating (VPR), which uses a scale from 0 to 10, with 10 being the highest risk, to rate its severity: critical, high, medium or low. IT teams can also use pre-built policies and templates to quickly find vulnerabilities and understand the threat situation.



Vulnerability scores and categories

SCORE RANGE	SEVERITY CATEGORY
0.0	None
0.1–3.9	Low
4.0–6.9	Medium
7.0–8.9	High
9.0–10.0	Critical



Cisco Vulnerabilities and Events

Cisco Vulns and Events - Cisco Event By Type

Access Denied	Application	Connection	Detected Change
DHCP	DoS	Error	File Access
Firewall	Intrusion	Login	Login Failure
Logout	Restart	Scanning	System
Threatlist	virus	Web Access	Web Error

Credentialed Cisco Scanning - Appliance Interfaces Available with SSH Port

	Hosts
TCP 22	8%

Credentialed Cisco Scanning - OS Identification

Name	Count	Detection Method
CISCO IOS / Cisco IOS XE	5	Active

Cisco Vulns and Events - Vulnerabilities by Search Method

	Info	Low	Medium	High	Critical
Plugin Fam...	3	0	2	2	0
Plugin Name	13	0	2	4	0
CPE	2	0	2	2	0

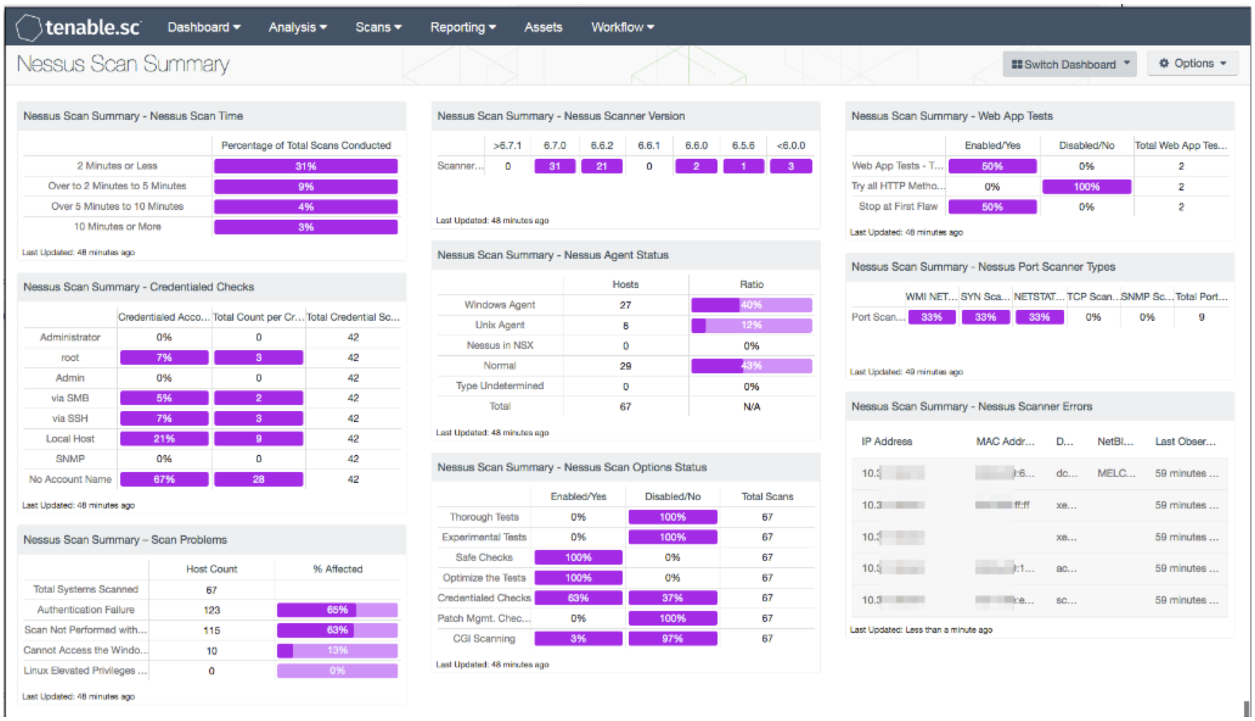
Cisco Vulns and Events - Event Subnet Usage

IP Address	Count
[redacted]34.0/24	2000105
[redacted].0/24	1278792
[redacted].0/24	1055281
[redacted].0/24	58785
[redacted].0/24	13776

Cisco IOS Audit Results - Compliance Summary

	Passed	Manual Check	Failed
Check Count	100	80	299
Check Ratio	100	80	299
System Count	2	2	2
System Ratio	2	2	2

Cisco Vulns and Events - Vulnerabilities by Subnet



Nessus Scan Summary

Nessus Scan Summary - Nessus Scan Time

	Percentage of Total Scans Conducted
2 Minutes or Less	31%
Over to 2 Minutes to 5 Minutes	9%
Over 5 Minutes to 10 Minutes	4%
10 Minutes or More	3%

Last Updated: 48 minutes ago

Nessus Scan Summary - Credentialed Checks

	Credentialed Acco...	Total Count per Cr...	Total Credential Sc...
Administrator	0%	0	42
root	7%	3	42
Admin	0%	0	42
via SMB	5%	2	42
via SSH	7%	3	42
Local Host	21%	9	42
SNMP	0%	0	42
No Account Name	67%	28	42

Last Updated: 48 minutes ago

Nessus Scan Summary – Scan Problems

	Host Count	% Affected
Total Systems Scanned	67	
Authentication Failure	123	65%
Scan Not Performed with...	115	63%
Cannot Access the Windo...	10	13%
Linux Elevated Privileges ...	0	0%

Last Updated: 48 minutes ago

Nessus Scan Summary - Nessus Scanner Version

	>6.7.1	6.7.0	6.6.2	6.6.1	6.6.0	6.5.6	<6.0.0
Scanner...	0	31	21	0	2	1	3

Last Updated: 48 minutes ago

Nessus Scan Summary - Nessus Agent Status

	Hosts	Ratio
Windows Agent	27	40%
Unix Agent	8	12%
Nessus in NSX	0	0%
Normal	29	43%
Type Undetermined	0	0%
Total	67	N/A

Last Updated: 48 minutes ago

Nessus Scan Summary - Nessus Scan Options Status

	Enabled/Yes	Disabled/No	Total Scans
Thorough Tests	0%	100%	67
Experimental Tests	0%	100%	67
Safe Checks	100%	0%	67
Optimize the Tests	100%	0%	67
Credentialed Checks	63%	37%	67
Patch Mgmt. Chec...	0%	100%	67
CGI Scanning	3%	97%	67

Last Updated: 48 minutes ago

Nessus Scan Summary - Web App Tests

	Enabled/Yes	Disabled/No	Total Web App Tes...
Web App Tests - T...	50%	0%	2
Try all HTTP Metho...	0%	100%	2
Stop at First Flaw	50%	0%	2

Last Updated: 48 minutes ago

Nessus Scan Summary - Nessus Port Scanner Types

	WMI NET...	SYN Sca...	NETSTAT...	TCP Scan...	SNMP Sc...	Total Port...
Port Scan...	33%	33%	33%	0%	0%	9

Last Updated: 49 minutes ago

Nessus Scan Summary - Nessus Scanner Errors

IP Address	MAC Addr...	D...	NetBI...	Last Obser...
10.3[redacted]	[redacted]:6...	dc...	MELC...	59 minutes ...
10.3[redacted]	[redacted]ff:ff	xe...		59 minutes ...
10.3[redacted]		xe...		59 minutes ...
10.3[redacted]	[redacted]:1...	ac...		59 minutes ...
10.3[redacted]	[redacted]:e...	sc...		59 minutes ...

Last Updated: Less than a minute ago

PROS

- Highly accurate scanning with low false +ves (Per 1 million tests, the device has just .32 errors)
- Compressive and deep scanning capabilities
- Highly scalable to 100 to 1000 of systems
- Ease of deployment and maintenance
- Low cost to administer and operations
- Common vulnerabilities and exposure coverage of around 47,000
- Facilitates group testing

- Built in scan templates

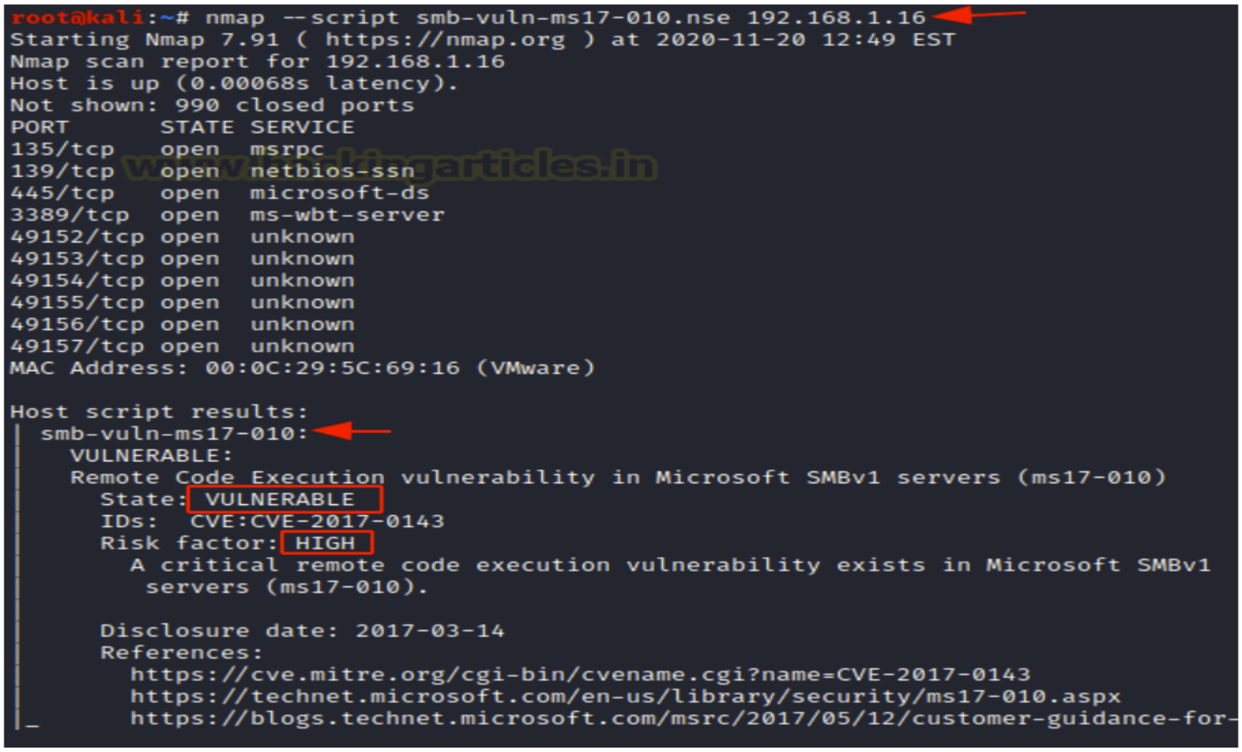
CONS

- Highly priced for commercial use not viable for smaller organizations
- Does not allow to check local security policies of remote systems
- Network overload could be a potential drawback
- Does not offer asset tagging and risk management

Nmap

Nmap (network mapper) can be used for vulnerability scanning to identify known vulnerabilities. While Nmap is not primarily a vulnerability scanner, Nmap's scripts can help cybersecurity experts perform scans for safety. Three of the most popular scripts for Nmap vulnerability scanning are vuln, vulscan, and nmap-vulners.   Nmap scripts contain well over 100 specific scans for vulnerabilities that can be run against domains or against IP addresses

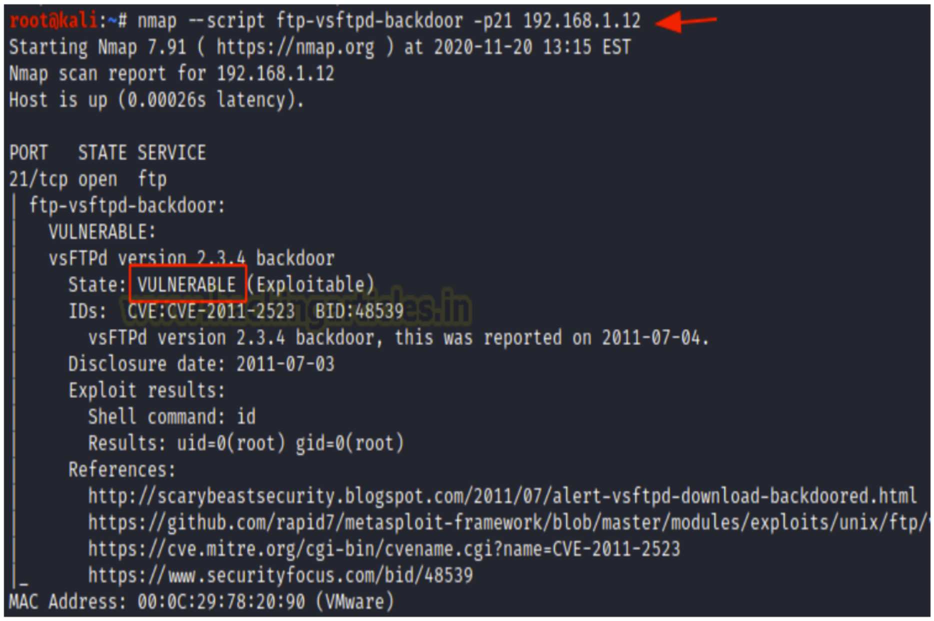
Ms17-010 Vulnerability



```
root@kali:~# nmap --script smb-vuln-ms17-010.nse 192.168.1.16
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 12:49 EST
Nmap scan report for 192.168.1.16
Host is up (0.00068s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:0C:29:5C:69:16 (VMware)

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-
```

Vsftpd backdoor



```
root@kali:~# nmap --script ftp-vsftpd-backdoor -p21 192.168.1.12
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 13:15 EST
Nmap scan report for 192.168.1.12
Host is up (0.00026s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  BID:48539
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_      https://www.securityfocus.com/bid/48539
MAC Address: 00:0C:29:78:20:90 (VMware)
```

Pros

- Open source and free so great for hackers, students, and all organizations
- Quick scans provide a fast look at potential vulnerabilities
- Lightweight TCP scans do not consume enormous network bandwidth and can escape some network security tools
- A hacker preview for organizations checking their internal systems
- Scriptable scans enable an organization to create repeatable vulnerability scans usable by non-technical users and for hackers to embed Nmap commands and scans into malware

Cons

- Easy to make mistakes with command line entries
- Lack of programmers in an organization’s IT staff to create custom scripts or understand Nmap scripts
- Less formal support than commercial tools
- Limited vulnerability scans through the basic vuln command

REFERENCES

https://www.balbix.com/insights/what-to-know-about-vulnerability-scanning-and-tools/

https://www.datamation.com/security/how-to-easily-run-a-vulnerability-scan-using-nmap/#:~:text=Nmap%20(network%20mapper)%20can%20be,experts%20perform%20scans%20for%20safety.

https://www.esecurityplanet.com/networks/nmap-vulnerability-scanning-made-easy/#vulnerability-scanning

https://nmap.org/nsedoc/categories/vuln.html

https://www.tenable.com/sc-dashboards/cisco-vulnerabilities-and-events

https://sharkfestus.wireshark.org/sharkfest.12/presentations/A-13_A-17_Secrets_of_Vulnerability_Scanning_Nessus_Nmap_and_More.pdf

https://www.techtarget.com/searchnetworking/definition/Nessus#:~:text=What%20is%20Nessus%3F,services%20and%20other%20network%20resources.

https://www.tenable.com/sc-dashboards/nessus-scan-summary-dashboards

https://networkinterview.com/nessus-network-vulnerability-scanner/

https://wisdomplexus.com/blogs/openvas-vs-nessus/

https://hackertarget.com/openvas-scan/

https://www.tcg.com/blog/faster-openvas-vulnerability-scanning/#:~:text=OpenVAS%20is%20a%20system%20vulnerability,vulnerabilities%20and%20improper%20file%20access).
https://www.shiksha.com/online-courses/articles/burp-suite-download/#4

https://www.pluralsight.com/paths/web-security-testing-with-burp-suite#:~:text=Burp%20Suite%20is%20an%20integrated%20platform%2Fgraphical%20tool%20for%20performing,finding%20and%20exploiting%20security%20vulnerabilities.

https://www.scaler.com/topics/cyber-security/burp-suite/

https://www.hackingarticles.in/nmap-for-pentester-vulnerability-scan/

https://www.comparitech.com/net-admin/nikto-review/

https://www.freecodecamp.org/news/an-introduction-to-web-server-scanning-with-nikto/