

### 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 sV
-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 <url> -w <wordlist_file.txt> -x <file_extensions>
```

#### vhost mode

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

```
gobuster vhost -v -w <wordlist.txt> -u <url> -o <output_file.txt>
```

#### DNS mode

To find subdomains in a specific domain.

```
gobuster dns -d <domain> -w <wordlist.txt> -i
```

-k to skip SSL verification

### Linux

helpfull linux commands

#### connect to remote host

```
ssh username@server Ex. ssh root@192.168.1.250
```

#### search for files in a directory hierarchy

find file in the current directory

```
find . -name test
```

find files with certain permission

```
find . -perm 664
```

#### search words in file

```
grep "literal_string" filename
```

#### 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/](https://cheatography.com/imousrf/)

Published 6th November, 2020.  
 Last updated 6th November, 2020.  
 Page 1 of 1.

Sponsored by **Readable.com**  
 Measure your website readability!  
<https://readable.com>