3.3 Report on the results of the attacks.

Report & recommend based on execution

1.Overview

This report presents the execution of a series of ethical hacking attacks from 3.2 based on the plan from 3.1. The attacks were made on the various targets and explored various vulnerabilities on the a system and network by using different technologies and tools. The purpose of this task is to identify vulnerabilities that could harm to the system and could be exploited by malicious actors and to recommend mitigations to enhance the overall security posture.

2.Key Findings

As a result, found vulnerabilities on the servers, systems, using weak passwords, outdated software versions, multiple open ports, unused subdomains and servers.

Critical – regsvc service in Microsoft windows 2000 system could lead to DoS attack

High - MS 17-010, CVSS 10.0

Medium – weak password for log in

3.Recommendation

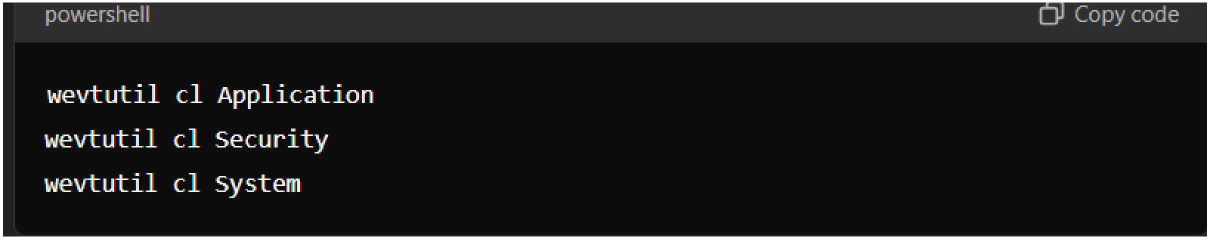
- Update OS version. Always use the latest version. Upgrade to Windows 11 or Window Server 2022.
- Apply security patches.
- Perform network segmentation by isolating the vulnerable system from the network.
- Use firewalls to restrict network traffic to and from regsvc service will reduce the exoploitation.
- Apply IPS/IDS to detect and block exploitation attempts of MS 17-010.
- Regular Vulnerability scanning.
- Implement strong password polices, eg- minimum 12 characters, a mix of upper and lower case, numbers, and special characters. Regular password changes (eg. Every 90 days). Don’t use previously used passwords again.

Clear Tracks

After written report, clear tracks of ethical hacking activities. Ensure the command history is its original state. Validate the network and system are functioning as normal.

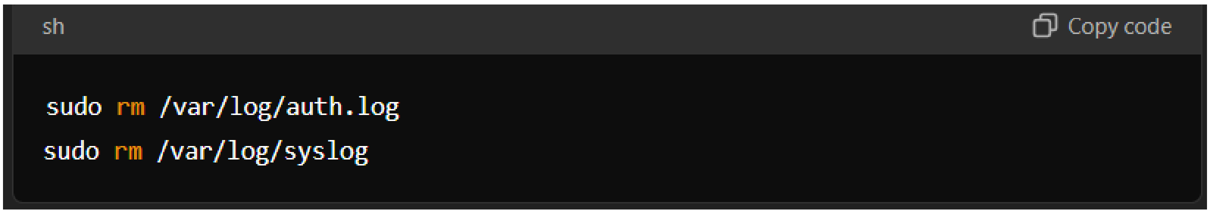
1.Perform log deletion – because system logs can contain records of the attacker's activities.

Clear Window Event Logs



```
wevtutil cl Application
wevtutil cl Security
wevtutil cl System
```

Fig (3.3/1) clearing specific logs in command line

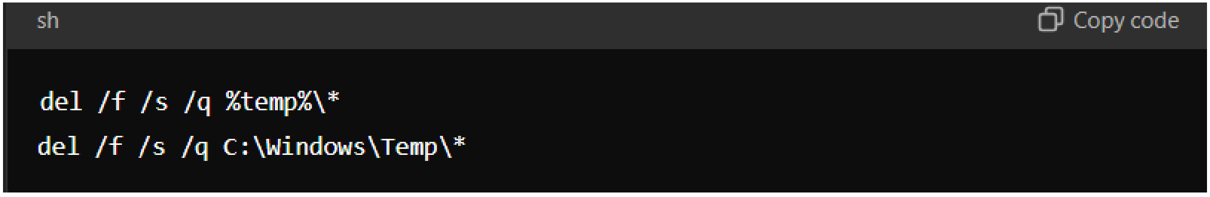


```
sudo rm /var/log/auth.log
sudo rm /var/log/syslog
```

Fig (3.3/2) clearing Linux logs

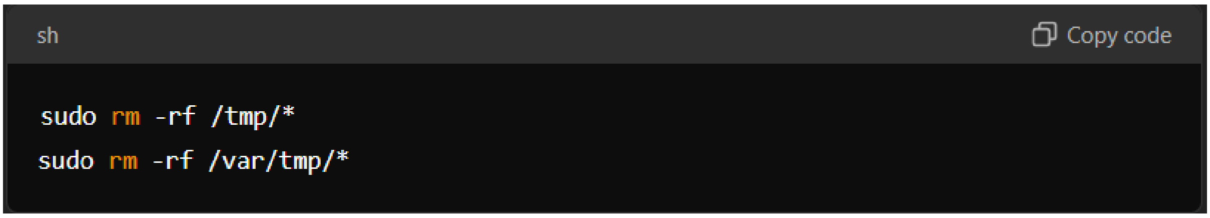
2. Delete history and prevent saving history.

3.Remove temporary files



```
del /f /s /q %temp%\*
del /f /s /q C:\Windows\Temp\*
```

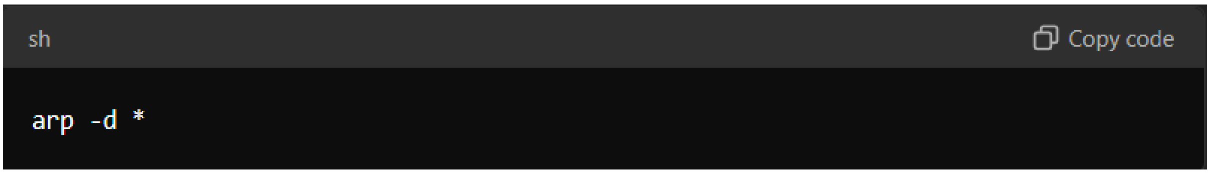
Fig (3.3/3) Window command for removing temporary files



```
sudo rm -rf /tmp/*
sudo rm -rf /var/tmp/*
```

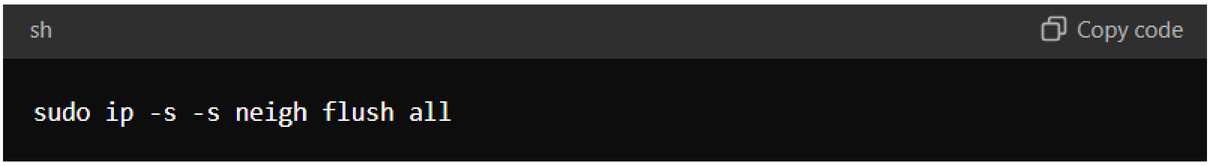
Fig (3.3/4) Linux command for removing temporary files

4.Network Cleanup – Clear network activities such as closing connections, removing ARP cache entries.



```
arp -d *
```

Fig (3.3/5) Window command for ARP clearing



```sh
sudo ip -s -s neigh flush all
```

Fig (3.3/6) ARP cleaning Linux command