Enumeration Cheat Sheet

by imousrf via cheatography.com/128342/cs/25087/

Nmap

Switch	Example	Description
	nmap 192.16-8.1.1	Scan a single IP
	nmap 192.16-8.1.1-254	Scan IP range
	nmap 192.16-8.1.0/24	Scan a network
-sV	nmap 192.16-8.1.1 -sV	Attempts to determine the version of the service running on port
-A	nmap 192.16-8.1.1 -A	Enables OS detection, version detection, script scanning, and traceroute
-sT	nmap 192.16-8.1.1 -sT	TCP connect port scan (Default without root privilege)
-sU	nmap 192.16-8.1.1 -sU	UDP port scan

Gobuster

Gobuster is a tool used to brute-force:

-URIs (directories and files) in web sites.

-DNS subdomains (with wildcard support).

-Virtual Host names on target web servers.

DIR mode

To find directories and files.

```
gobuster dir -u <ur l> -w <wo rdl ist.fi le.tx t> -x <fi le_ ext ens ion s>
```

vhost mode

Check if subdomain exists by visiting url and verifying the IP address.

```
gobuster vhost -v -w <wo rdl ist.tx t> -u <ur l> -o <ou tpu t_f il e.tx t>
```

DNS mode

To find subdomains in a specific domain.

```
gobuster dns -d <do mai n> -w <wo rdl ist.tx t> -o <ou tpu t_f il e.tx t>
```

-k to skip SSL verification

Linux

helpfull linux commands

connect to remote host

```
ssh userna me@ server
```
Ex. `ssh roo t@1 92.1 68.1.250`

search for files in a directory hierarchy

find file in the current directory

```
find . -name "test<fi le_ ext
```

find files with certain permission

```
find . -perm 664
```

search words in file

```
grep "<wo rd_t o_s ear ch> <fi le_ na me>"
```

pipe

you can redirect the output of a command to the input of an other command

```
cat file | wc -l
```
get number of lines in file

output redirection

you can redirect the output to file

```
echo 'hello there' > file
```

By **imousrf**
cheatography.com/imousrf/

Published 6th November, 2020.
Last updated 6th November, 2020.