Executive Summary: Cybersecurity Assessment Report

A. SCOPE

Introduction: This report provides a high-level overview of the recent cybersecurity assessment conducted for [Customer Organization]. The assessment aimed to evaluate the organization's security posture, identify potential risks, and highlight areas for improvement. The findings are summarized below for the senior leadership of [Customer Organization].

Key Risks: The assessment revealed several key risks that warrant attention and proactive management. These risks include:

- **Phishing and Social Engineering:**
- Employees are susceptible to phishing attacks, posing a significant risk to sensitive information.
- Lack of awareness and training increases the likelihood of successful social engineering attempts.
- **Outdated Software and Patching:**
- Some systems and applications are running outdated software versions, exposing vulnerabilities.
- Inconsistent patch management practices contribute to an increased risk of exploitation.
- **Insufficient Access Controls:**
- Inconsistent enforcement of access controls may lead to unauthorized access to critical systems.
- Limited monitoring and auditing of user access increase the potential for insider threats.
- **Inadequate Incident Response Plan:**
- The current incident response plan lacks comprehensiveness and may result in delayed response times during security incidents.
- Limited testing and training contribute to potential gaps in the effectiveness of the plan.

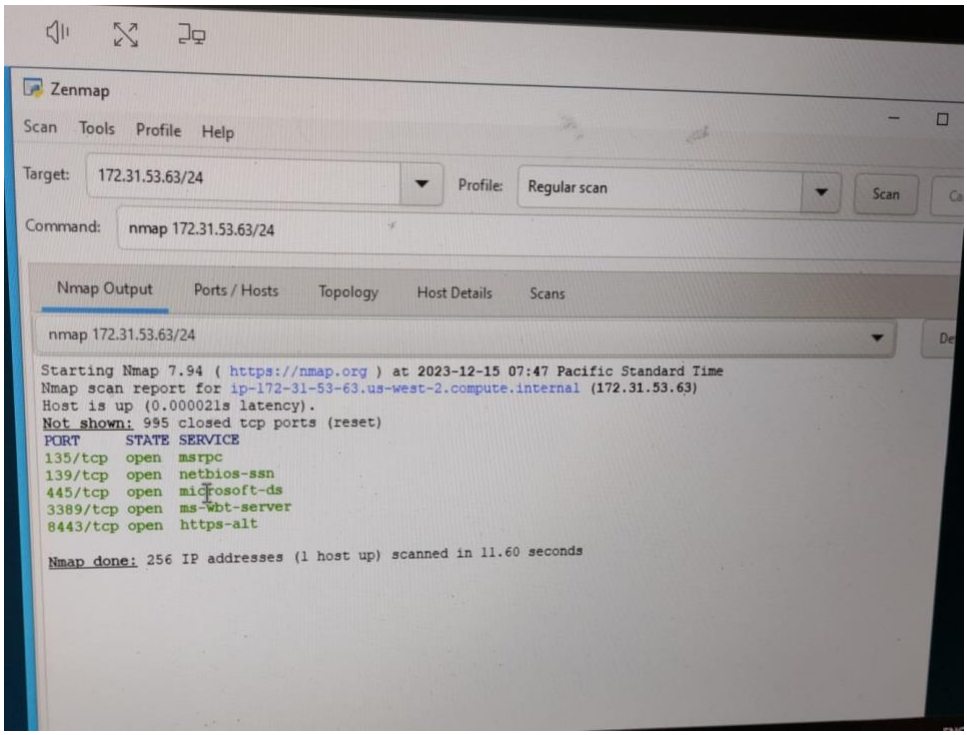
<u>Steps to be followed:</u>

<u>1</u> Information gathering and recon
2. Enumeration and service scanning
3. Vulnerability assessment
4. Vulnerability classification and ranking
5. Conclusion

B. Findings from Executive Dashboard:

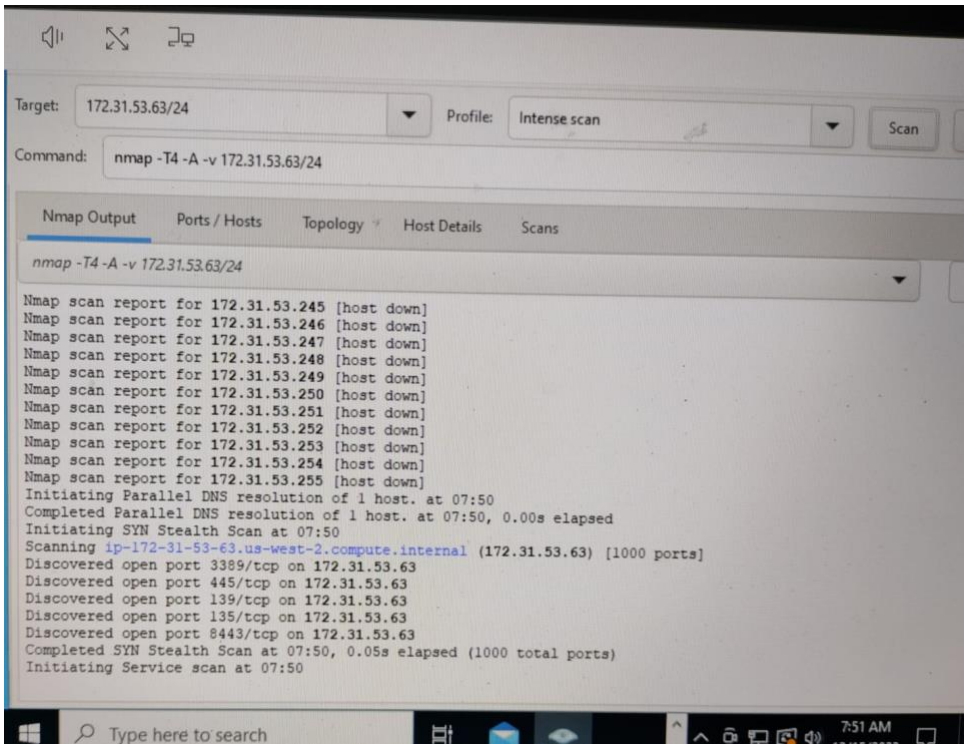
The executive dashboard provided a concise visual representation of the organization's cybersecurity posture. Key findings include:

1. Results for regular scan using Zenmap on Windows



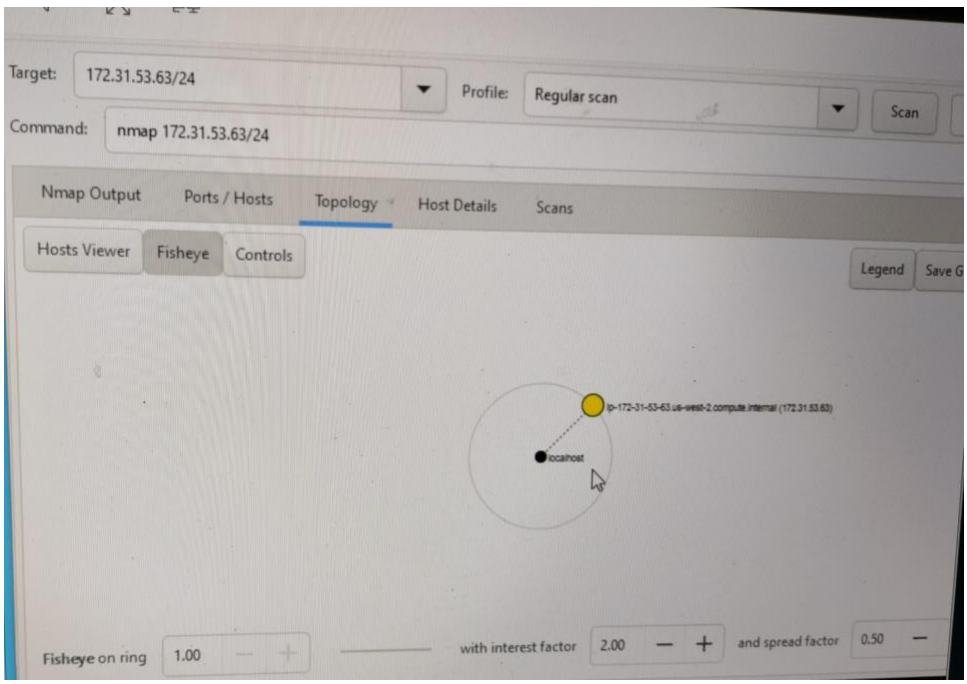
<u>Findings</u>:- When a regular scan is done on Windows with subnet 172.31.53.63/24 , It shows 5 open ports mentioned in the figure.

2. Results for intense scan using Zenmap on Windows



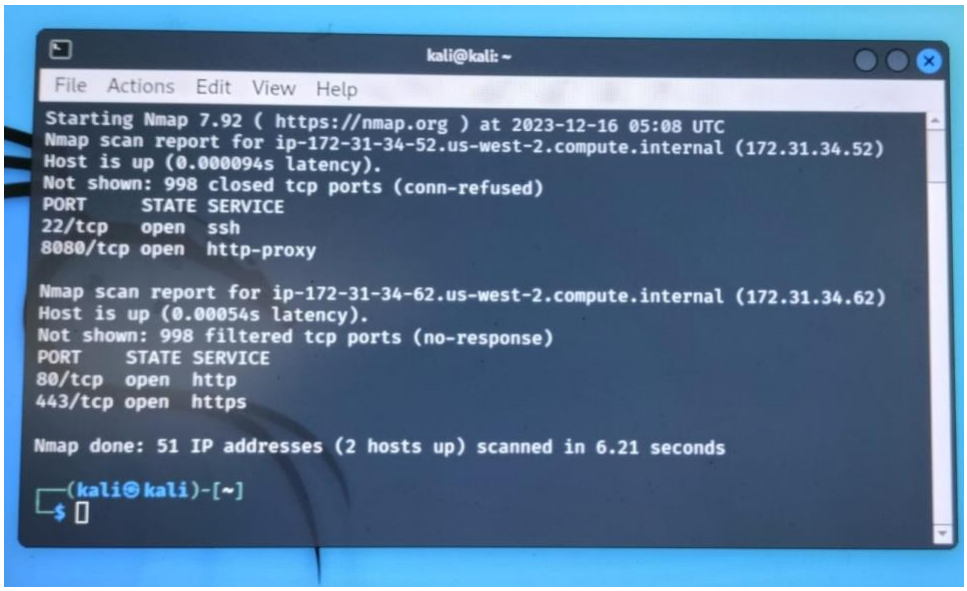
<u>Findings</u>:- It has done a comprehensive scan with IP add or subnet 172.31.53.63/24 and shows tcp ports 3389, 445, 139, 135, 8443 are open.

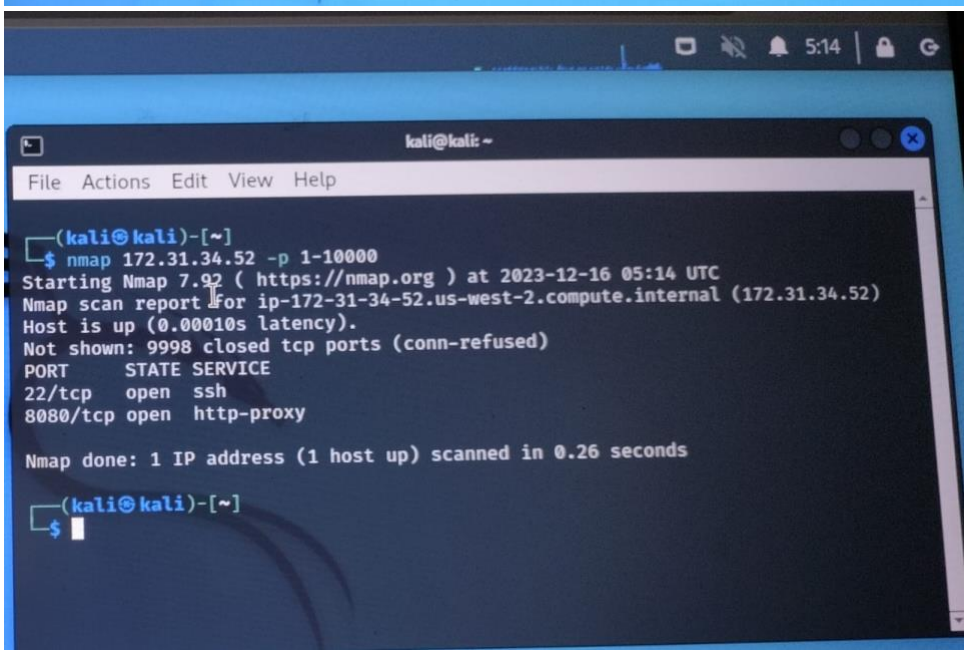
3. Topology

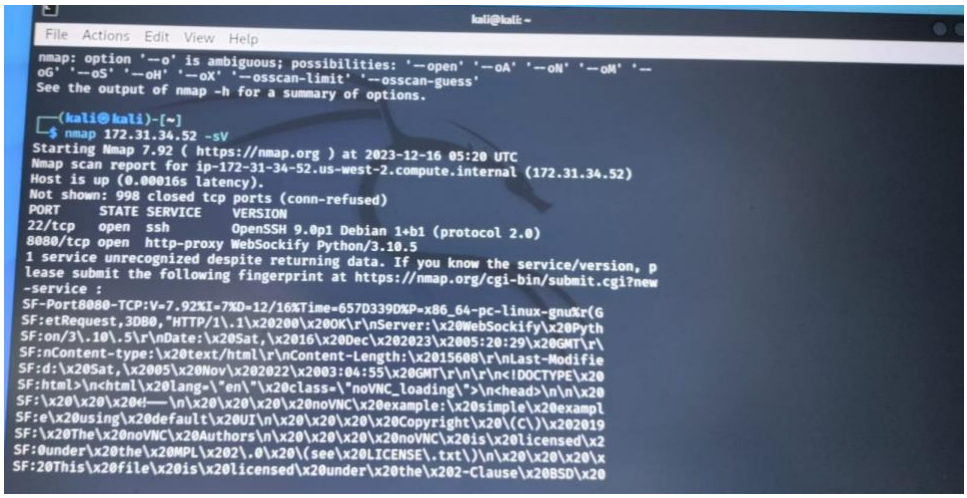


Findings:- The above figure helps to identify the target system for further reconnaissance

4. Results for regular and Intense scan on Kali/ Debian Linux





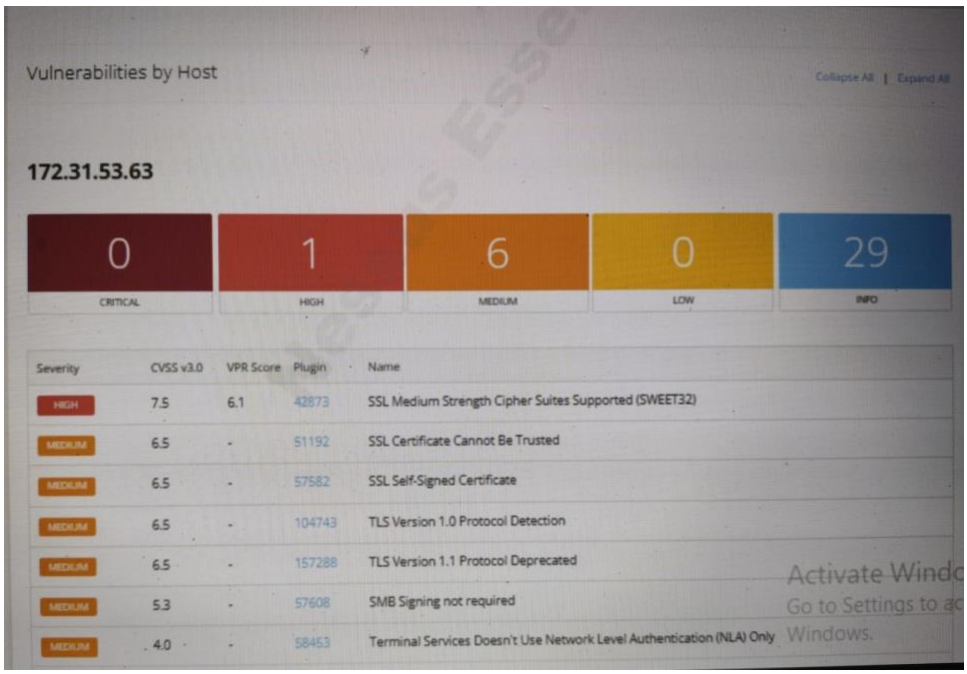


```
kali@kali: ~
File  Actions  Edit  View  Help
nmap: option '--o' is ambiguous; possibilities: '--open' '--oA' '--oN' '--oM' '--
oG' '--oS' '--oH' '--oX' '--osscan-limit' '--osscan-guess'
See the output of nmap -h for a summary of options.

┌──(kali㉿kali)-[~]
└─$ nmap 172.31.34.52 -sV
Starting Nmap 7.92 ( https://nmap.org ) at 2023-12-16 05:20 UTC
Nmap scan report for ip-172-31-34-52.us-west-2.compute.internal (172.31.34.52)
Host is up (0.00016s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 9.0p1 Debian 1+b1 (protocol 2.0)
8080/tcp open  http-proxy WebSockify Python/3.10.5
1 service unrecognized despite returning data. If you know the service/version, p
lease submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new
-service :
SF-Port8080-TCP:V=7.92%I=7%D=12/16%Time=657D339D%P=x86_64-pc-linux-gnu%r(G
SF:etRequest,3D80,"HTTP/1\.1\x20200\x20OK\r\nServer:\x20WebSockify\x20Pyth
SF:on/3\.10\.5\r\nDate:\x20Sat,\x2016\x20Dec\x202023\x2005:20:29\x20GMT\r\
SF:nContent-type:\x20text/html\r\nContent-Length:\x2015608\r\nLast-Modifie
SF:d:\x20Sat,\x2005\x20Nov\x202022\x2003:04:55\x20GMT\r\n\r\n<!DOCTYPE\x20
SF:html>\n<html\x20lang=\"en\"\x20class=\"noVNC_loading\">\n<head>\n\n\x20
SF:\x20\x20\x20<!--\n\x20\x20\x20\x20noVNC\x20example:\x20simple\x20exampl
SF:e\x20using\x20default\x20UI\n\x20\x20\x20\x20Copyright\x20\(C\)\x202019
SF:\x20The\x20noVNC\x20Authors\n\x20\x20\x20\x20noVNC\x20is\x20licensed\x2
SF:0under\x20the\x20MPL\x202\.0\x20\(see\x20LICENSE\.txt\)\n\x20\x20\x20\x
SF:20This\x20file\x20is\x20licensed\x20under\x20the\x202-Clause\x20BSD\x20
```

Findings:- Here tcp ports 22 and tcp port 8080 are open when scans are done on Kali/ Debian linux

5. Results for Vulnerability Assessment on Windows using Nessus tool



Vulnerabilities by Host

Collapse All | Expand All

172.31.53.63

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	1	6	0	29

Severity	CVSS v3.0	VPR Score	Plugin	Name
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	157288	TLS Version 1.1 Protocol Deprecated
MEDIUM	5.3	-	57608	SMB Signing not required
MEDIUM	4.0	-	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only

INFO	N/A	-	10940	Remote Desktop Protocol Service Detection
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	64814	Terminal Services Use SSL/TLS
INFO	N/A	-	135860	WMI Not Available
INFO	N/A	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

* indicates the v3.0 score was not available; the v2.0 score is shown

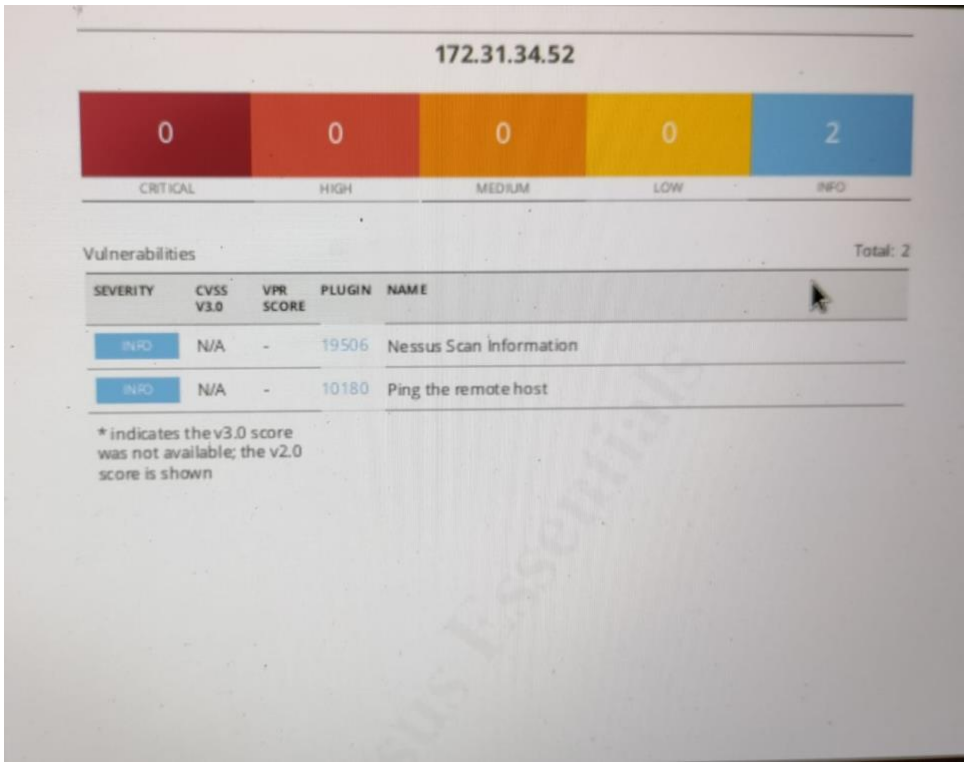
New Tab | Nessus Essentials | My Basic Network Sca

file:///C:/Users/labsuser/Downloads/My Basic Network 67%

INFO	N/A	-	12634	Authenticated Check : OS Name and Installed Package Enumeration
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	10736	DCE Services Enumeration
INFO	N/A	-	54615	Device Type
INFO	N/A	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	46215	Inconsistent Hostname and IP Address
INFO	N/A	-	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
INFO	N/A	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	97993	OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	66173	RDP Screenshot
INFO	N/A	-	10940	Remote Desktop Protocol Service Detection

<u>Findings</u>:- There are 0 critical 1 high risk and 6 medium risk vulnerabilities are found on Windows with IP Address 172.31.53.63 using Nessus tool.

6. Results for Vulnerability Assessment on Kali/Debian Linux



172.31.34.52

0	0	0	0	2
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 2

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10180	Ping the remote host

* indicates the v3.0 score was not available; the v2.0 score is shown

Findings:- No critical vulnerability is found when Nessus scan is done on Linus (Kali/ Debian) with IP address 172.31.34.52

C. Preventive suggestions:-

- **Risk Distribution:**
- Risks are distributed across various departments, emphasizing the need for a holistic approach to cybersecurity.
- **Incident Trends:**
- A notable increase in security incidents, particularly phishing attempts, highlights the urgency for improved security measures.
- **Compliance Status:**
- Some areas require attention to ensure compliance with industry standards and regulations.

Areas of Improvement: To enhance the organization's cybersecurity resilience, the following areas require immediate attention:

- **Employee Training:**
- Implement a comprehensive cybersecurity training program to educate employees on phishing risks and best practices.
- **Patch Management:**
- Establish a robust and consistent patch management process to promptly address software vulnerabilities.
- **Access Control Enhancements:**

- Strengthen access controls through regular reviews, privileged access management, and enhanced monitoring.
- **Incident Response Plan Enhancement:**
- Review and update the incident response plan, ensuring regular testing and training for all relevant stakeholders.

D. Conclusion: Addressing the identified risks and implementing improvements in the highlighted areas is crucial for strengthening [Customer Organization]'s cybersecurity posture. By proactively managing these challenges, the organization can significantly reduce the risk of security incidents and better safeguard its sensitive information.

For further details and a more in-depth technical analysis, the detailed assessment report is available upon request.