2024

Penetration Testing Report for DePaulSecLabs, Inc.

CONDUCTED BY DEPAULSECLABS, INC.
SOMOGYI, ERIC – CSEC-488

DEPAULSECLABS, INC. | 25 E Jackson St. Chicago, IL 60604

Table of Contents

Executive Summary

This report is a summary of the penetration test conducted by DePaulSecLabs, Inc for the client DePaulSecLabs, Inc. Within this report, the results of this internal penetration test for our client DePaulSecLabs, Inc. with the domain name csec388.depalseclabs.com. The subject of these tests was 4 hosts within the Local Area Network (LAN) of the network IP range of the 10.12.0.0/24 subnet.

This penetration test was conducted using the Blackbox approach and is a CTF-style internal network penetration test. This CTF style approach includes for each target a FLAG in the format of CSEC-XXXX-XXXX for each vulnerability that was exploited. This approach used offensive security practices simulating a real-world penetration testing scenario to assess the effectiveness of existing security controls. The report details the methodologies used, risk assessments, severity levels, and remediation recommendations for each vulnerability. The purpose of this report is to ensure that the client has a full understanding of the penetration test and for each FLAG the detailed findings below:

- Methodologies used
- Risk of each vulnerability
- Severity
- Recommendations for remediation

Furthermore, the techniques used are mapped to the MITRE ATT&CK framework to provide a comprehensive understanding of the attack vectors. This report serves to inform DePaulSecLabs, Inc. of their current security posture, enabling them to take proactive steps to mitigate risks and enhance the overall security.

Objective

The objective of this penetration test was to discover vulnerabilities and exploit these vulnerabilities within the infrastructure of DePaulSecLabs, Inc. It was intended to simulate real-world attack scenarios, identify vulnerabilities, and provide recommendations for remediation. According to the initial client meeting, our 4 target virtual machine addresses do not have internet access.

Scope

Although 10.12.0.0/24 is DePaulSecLabs subnet, within that attack surface the only machines we were tasked with targeting were IP addresses 10.12.0.203, 10.12.0.89, 10.12.0.136, and 10.12.0.161. Also, from within this subnet we are running a Windows 10 client at IP address 10.12.0.15 and a Kali Linux machine running Debian version with an IP address of 10.12.0.25. From these two machines we were able to access the internet and access the targets in the 10.12.0.0/24 subnet.

Exclusions include:

- Physical Access: No physical access to DePaulSecLabs, Inc. premises or devices is permitted.
- Social Engineering: Social engineering tactics are outside the scope of this assessment.

Duration:

The time frame of this penetration test is considered short beginning on November 4, 2024 at 5:45pm and ending on November 18, 2024 5:44 pm.

Assumptions and Constraints

Assumptions:

The following criteria below are assumptions from the penetration testing environment:

1. The CEO of DePaulSecLabs, Inc. will provide assistance and access to information as required for the penetration test.
2. Network stability the penetration testing internal environment.
3. The technology used within the scope of this assessment is consistent.

Constraints:

The following are constraints during the duration of this penetration test:

1. The time available and availability of the DePaulSecLabs portal reservation time.
2. Access to the systems is and information is limited.

Methodology

The penetration testing methodology used during this penetration test is guided by the following guides and frameworks:

- Penetration Testing Execution Standard (PTES): http://www.pentest-standard.org/index.php/Main_Page
- OWASP Top 10 Web Application Security Risks 2021: https://owasp.org/www-project-top-ten/
- MITRE ATT&CK Tactics and techniques for Enterprise: https://attack.mitre.org/matrices/enterprise/
- Open-Source Intelligence (OSINT) Framework: https://osintframework.com/
- National Institute of Standards and Technology (NIST) publication SP 800-115: Technical Guide to Information Security Testing an Assessment https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

For further information on details of what each guide and standard does in detail, that information is available the links above. This methodology encompasses a structured approach to internal penetration testing, which allows the identification and mitigation of critical security risks within the client, DePaulSecLabs, Inc.'s IT infrastructure targets. This is possible because of the reconnaissance, identification of vulnerabilities, exploiting those vulnerabilities, and reporting the findings which include the severity levels and remediation recommendations and techniques and methods used.

Severity Rating

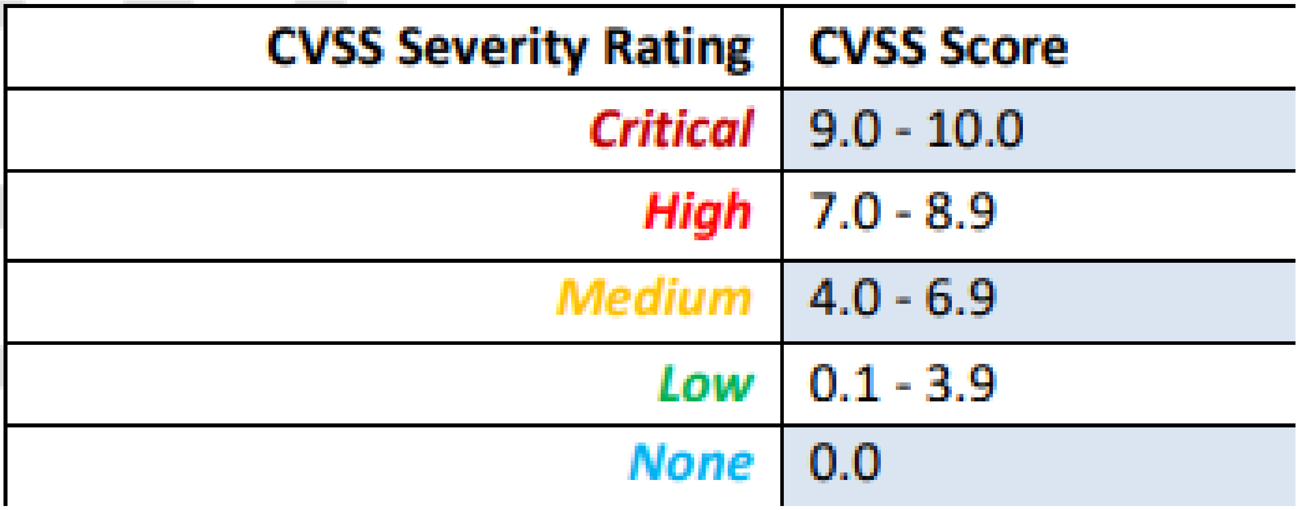
DepaulSecLabs follow the Common Vulnerability Scoring System (CVSS) version 3.x scoring system to rate vulnerabilities. Definition: “CVSS is a scoring system used to assess the severity of security vulnerabilities. It provides a numerical score (0.0 to 10.0) that indicates the risk level of a given vulnerability.” – (Source search.brave.com) The following bullet points are sourced and quoted from the NIST Vulnerability Database here: https://nvd.nist.gov/vuln-metrics/cvss. The CVSS assessment measures three areas:

- Base Metrics for qualities intrinsic to a vulnerability
  - Includes attack vector, complexity, privileges required, and impact.
- Temporal Metrics for characteristics that evolve over the lifetime of vulnerability.
  - Includes availability of the exploit as well.
- Environmental Metrics for vulnerabilities that depend on implementation or environment
  - Includes user roles or security controls in place in the current environment.

The findings in this report are scored on the base-metric rating of the vulnerability meaning. For example, the vulnerability, Eternal Blue CVE-2017-0144, has a CVSS Score of 8.8 High according to nvd.nist.gov of CVSS Version 3.x. – (Source): https://nvd.nist.gov/vuln/detail/cve-2017-0144

To view the Qualitative Severity rating scale for detailed definitions and details of severity ratings, please go to Appendix A in this report. So based on the severity of the vulnerabilities discovered, they are assigned the ratings below. **See Table A throughout this report below for reference:**

Table A:



CVSS Severity Rating	CVSS Score
Critical	9.0 - 10.0
High	7.0 - 8.9
Medium	4.0 - 6.9
Low	0.1 - 3.9
None	0.0

Risk Rating Classification

Review this table below which is intended to educate DePaulSecLabs, Inc about how the level of risk is defined in this report. It uses the likelihood and impact factors, and based on the combination of those to vulnerability is assigned a Risk Rating in Column 1. This is based off the NIST framework for Risk Assessments. Note to client for source credit - this table was generated with the assistance of AGI, based on the custom parameters we gave the AI tool in following the NIST framework. **See Table B below for reference throughout this report.**

Table B:

Risk Rating	Likelihood	Impact	Description
Very High	Almost Certain	Catastrophic	Exploitation is expected to occur imminently or has already occurred. This will lead to severe, widespread impact on operations, significant financial losses, or serious damage to reputation or legal compliance.
High	Likely	Major	Exploitation is probable within the next year. This will lead to considerable disruption of critical operations, substantial financial loss, or notable damage to reputation.
Moderate	Possible	Moderate	Exploitation may occur within the next few years. This could result in noticeable disruption of operations, financial impact, or reputational harm.
Low	Unlikely	Minor	Exploitation is not expected to occur, or the impact would be limited to minor operational inconvenience or minimal financial loss.

Summary of Findings

Vulnerabilities by severity:

The following table summarizes the key vulnerabilities discovered during this penetration test, categorized by their severity level and associated CVSS score. Each vulnerability is accompanied by a brief description and key remediation steps. The risk rating is determined based on a qualitative assessment of the likelihood and impact of each vulnerability.

Severity # Rank	Title	Severity Rating	CVSS Rating	Risk Rating	Key Remediation
1	**Credential Theft via XSS**	Critical	9.2	High	1. Review and restrict access permission
2	**Cloud Misconfiguration: Exposed S3 Bucket**	High	8.5	Medium	1.Update the web server software to the latest patched version.
3	**Unpatched Web Server Vulnerability**	High	8.1	High	1.Enforce a strong password policy with minimum length and complexity requirements. * Implement account lockout policies to prevent
4	**Weak Password Policy**	Medium	6	High	1Disable directory listing in the web server configuration. * Implement access controls to restrict access to sensitive directories 2.Regularly review web server configurations for security misconfigurations.

High-Level Recommendations

After conducting this first ever penetration test on DePaulSecLabs, Inc hosts on the network, in order to enhance the overall security posture, we are addressing the identified vulnerabilities in this report, and this is summarizing strategic high-level recommended actions to take to prevent these problems from reoccurring. For detailed actions to take, please see the remediation subsection in the technical report section for each vulnerability.

1. Close all unused TCP/UDP ports on each host. Only use encrypted channels for communication.
2. Apply system updates to the Operating systems as they become available. Some of the Operating systems running on the hosts are old versions and there are newly patched version available to download from the internet.
3. Apply patch management updates to all software, tools, and plugins that are necessary for the company to operate. Uninstall unnecessary tools and apps.
4. Conduct regular system scans, annual penetration tests, and vulnerability assessments.
5. Back up necessary drives and reset all machines with the most up to date versions.
6. Ensure that the client and servers being used on the internal network meet industry standard *current* best security practices.

Detailed Technical Report

10550 - SNMP Query Running Process List Disclosure

Flag 1 – CSEC-4848-SNMP – Method 1

System Vulnerable:

10.12.0.61 using the UDP protocol

Description:

The list of processes running on the remote host can be obtained via SNMP. An attacker can use this information to gather more information about the target host.

Steps taken:

1. First I conducted a Nmap scan of the entire 10.12.0.0/24 subnet
2. Next, I narrowed it down and ran a Nmap scan only on the target 10.12.0.161 and did not find anything.
3. I exported a generated report from the Nessus Server from port 8080 and analyzed it.
4. In the report on page 225, there is the FLAG under PID 1328 running calc.exe.

Exploit Method Used:

1. The Nessus Scanner itself performing SNMP enumeration.

CVE Vulnerability Classification:

There is no known CVE Vulnerability for this. There is also no known CVE directly assigned to the process calc.exe itself.

MITRE ATT&CK ID:

T1057 – Process Discovery https://attack.mitre.org/techniques/T1057/

Risk Rating: Low- information disclosure has minor impact. See Table B.

Severity: Low. See Table A.

Tools used:

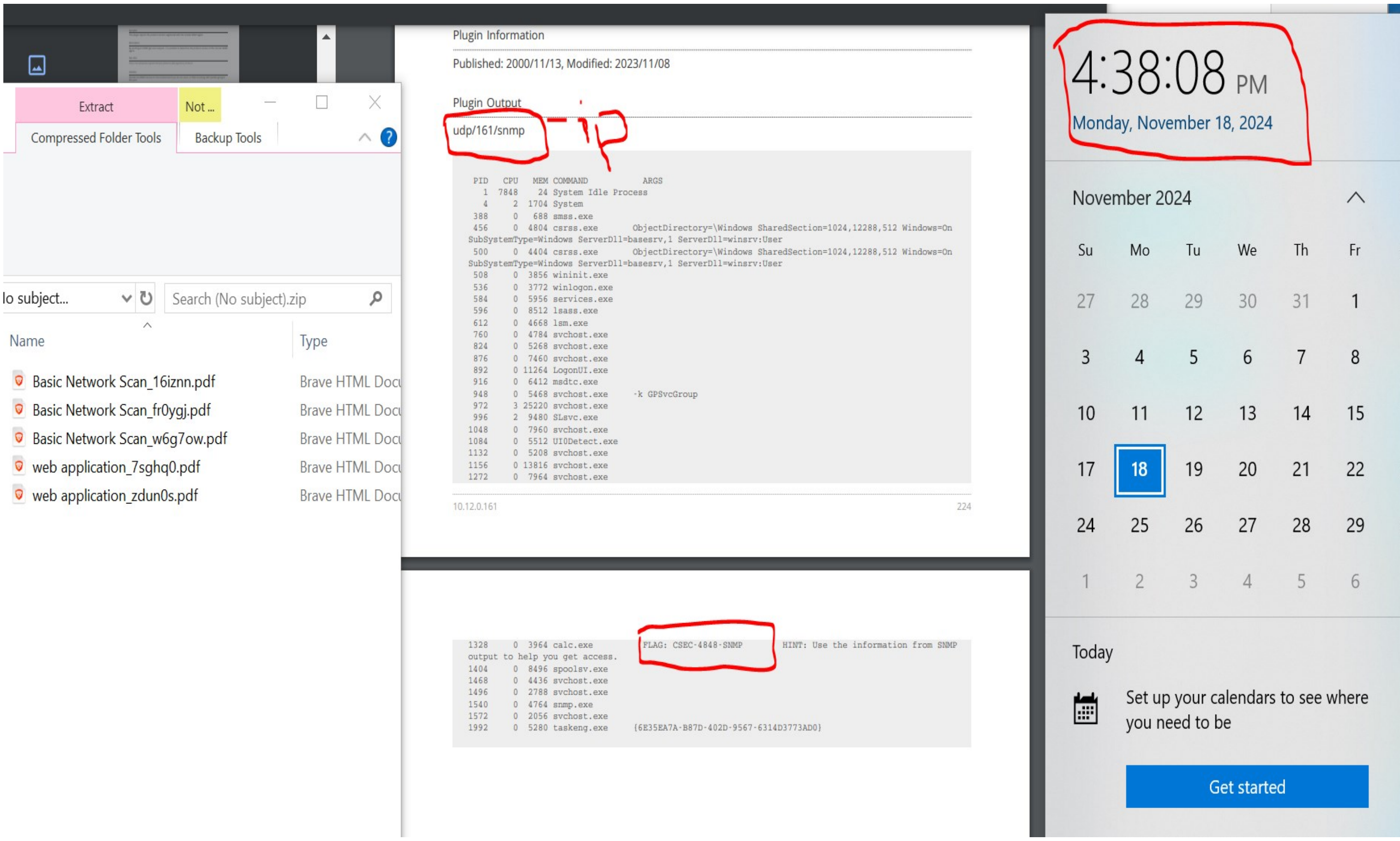
1. Nmap
2. PDF Viewer
3. Nessus Scanner

4. FireFox
5. Web Access to access Nessus download
6. Kali Linux

Remediation:

1. According to Nessus, disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

Proof of Vulnerability (See Screenshot below):



Plugin Information

Published: 2000/11/13, Modified: 2023/11/08

Plugin Output

udp/161/snmp

```
  PID   CPU   MEM COMMAND            ARGS
    1  7848    24 System Idle Process
    4     2  1704 System
  388     0   688 smss.exe
  456     0  4804 csrss.exe       ObjectDirectory=\Windows SharedSection=1024,12288,512 Windows=On
 SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:User
  500     0  4404 csrss.exe       ObjectDirectory=\Windows SharedSection=1024,12288,512 Windows=On
 SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:User
  508     0  3856 wininit.exe
  536     0  3772 winlogon.exe
  584     0  5956 services.exe
  596     0  8512 lsass.exe
  612     0  4668 lsm.exe
  760     0  4784 svchost.exe
  824     0  5268 svchost.exe
  876     0  7460 svchost.exe
  892     0 11264 LogonUI.exe
  916     0  6412 msdtc.exe
  948     0  5468 svchost.exe     -k GPSvcGroup
  972     3 25220 svchost.exe
  996     2  9480 SLsvc.exe
 1048     0  7960 svchost.exe
 1084     0  5512 UI0Detect.exe
 1132     0  5208 svchost.exe
 1156     0 13816 svchost.exe
 1272     0  7964 svchost.exe
```

10.12.0.161 224

```
 1328     0  3964 calc.exe          FLAG: CSEC-4848-SNMP        HINT: Use the information from SNMP
 output to help you get access.
 1404     0  8496 spoolsv.exe
 1468     0  4436 svchost.exe
 1496     0  2788 svchost.exe
 1540     0  4764 snmp.exe
 1572     0  2056 svchost.exe
 1992     0  5280 taskeng.exe     {6E35EA7A-B87D-402D-9567-6314D3773AD0}
```

2.
3.

Flag 1 – CSEC-4848-SNMP – Method #2 - BONUS

System Vulnerable: 10.12.0.161

Steps taken:

1. After analyzing the Nessus scan, I used a Linux tool called SNMPwalk.
2. I performed an SNMP enumeration scan on the target using SNMPwalk.
3. The results were many many pages so I had to scroll and analyze the results by scrolling to see all the results from the SNMP GETNEXT requests that the tool performs sequentially. This is called extracting the flag from the SNMP output.

Exploit Method Used: SNMP Enumeration

CVE Vulnerability Classification: There is no known CVE Vulnerability for this. There is also no known CVE directly assigned to the process calc.exe itself.

MITRE ATT&CK ID:

Risk Rating: Low- information disclosure has minor impact. See Table B.

Severity: Low. See Table A.

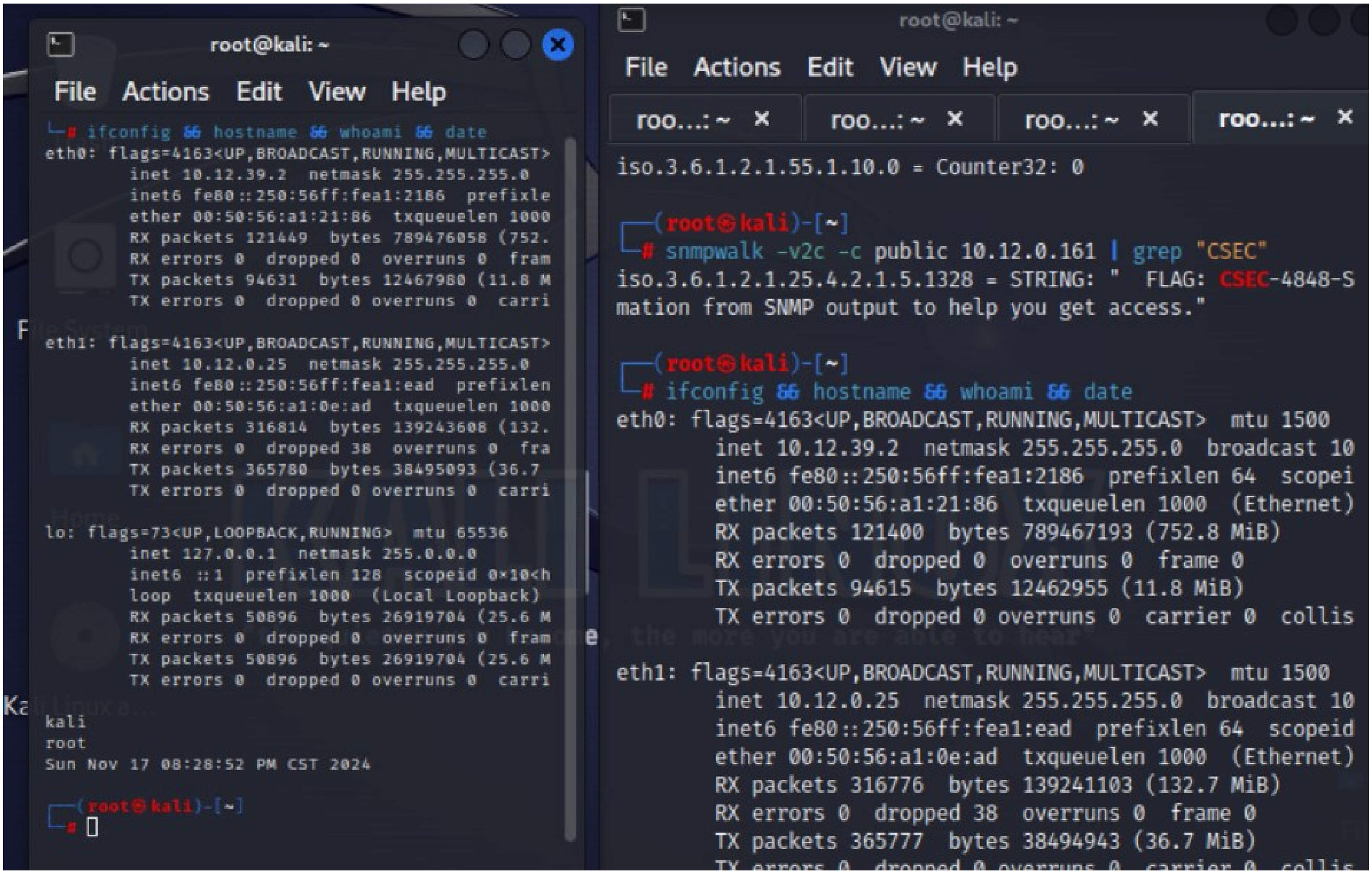
Tools used:

1. Snmpwalk which is a command line tool used to retreieve management information from a network device using the Simple Network Management Protocol (SNMP).
2. Kali Linux

Remediation:

1. Restrict SNMP by configuring SNMP to only allow authorized management stations to access it.
2. System administrators update the system to use SNMP version 3 for better security.

Proof of Vulnerability below:



```
└─# ifconfig && hostname && whoami && date
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>
        inet 10.12.39.2  netmask 255.255.255.0
        inet6 fe80::250:56ff:fea1:2186  prefixle
        ether 00:50:56:a1:21:86  txqueuelen 1000
        RX packets 121449  bytes 789476058 (752.
        RX errors 0  dropped 0  overruns 0  fram
        TX packets 94631  bytes 12467980 (11.8 M
        TX errors 0  dropped 0 overruns 0  carri

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>
        inet 10.12.0.25  netmask 255.255.255.0
        inet6 fe80::250:56ff:fea1:ead  prefixlen
        ether 00:50:56:a1:0e:ad  txqueuelen 1000
        RX packets 316814  bytes 139243608 (132.
        RX errors 0  dropped 38  overruns 0  fra
        TX packets 365780  bytes 38495093 (36.7
        TX errors 0  dropped 0 overruns 0  carri

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<h
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 50896  bytes 26919704 (25.6 M
        RX errors 0  dropped 0  overruns 0  fram
        TX packets 50896  bytes 26919704 (25.6 M
        TX errors 0  dropped 0 overruns 0  carri

kali
root
Sun Nov 17 08:28:52 PM CST 2024

┌──(root㉿kali)-[~]
└─# 
```

```
iso.3.6.1.2.1.55.1.10.0 = Counter32: 0

┌──(root㉿kali)-[~]
└─# snmpwalk -v2c -c public 10.12.0.161 | grep "CSEC"
iso.3.6.1.2.1.25.4.2.1.5.1328 = STRING: "  FLAG: CSEC-4848-S
mation from SNMP output to help you get access."

┌──(root㉿kali)-[~]
└─# ifconfig && hostname && whoami && date
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.12.39.2  netmask 255.255.255.0  broadcast 10
        inet6 fe80::250:56ff:fea1:2186  prefixlen 64  scopei
        ether 00:50:56:a1:21:86  txqueuelen 1000  (Ethernet)
        RX packets 121400  bytes 789467193 (752.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 94615  bytes 12462955 (11.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collis

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.12.0.25  netmask 255.255.255.0  broadcast 10
        inet6 fe80::250:56ff:fea1:ead  prefixlen 64  scopeid
        ether 00:50:56:a1:0e:ad  txqueuelen 1000  (Ethernet)
        RX packets 316776  bytes 139241103 (132.7 MiB)
        RX errors 0  dropped 38  overruns 0  frame 0
        TX packets 365777  bytes 38494943 (36.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collis
```

10263 - SMTP Server Detection

Flag 2 – CSEC-0007-SMTP

Description: The remote host is running a mail (SMTP) server on this port 25. Since SMTP severs are the targets of spammers, it is recommended to disable if it's not being used.

System Vulnerable: 10.12.0.89

Steps taken:

1. I ran a basic network scan using nmap on target 10.12.0.136 first
2. After finding all the active open ports, I used netcat to connect to port 25.

Exploit Method Used: Banner Grabbing

CVE Vulnerability Classification: There is no known CVE Vulnerability for this. There is also no known CVE directly assigned to the process calc.exe itself.

MITRE ATT&CK ID: This method uses the Discovery Tactic and the Network Sniffing T1040 technique.

Risk Rating: Low- information disclosure has minor impact. See Table B.

Severity: Low. See Table A.

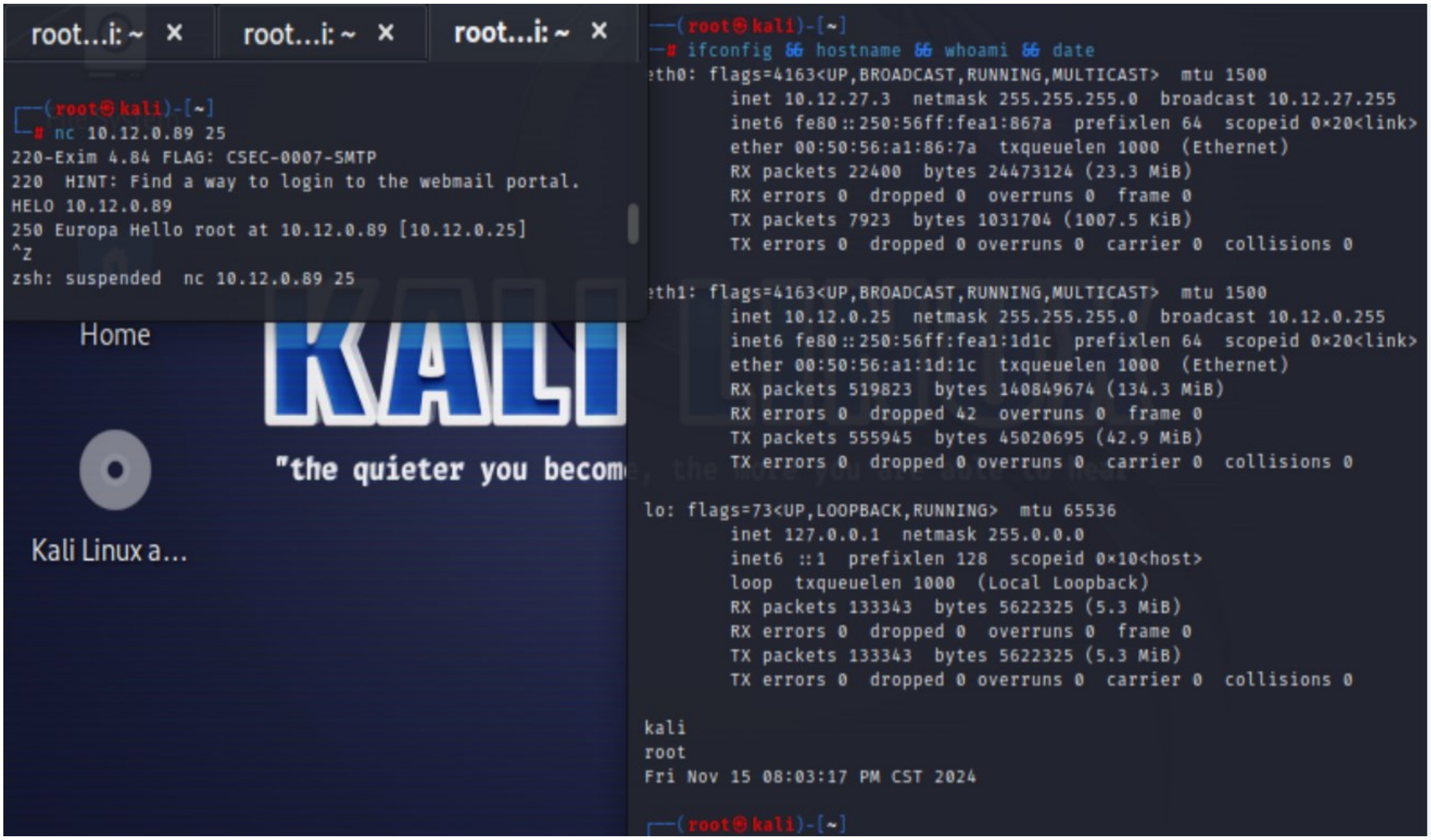
Tools used:

1. Nmap
2. Netcat

Remediation:

1. Configure the SMTP server port on the target to provide no banners.
2. Implement more secure firewall rules to deny the nmap traffic requests.
3. Disable the service if you do not use it or filter incoming traffic on this port.

Proof of Vulnerability below:



```
┌──(root㉿kali)-[~]
└─# nc 10.12.0.89 25
220-Exim 4.84 FLAG: CSEC-0007-SMTP
220  HINT: Find a way to login to the webmail portal.
HELO 10.12.0.89
250 Europa Hello root at 10.12.0.89 [10.12.0.25]
^Z
zsh: suspended  nc 10.12.0.89 25
```

```
┌──(root㉿kali)-[~]
└─# ifconfig && hostname && whoami && date
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.12.27.3  netmask 255.255.255.0  broadcast 10.12.27.255
        inet6 fe80::250:56ff:fea1:867a  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:a1:86:7a  txqueuelen 1000  (Ethernet)
        RX packets 22400  bytes 24473124 (23.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7923  bytes 1031704 (1007.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.12.0.25  netmask 255.255.255.0  broadcast 10.12.0.255
        inet6 fe80::250:56ff:fea1:1d1c  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:a1:1d:1c  txqueuelen 1000  (Ethernet)
        RX packets 519823  bytes 140849674 (134.3 MiB)
        RX errors 0  dropped 42  overruns 0  frame 0
        TX packets 555945  bytes 45020695 (42.9 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 133343  bytes 5622325 (5.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 133343  bytes 5622325 (5.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

kali
root
Fri Nov 15 08:03:17 PM CST 2024

┌──(root㉿kali)-[~]
```

Flag 3 – CSEC-3961-QOTD

System Vulnerable: 10.12.0.136

Steps taken:

1. A Nessus scan on the target host at 10.12.0.136
2. Observe the service banner in the scan output.

Exploit Method Used: Banner Grabbing

CVE Vulnerability Classification: There is no known CVE Vulnerability for this.

MITRE ATT&CK ID: This uses the Reconnaissance tactic, and this is the Active Scanning Technique T1595.002 or this could also be the Discovery Tactic and the Network Sniffing T1040 technique.

Risk Rating: Low- information disclosure has a minor impact. See Table B.

Severity: Low. See Table A.

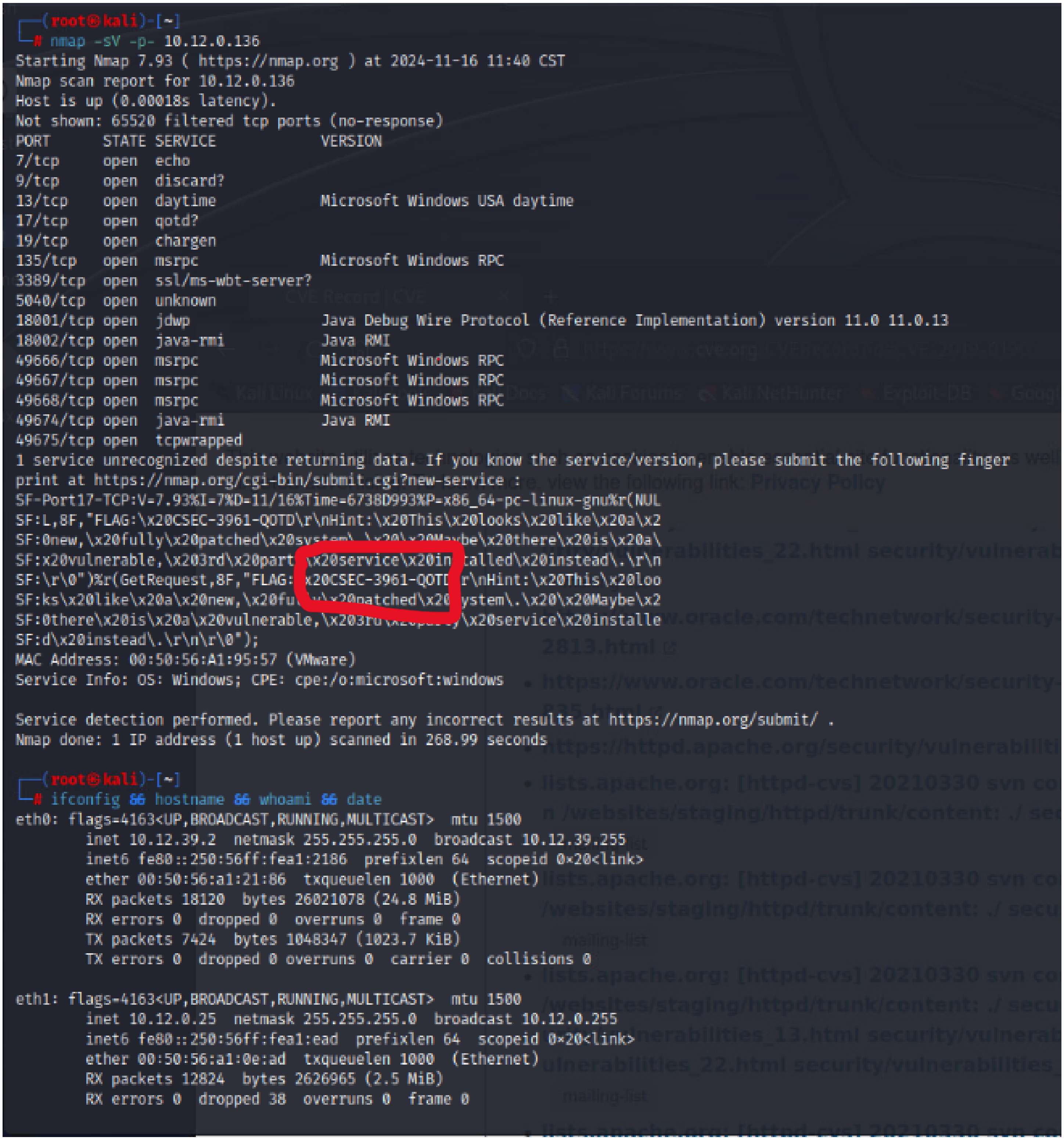
Tools used:

3. nmap

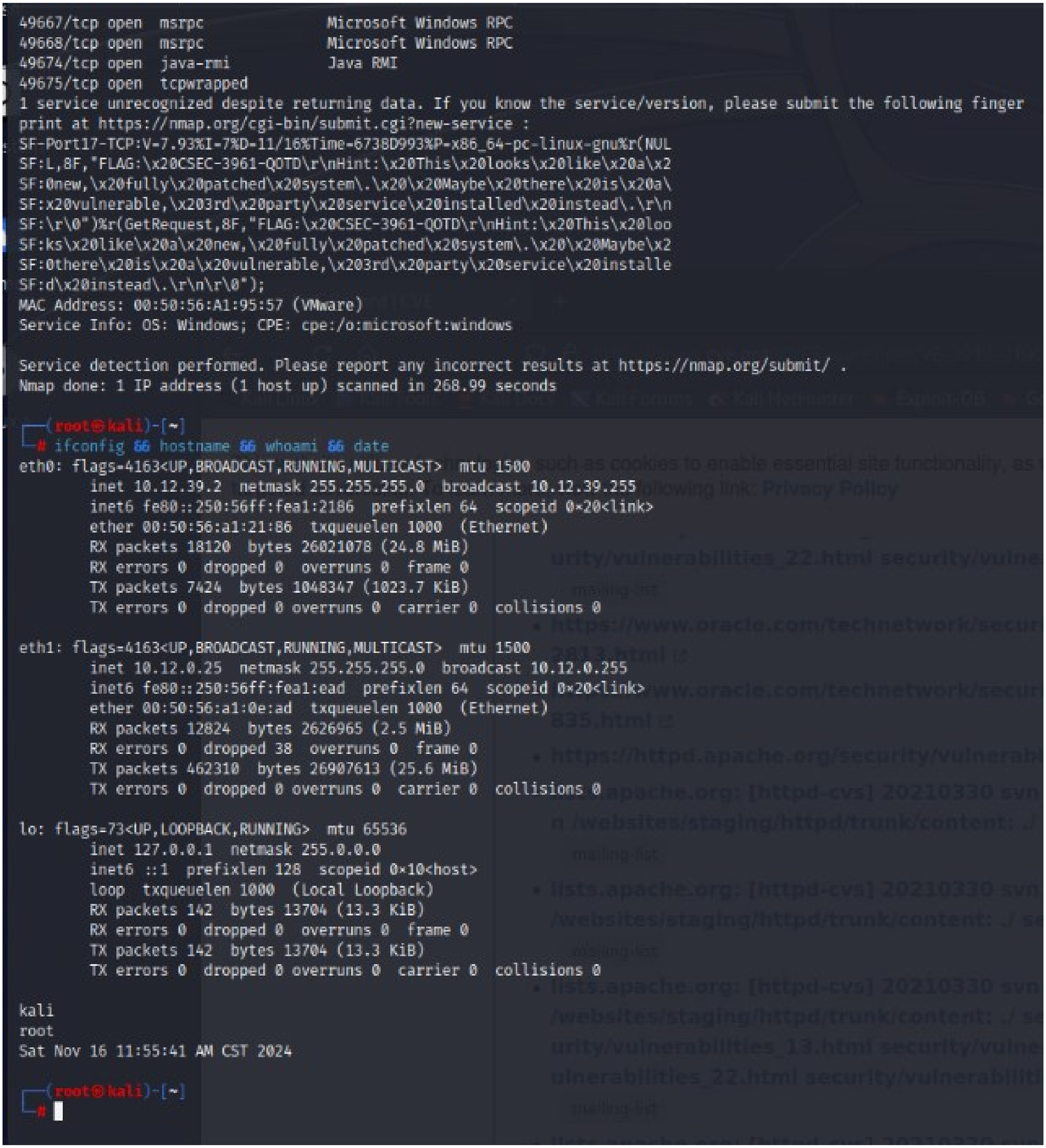
Remediation:

1. Limit banner information by configuring services on the target device. Have administrator tell the service to not advertise Version details.

Proof of Vulnerability below:



```
┌──(root㉿kali)-[~]
└─# nmap -sV -p- 10.12.0.136
Starting Nmap 7.93 ( https://nmap.org ) at 2024-11-16 11:40 CST
Nmap scan report for 10.12.0.136
Host is up (0.00018s latency).
Not shown: 65520 filtered tcp ports (no-response)
PORT      STATE SERVICE            VERSION
7/tcp     open  echo
9/tcp     open  discard?
13/tcp    open  daytime            Microsoft Windows USA daytime
17/tcp    open  qotd?
19/tcp    open  chargen
135/tcp   open  msrpc              Microsoft Windows RPC
3389/tcp  open  ssl/ms-wbt-server?
5040/tcp  open  unknown
18001/tcp open  jdwp               Java Debug Wire Protocol (Reference Implementation) version 11.0 11.0.13
18002/tcp open  java-rmi           Java RMI
49666/tcp open  msrpc              Microsoft Windows RPC
49667/tcp open  msrpc              Microsoft Windows RPC
49668/tcp open  msrpc              Microsoft Windows RPC
49674/tcp open  java-rmi           Java RMI
49675/tcp open  tcpwrapped
1 service unrecognized despite returning data. If you know the service/version, please submit the following finger
print at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port17-TCP:V=7.93%I=7%D=11/16%Time=6738D993%P=x86_64-pc-linux-gnu%r(NUL
SF:L,8F,"FLAG:\x20CSEC-3961-QOTD\r\nHint:\x20This\x20looks\x20like\x20a\x2
SF:0new,\x20fully\x20patched\x20system\.\x20\x20Maybe\x20there\x20is\x20a\
SF:x20vulnerable,\x203rd\x20party\x20service\x20installed\x20instead\.\r\n
SF:\r\0")%r(GetRequest,8F,"FLAG:\x20CSEC-3961-QOTD\r\nHint:\x20This\x20loo
SF:ks\x20like\x20a\x20new,\x20fully\x20patched\x20system\.\x20\x20Maybe\x2
SF:0there\x20is\x20a\x20vulnerable,\x203rd\x20party\x20service\x20installe
SF:d\x20instead\.\r\n\r\0");
MAC Address: 00:50:56:A1:95:57 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 268.99 seconds

┌──(root㉿kali)-[~]
└─# ifconfig && hostname && whoami && date
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.12.39.2  netmask 255.255.255.0  broadcast 10.12.39.255
        inet6 fe80::250:56ff:fea1:2186  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:a1:21:86  txqueuelen 1000  (Ethernet)
        RX packets 18120  bytes 26021078 (24.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7424  bytes 1048347 (1023.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.12.0.25  netmask 255.255.255.0  broadcast 10.12.0.255
        inet6 fe80::250:56ff:fea1:ead  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:a1:0e:ad  txqueuelen 1000  (Ethernet)
        RX packets 12824  bytes 2626965 (2.5 MiB)
        RX errors 0  dropped 38  overruns 0  frame 0
```



```
49667/tcp open  msrpc              Microsoft Windows RPC
49668/tcp open  msrpc              Microsoft Windows RPC
49674/tcp open  java-rmi           Java RMI
49675/tcp open  tcpwrapped
1 service unrecognized despite returning data. If you know the service/version, please submit the following finger
print at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port17-TCP:V=7.93%I=7%D=11/16%Time=6738D993%P=x86_64-pc-linux-gnu%r(NUL
SF:L,8F,"FLAG:\x20CSEC-3961-QOTD\r\nHint:\x20This\x20looks\x20like\x20a\x2
SF:0new,\x20fully\x20patched\x20system\.\x20\x20Maybe\x20there\x20is\x20a\
SF:x20vulnerable,\x203rd\x20party\x20service\x20installed\x20instead\.\r\n
SF:\r\0")%r(GetRequest,8F,"FLAG:\x20CSEC-3961-QOTD\r\nHint:\x20This\x20loo
SF:ks\x20like\x20a\x20new,\x20fully\x20patched\x20system\.\x20\x20Maybe\x2
SF:0there\x20is\x20a\x20vulnerable,\x203rd\x20party\x20service\x20installe
SF:d\x20instead\.\r\n\r\0");
MAC Address: 00:50:56:A1:95:57 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 268.99 seconds

┌──(root㉿kali)-[~]
└─# ifconfig && hostname && whoami && date
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.12.39.2  netmask 255.255.255.0  broadcast 10.12.39.255
        inet6 fe80::250:56ff:fea1:2186  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:a1:21:86  txqueuelen 1000  (Ethernet)
        RX packets 18120  bytes 26021078 (24.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7424  bytes 1048347 (1023.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.12.0.25  netmask 255.255.255.0  broadcast 10.12.0.255
        inet6 fe80::250:56ff:fea1:ead  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:a1:0e:ad  txqueuelen 1000  (Ethernet)
        RX packets 12824  bytes 2626965 (2.5 MiB)
        RX errors 0  dropped 38  overruns 0  frame 0
        TX packets 462310  bytes 26907613 (25.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 142  bytes 13704 (13.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 142  bytes 13704 (13.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

kali
root
Sat Nov 16 11:55:41 AM CST 2024

┌──(root㉿kali)-[~]
└─#
```

110723 - Target Credential Status by Authentication Protocol - No Credentials Provided

Flag 4-CSEC-3697-SHRE

System Vulnerable: 10.12.0.136

Steps taken:

1. Change password on Windows Student
2. Net user Annie CSEC388password
3. Right click logon switch user to Annie and enter in password
4. Browse through folders and see if there are any files and find in Network Share folder more devices.

Exploit Method Used: Privileged Access.

CVE Vulnerability Classification: There is no known CVE Vulnerability for this. There is also no known CVE directly assigned to the process calc.exe itself.

MITRE ATT&CK ID: This is the Privileged Escalation Tactic and the Exploitation Privilege Escalation Tactic T1068.

Risk Rating: Low- information disclosure has minor impact. See Table B.

Severity: Low. See Table A.

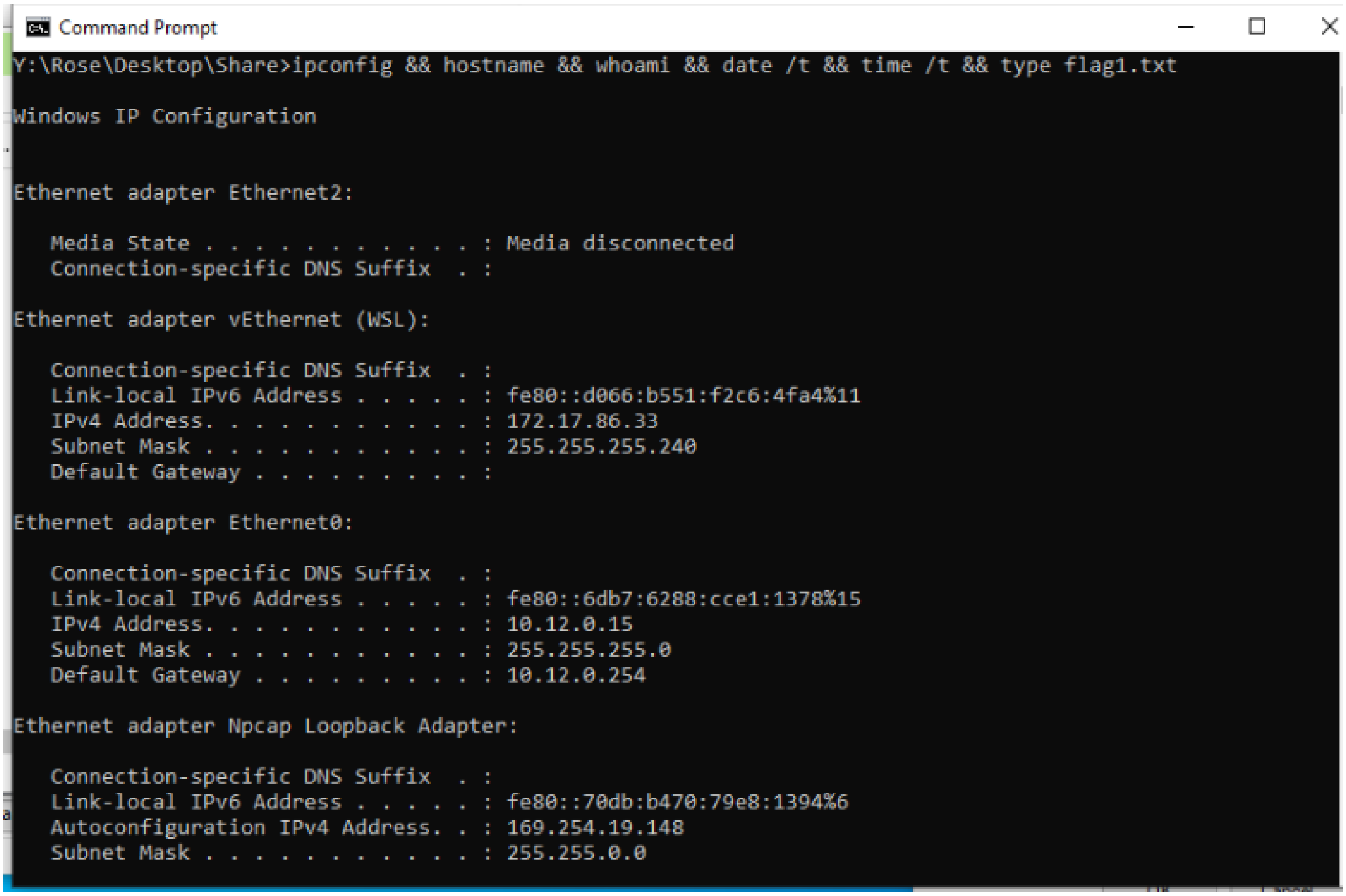
Tools used:

1. Command Prompt
2. Windows Explorer

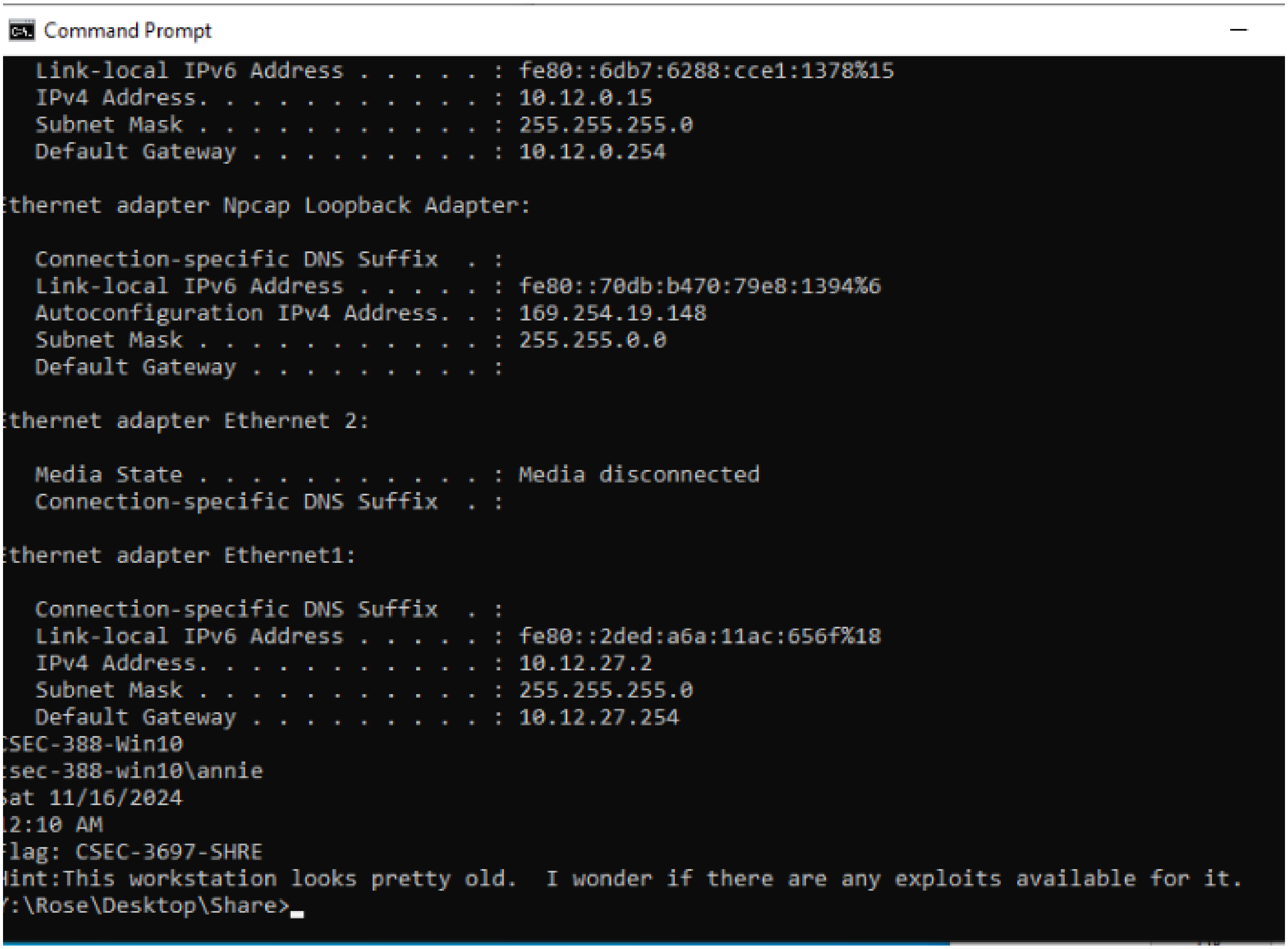
Remediation:

1. Remove access to Network shared Drives.

Proof of Vulnerability below:



```
Y:\Rose\Desktop\Share>ipconfig && hostname && whoami && date /t && time /t && type flag1.txt

Windows IP Configuration


Ethernet adapter Ethernet2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter vEthernet (WSL):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::d066:b551:f2c6:4fa4%11
   IPv4 Address. . . . . . . . . . . : 172.17.86.33
   Subnet Mask . . . . . . . . . . . : 255.255.255.240
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6db7:6288:cce1:1378%15
   IPv4 Address. . . . . . . . . . . : 10.12.0.15
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.12.0.254

Ethernet adapter Npcap Loopback Adapter:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::70db:b470:79e8:1394%6
   Autoconfiguration IPv4 Address. . : 169.254.19.148
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
```



```
   Link-local IPv6 Address . . . . . : fe80::6db7:6288:cce1:1378%15
   IPv4 Address. . . . . . . . . . . : 10.12.0.15
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.12.0.254

thernet adapter Npcap Loopback Adapter:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::70db:b470:79e8:1394%6
   Autoconfiguration IPv4 Address. . : 169.254.19.148
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

thernet adapter Ethernet 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

thernet adapter Ethernet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::2ded:a6a:11ac:656f%18
   IPv4 Address. . . . . . . . . . . : 10.12.27.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.12.27.254
SEC-388-Win10
sec-388-win10\annie
at 11/16/2024
2:10 AM
lag: CSEC-3697-SHRE
int:This workstation looks pretty old.  I wonder if there are any exploits available for it.
:\Rose\Desktop\Share>_
```

Flags 4-12

System Vulnerable: 10.12.0.203

Reasoning: Due to unforeseen circumstances, we were not able to complete the scan on target 10.12.0.203. This was difficult for us to achieve but we did attempt several hours attempting to exploit this. This is an Appache Web Server and it hosts a website at http://10.12.0.203.

Update on Other Systems Vulnerable: 10.12.0.89, 10.12.0.161, 10.12.0.89

Reasoning: We were not able to obtain the proper administrator login plus an addition of not running the proper command line Remote Code Execution to break in to retrieve the remaining flags at these addresses. Please contact us for further assistance due to the Time Constraint limitation on this Pen-test.

APPENDIX A:

SEVERITY RATING DETAILS

This entire section is exactly quoted from the first.org Common Vulnerability Scoring System v3.0: Specification Document. Use this appendix to understand the scoring system from the **Severity Section** in this report. The link to get to the document is here:

- https://www.first.org/cvss/v3.0/specification-document
  - The document direct PDF link is here: https://www.first.org/cvss/v3.0/cvss-v30-specification_v1.9.pdf

"The Common Vulnerability Scoring System (CVSS) is a free and open industry standard for assessing the severity of computer system security vulnerabilities. CVSS attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to the threat. Scores are calculated based on a formula that depends on several metrics that approximate ease of exploit and the impact of exploit. Scores range from 0 to 10, with 10 being the most severe."