Enumaration

* in this phase we just gathering information
* NMAP

one of the most used tool especially for the big features

nmap -sS -O 192.168.0.1 192.168.0.4

nmap -sP 192.168.0.0/24

nikto -host [http://192.168.0.10](http://192.168.0.10/)

nmap -sn 192.168.0.0/24

nmap --traceroute 192.168.0.0/24

nmap 192.168.0.1-4

nmap 192.168.0.\*

nmap -PR 192.168.0.0/24

nmap -p 80 192.168.0.0/24

nmap -sn -PS80 192.168.0.0/24

nmap 192.168.0.2

nmap -p 1-100 192.168.0.1

nmap -F 192.168.0.1

nmap -p- 192.168.0.1

nmap -sT 192.168.0.1

nmap -sU -p 53,80,3389 192.168.0.1

nmap -O --osscan-limit 192.168.0.0/24

nmap -O --osscan-guess 192.168.0.3

nmap -A 192.168.0.6

nmap -sV -O 192.168.0.1

-HPING3

hping3 192.168.0.1 --icmp

(lo sappiamo tutti cosa fa)

hping3 192.168.0.1 --icmp -c 5

(ne raccoglie 5 pacchetti icmp)

hping3 intranet --scan 80 -S

hping3 intranet --scan 22,80,443 -S

hping3 192.168.0.1 --scan 1-65535 -S

(-S sta per settare il SYN flag)

hping3 -8 0-100 -S 192.168.0.1

(-8 per attivare lo SCAN mode)

-NIKTO

nikto -host [http://192.168.0.10](http://192.168.0.10/)

-FROM WEBSITE

[https://hunter.io](https://hunter.io/)

(cerca informazioni attraverso email address)

[https://burrrd.com](https://burrrd.com/)

(estrae informazioni attraverso Twitter)

[http://www.anywho.com](http://www.anywho.com/)

(estrae informazioni)

-HARVESTER

theharvester -d practice-labs.com -l 500 -b google

theharvester -d theguardian.com -b pgp

-DMITRY

dmitry -p intranet

(porte disponibili per lo scan)

dmitry -p intranet -o plab

(sarebbe come fare un nmap &)

cat plab.txt

-FPING

fping 192.168.0.1

(controlla se l' ip è vivo or not)

fping -g 192.168.0.1 192.168.0.2

(-g sta per il gruppo)

fping -g 192.168.0.0/24

-NSLOOKUP

nslookup practicelabs.com

nslookup -type=A practicelabs.com

nslookup -type=soa practicelabs.com

nslookup -type=A -debug practicelabs.com

nslookup -query=MX practicelabs.com

nslookup -type=ns practicelabs.com

nslookup practicelabs.com 192.168.0.1

nslookup -query=any practicelabs.com

-SOFTWARE PER L’ ENUMERATION

idserve.exe

(fa query particolari)

csports.exe

(guess what he do)

Mylanviewer-setup.exe

(una specie di nmap ma grafico un pò alla zenmap )

-ENUMERATION NETCAT

nc -nvz 192.168.0.1 88

(-n per utilizzare quell' ip -z per effettuare lo scanning)

-NETDISCOVER

netdiscover -r 192.168.0.0/24

(tools utilizzare per lo scanning)

netdiscover -p

-SCANNING THROUGH MSFCONSOLE

>msfconsole

>use auxiliary/scanner/portscan/syn

>set RHOSTS 192.168.0.1

>set THREADS 25

>set PORTS 53

>run

-----> MSFCONSOLE (if you want to group some ip trough one command)

set PORTS 1-100

run

--

set RHOSTS 192.168.0.1-3

run

-ENUMERATION THROUGH WINDOWS

superscan4.1

(viene usato per l'enumerazione di Windows)

--->to deactive firewall policies   
(Poweshell Admin)

Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled False

(turn off the firewall policies)

-ENUMERATION DOMAINS

hyena.zip

(usato per aggiungere domini e l'enumerazione del dominio)

---LDAP Enumeration

ldapadmin-4.12

(aggiungere il dominio e inserire all'utente i privilegi)

-----SNMP Enumeration

Solarwinds DesktopToolSet

Windows adminitstrative tools--> Services --> SNMP

MIB Viewer --> compila i campi

host -t mx practicelabs.com

echo www > plab.txt

echo ftp >> plab.txt

echo mail >> plab.txt

echo proxy >> plab.txt

for ip in $(cat plab.txt); do host $ip.practicelabs.com;done

dnsenum practicelabs.com

(enum attraverso il dns)

nmap 192.168.0.10 --script smb-os-discovery.nse

(nmap script nse attraverso smb)

rpcclient 192.168.0.3 -U admin

(inseriamo la password che abbiamo rimpostato attraverso ldap enum)

>srvinfo

>enumprivs

>lsaenumsid

--enumeration preventing techinques

Kali:

wafw00f [http://intranet](http://intranet/)

waf

win 10:

group policy managemente --> domains --> edit --> computer configuration --> Policies --> Windows Settings --> Security Settings --> Account Lockout Policy --> modificare i valori

---DNS Enumaration

DNS --> proprieties --> security

Prevent Windows Enumeration:

services.msc --> cerca Print Spooler --> e metterlo a stop (status) e cambiare lo startup type in disabled

---->Enumeration su Windows

C:\Users\alex>systeminfo

C:\Users\alex>netstat -ano

C:\Users\alex>net user /domain alex

check token + info personali

meterpreter > use incognito

meterpreter > list\_tokens -u

i mean..