Vulnerability assessment report

Week 6 day 1

Submitted by NAVNEET KAUR

Executive summary:

This is the vulnerability assessment report Cat's company, where Cat needs my help to gather all the crucial information regarding vulnerabilities in the company and help her to make decisions and preparation that uphold the security of the company. The company hold the ip address 172.16.14.0/24 with different machines including Linux, windows server and windows 10 machine, whereas Kali Linux is main machine on which all vulnerability scans have to done. We will be performing scans on three devices Linux, windows server and windows 1. By implementing the recommended measures, the company can significantly reduce the risk of potential security incidents, protect sensitive data and maintain its reputation as a secure and trustworthy business entity. The vulnerabilities severity ranged from crucial to low to determine the impact of vulnerabilities. I will also give some suggestions to recommend fixing the security issues.

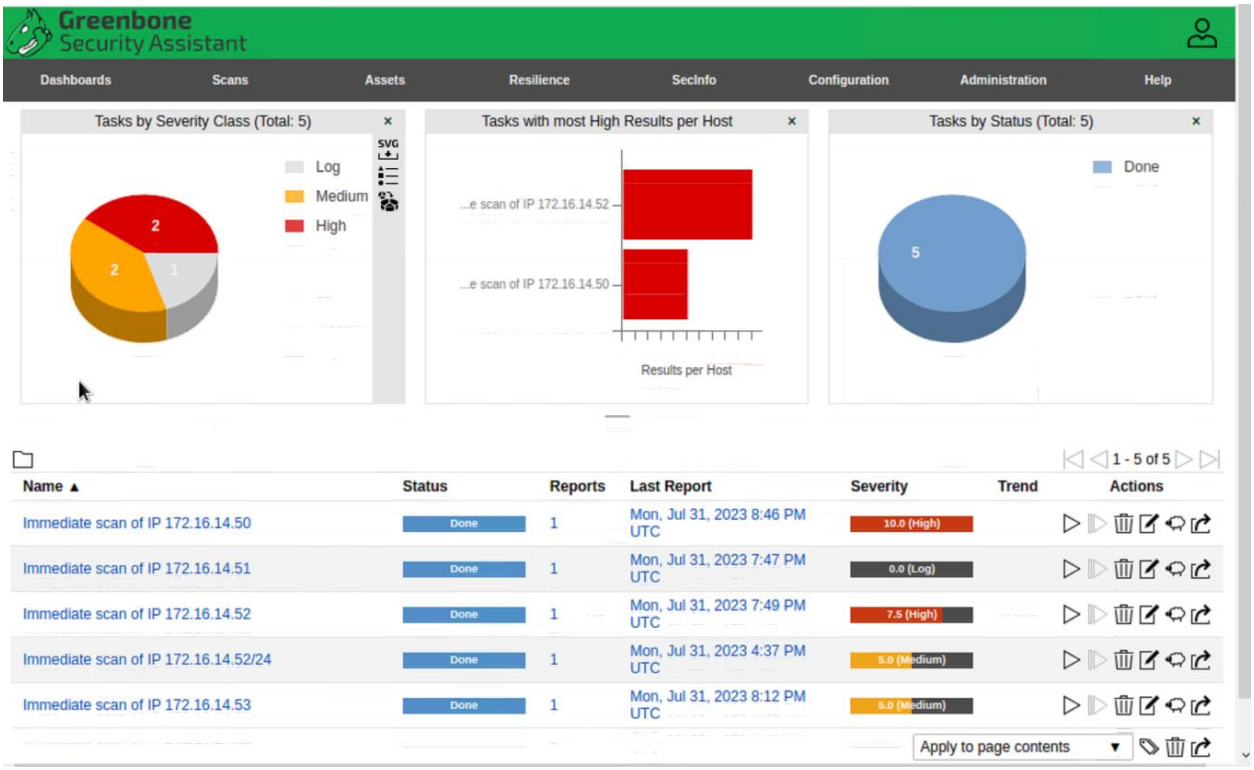
Vulnerability tools:

There are many tools to scan the network to find vulnerabilities such as Nessus, MITRE, Yara and OpenVAS. I'm using OpenVAS to scan the network. It is installed on Kali Linux machine also known as GVM-GreenBone vulnerability manager. All other three machines are active while scanning the network.

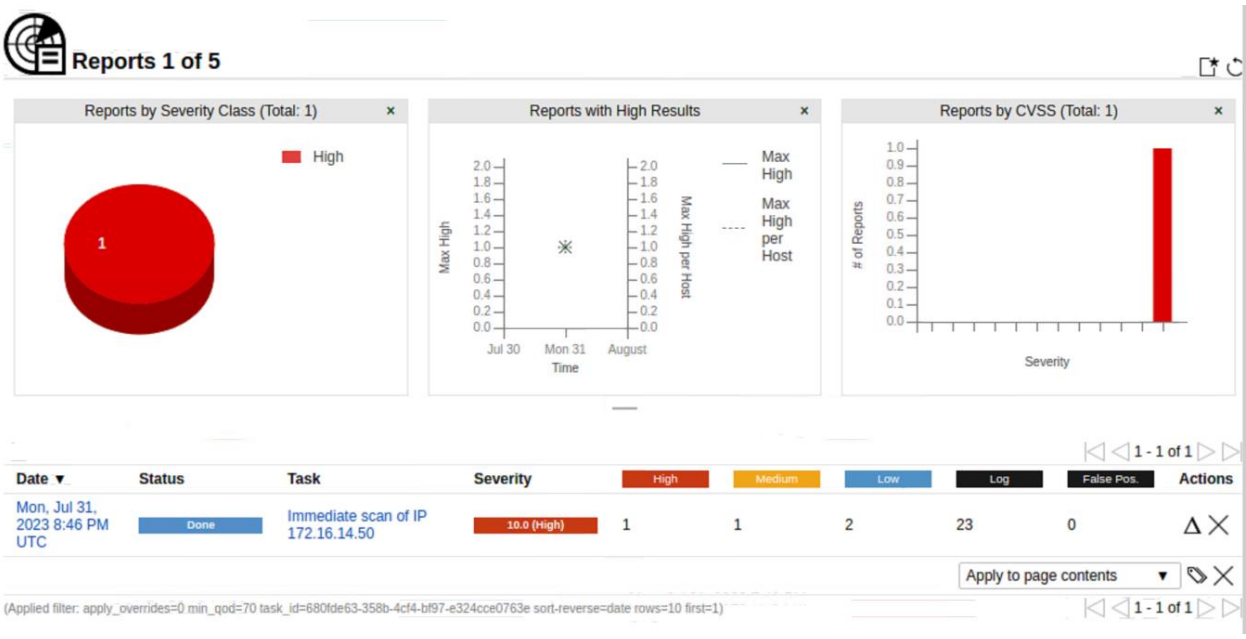
Scan results:

I've used OpenVAS to scan the network devices of Cat's company from the kali Linux machine. I've created three different dashboards for each device and scanned each device with their IP's assigned to them. The generated reports give us the detail of vulnerabilities on all devices with their severity level.

Overview screenshot of all devices scanned in OpenVAS



Immediate scan from Kali Linux 172.16.14.51 of Windows 1 having Ip address 172.16.14.50



Target

Target for immediate scan of IP 172.16.14.50 - 2023-07-31 20:46:24

Scanner

Name	OpenVAS Default
Type	OpenVAS Scanner
Scan Config	Full and fast
Order for target hosts	
Maximum concurrently executed NVTs per host	4
Maximum concurrently scanned hosts	20

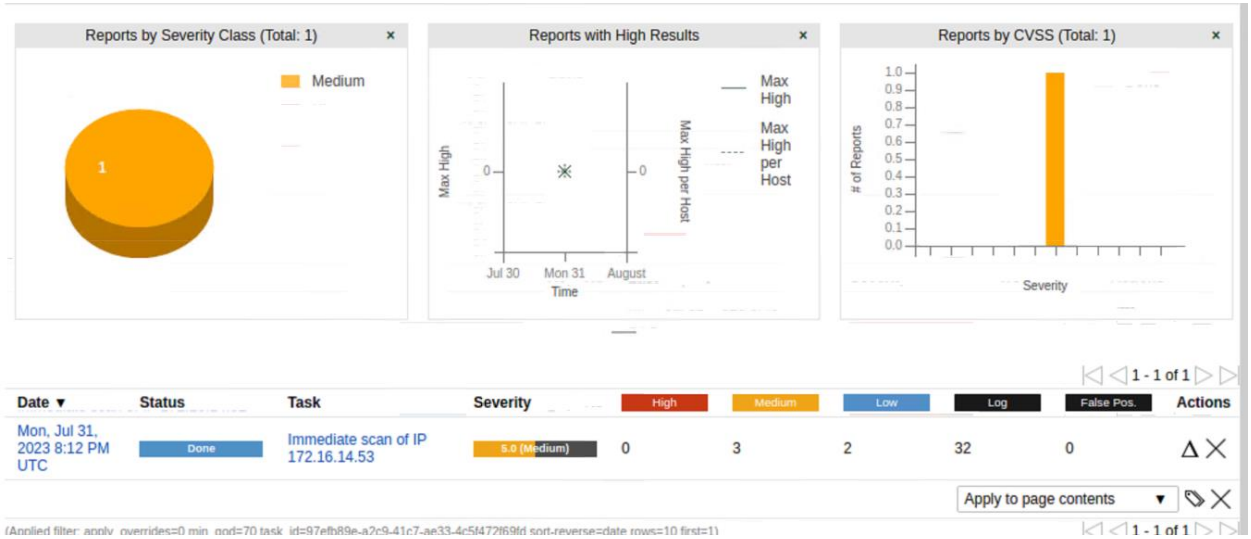
Assets

Add to Assets	Yes
Apply Overrides	Yes
Min QoD	70 %

Scan

Duration of last Scan	16 minutes
Auto delete Reports	Do not automatically delete reports

Scan of Windows Server ip address 172.16.14.53



Target

Target for immediate scan of IP 172.16.14.53 - 2023-07-31 20:12:44

Scanner

Name	OpenVAS Default
Type	OpenVAS Scanner
Scan Config	Full and fast
Order for target hosts	
Maximum concurrently executed NVTs per host	4
Maximum concurrently scanned hosts	20

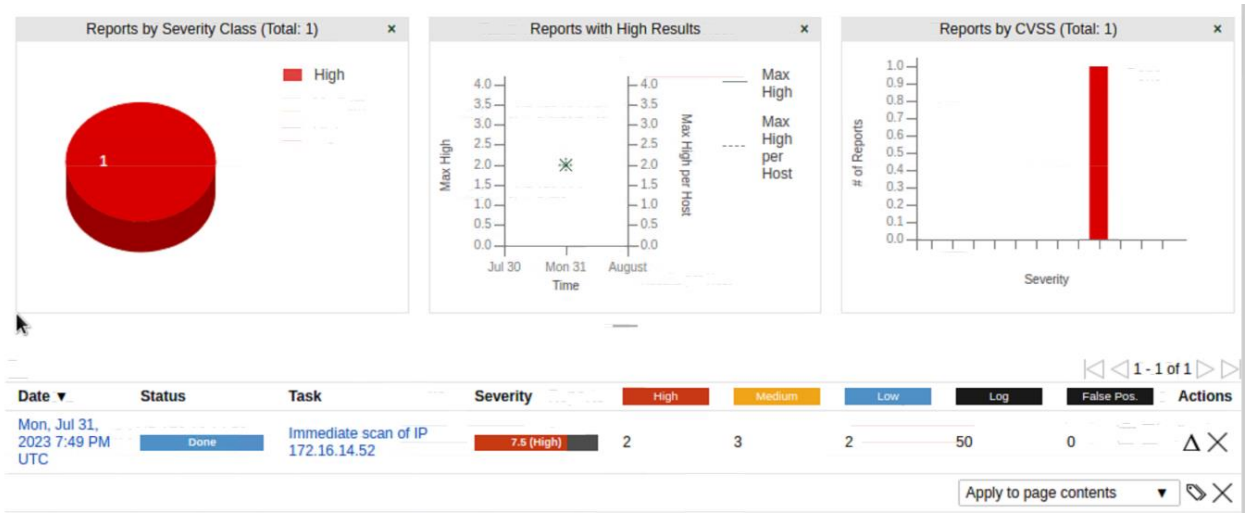
Assets

Add to Assets	Yes
Apply Overrides	Yes
Min QoD	70 %

Scan

Duration of last Scan	14 minutes
Auto delete Reports	Do not automatically delete reports

Scan for Linux 172.16.14.52



Target

Target for immediate scan of IP 172.16.14.52 - 2023-07-31 19:49:37

Scanner

Name	OpenVAS Default
Type	OpenVAS Scanner
Scan Config	Full and fast
Order for target hosts	
Maximum concurrently executed NVTs per host	4
Maximum concurrently scanned hosts	20

Assets

Add to Assets	Yes
Apply Overrides	Yes
Min QoD	70 %

Scan

Duration of last Scan	12 minutes
Auto delete Reports	Do not automatically delete reports

Our findings:

All three devices of Cat organization are successfully scanned and the results from the credential patch audit are listed below. The following image shows all the vulnerabilities in an organization on different machines in the network of Cat's company.

Vulnerabilities on windows 1:

Information | Results (4 of 28) | Hosts (1 of 1) | Ports (1 of 12) | Applications (0 of 0) | Operating Systems (1 of 1) | CVEs (1 of 1) | Closed CVEs (7 of 7) | TLS Certificates (0 of 0) | Error Messages (0 of 0) | User Tags (0)

1 - 4 of 4

Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location	Created
Operating System (OS) End of Life (EOL) Detection	10.0 (High)	80 %	172.16.14.50		general/tcp	Mon, Jul 31, 2023 8:55 PM UTC
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80 %	172.16.14.50		135/tcp	Mon, Jul 31, 2023 8:57 PM UTC
TCP Timestamps Information Disclosure	2.6 (Low)	80 %	172.16.14.50		general/tcp	Mon, Jul 31, 2023 8:55 PM UTC
ICMP Timestamp Reply Information Disclosure	2.1 (Low)	80 %	172.16.14.50		general/icmp	Mon, Jul 31, 2023 8:55 PM UTC

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

1 - 4 of 4

Linux:

Vulnerability	Severity ▼	QoD	Host IP	Name	Location	Created
Unprotected OSSEC/Wazuh ossec-authd (authd Protocol)	7.5 (High)	80 %	172.16.14.52		1515/tcp	Mon, Jul 31, 2023 7:53 PM UTC
HTTP Brute Force Logins With Default Credentials Reporting	7.5 (High)	95 %	172.16.14.52		9200/tcp	Mon, Jul 31, 2023 7:59 PM UTC
SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	5.0 (Medium)	70 %	172.16.14.52		1515/tcp	Mon, Jul 31, 2023 7:58 PM UTC
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	4.0 (Medium)	80 %	172.16.14.52		9300/tcp	Mon, Jul 31, 2023 7:56 PM UTC
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	4.0 (Medium)	80 %	172.16.14.52		9200/tcp	Mon, Jul 31, 2023 7:56 PM UTC
TCP Timestamps Information Disclosure	2.6 (Low)	80 %	172.16.14.52		general/tcp	Mon, Jul 31, 2023 7:55 PM UTC
ICMP Timestamp Reply Information Disclosure	2.1 (Low)	80 %	172.16.14.52		general/icmp	Mon, Jul 31, 2023 7:55 PM UTC

Windows server:

Vulnerability	Severity ▼	QoD	Host IP	Name	Location	Created
SSL/TLS: Report Weak Cipher Suites	5.0 (Medium)	98 %	172.16.14.53		3389/tcp	Mon, Jul 31, 2023 8:19 PM UTC
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80 %	172.16.14.53		135/tcp	Mon, Jul 31, 2023 8:21 PM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)	98 %	172.16.14.53		3389/tcp	Mon, Jul 31, 2023 8:19 PM UTC
TCP Timestamps Information Disclosure	2.6 (Low)	80 %	172.16.14.53		general/tcp	Mon, Jul 31, 2023 8:18 PM UTC
ICMP Timestamp Reply Information Disclosure	2.1 (Low)	80 %	172.16.14.53		general/icmp	Mon, Jul 31, 2023 8:18 PM UTC

The findings shows us that Windows 1 and Linux machine has crucial vulnerabilities with high severity levels more than 6.9 whereas windows server has medium and low severe vulnerabilities.

Risk assessment: In Cat's company, there is little vulnerability in the network. The following finding shows the severity index of vulnerabilities in the network. This includes the Kali machine as well.

Vulnerability	Severity ▼	QoD	Host IP	Name	Location	Created
Operating System (OS) End of Life (EOL) Detection	10.0 (High)	80 %	172.16.14.50		general/tcp	Mon, Jul 31, 2023 8:55 PM UTC
Unprotected OSSEC/Wazuh ossec-authd (authd Protocol)	7.5 (High)	80 %	172.16.14.52		1515/tcp	Mon, Jul 31, 2023 7:53 PM UTC
HTTP Brute Force Logins With Default Credentials Reporting	7.5 (High)	95 %	172.16.14.52		9200/tcp	Mon, Jul 31, 2023 7:59 PM UTC
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80 %	172.16.14.50		135/tcp	Mon, Jul 31, 2023 8:57 PM UTC
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80 %	172.16.14.3		135/tcp	Mon, Jul 31, 2023 4:46 PM UTC
SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	5.0 (Medium)	70 %	172.16.14.52		1515/tcp	Mon, Jul 31, 2023 7:58 PM UTC
SSL/TLS: Report Weak Cipher Suites	5.0 (Medium)	98 %	172.16.14.53		3389/tcp	Mon, Jul 31, 2023 8:19 PM UTC
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80 %	172.16.14.53		135/tcp	Mon, Jul 31, 2023 8:21 PM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)	98 %	172.16.14.3		3389/tcp	Mon, Jul 31, 2023 4:45 PM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)	98 %	172.16.14.53		3389/tcp	Mon, Jul 31, 2023 8:19 PM UTC

Apply to page contents

SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability		4.0 (Medium)	80 %	172.16.14.52	9300/tcp	Mon, Jul 31, 2023 7:56 PM UTC
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability		4.0 (Medium)	80 %	172.16.14.52	9200/tcp	Mon, Jul 31, 2023 7:56 PM UTC
TCP Timestamps Information Disclosure		2.6 (Low)	80 %	172.16.14.53	general/tcp	Mon, Jul 31, 2023 8:18 PM UTC
TCP Timestamps Information Disclosure		2.6 (Low)	80 %	172.16.14.2	general/tcp	Mon, Jul 31, 2023 5:08 PM UTC
TCP Timestamps Information Disclosure		2.6 (Low)	80 %	172.16.14.52	general/tcp	Mon, Jul 31, 2023 7:55 PM UTC
TCP Timestamps Information Disclosure		2.6 (Low)	80 %	172.16.14.50	general/tcp	Mon, Jul 31, 2023 8:55 PM UTC
ICMP Timestamp Reply Information Disclosure		2.1 (Low)	80 %	172.16.14.50	general/icmp	Mon, Jul 31, 2023 8:55 PM UTC
ICMP Timestamp Reply Information Disclosure		2.1 (Low)	80 %	172.16.14.53	general/icmp	Mon, Jul 31, 2023 8:18 PM UTC
ICMP Timestamp Reply Information Disclosure		2.1 (Low)	80 %	172.16.14.52	general/icmp	Mon, Jul 31, 2023 7:55 PM UTC
ICMP Timestamp Reply Information Disclosure		2.1 (Low)	80 %	172.16.14.2	general/icmp	Mon, Jul 31, 2023 5:07 PM UTC

Apply to page contents

HIGH	MEDIUM	LOW
3	**2**	**1**

Recommendations:

Recommendation is this report is based on the available findings from the credential patch audit. I suggest the following are the remediation's actions across all the devices that will resolve the 95% of the vulnerabilities on the network. Solutions are also provided to Cat to mitigate any threat by implementing the solutions.

HIGH/crucial severity

Device	Vulnerability	Severity index value	Mitigation solution
Windows1	The operating system(OS) on the remote host has reached the end of life (EOL) and should not be used anymore	10.0	Upgrade the OS on the remote host to a version which is still supported and receiving security updates by the vendor.
LINUX	The remote OSSEC/Wazuh ossec-authd service is not protected by password authentication or client certificate verification	7.5	Workaround needed. Enable password authentication or client verification within the configuration of ossec-authd.
LINUX	It was possible to login into the remote Web applications using default credentials.	7.5	Mitigation : change password asap References: **CVE-1999-0501** **CVE-1999-0502** **CVE-1999-0507** **CVE-1999-0508**

MEDIUM severity

Devices	Vulnerabilities	Severity index	Recommended solutions
Windows Server	This routine reports all weal SSL/TLS cipher suits accepted	5.0	The configuration of this services should be changed so that it doesn't accept the listed weak cipher suites anymore.
Windows Server	Distributed computing environment/ remote procedure calls(DCE/RPC) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.	5.0	Filter incoming traffic to this post
Windows Server	It was possible to detect the usage of the deprecated TLVv1.0 and or TLSv1.1 protocol on this system	4.3	It is recommended to disable the deprecated TLSv1.0 and TLSv1.1 protocols in favor of the TLSv1.2+ protocols.

LOW Index value:

It's a general vulnerability.

Date ▼	Status	Task	Severity	High	Medium	Low	Log	False Pos.	Actions
Mon, Jul 31, 2023 7:47 PM UTC	Done	Immediate scan of IP 172.16.14.51	0.0 (Log)	0	0	0	4	0	

Citations:

https://purplesec.us/wp-content/uploads/2019/03/Sample-Network-Security-Vulnerability-Assessment-Report-Purplesec.pdf

https://tryhackme.com/room/openvas

https://www.esecurityplanet.com/networks/vulnerability-scanning-what-it-is-and-how-to-do-it-right/

PowerPoint presentation:

https://docs.google.com/presentation/d/1WeLSizvIpYEz8kvMKmK85oZ-B2c_0RUL/edit#slide=id.p1