https://docs.google.com/document/d/18GpPSyaLBLvPevMIHt_K7iAiFdV9unpokQ4ubS-xqqA/edit?usp=sharing

lern 2 hack

claudia richoux

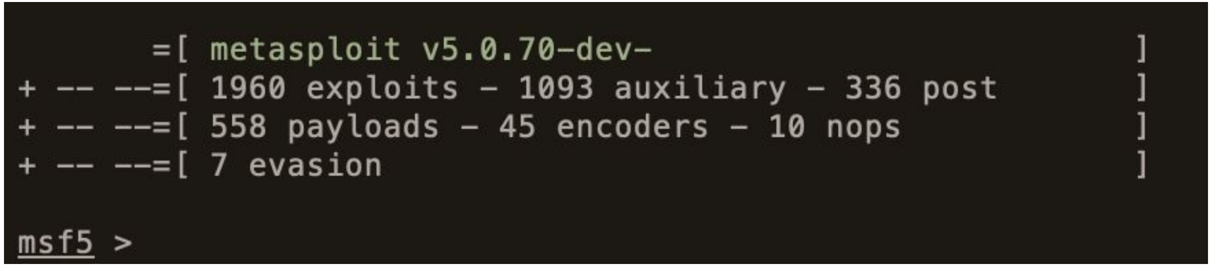
slides are at http://bit.ly/claudia-hack-talk-slides, please open them on your laptop and follow along for useful resources
Macos follow this:
http://www.arbaouimehdi.com/how-to-setup-metasploitable-3-on-mac-mojave/
windows/linux get VMware player and then download this
https://sourceforge.net/projects/metasploitable/

disclaimers and warnintgs

- please only scan/exploit things that you have clear permission to (today and always)
  - i am not responsible for you getting in trouble if you dont listen to this
  - CFAA prosecution is brutal; uchicago is not understanding about 1337 h4xx0r1ng
  - no really, not kidding, if you do something silly and get caught, that is a *you* problem :)
- please be considerate of others, i didn’t lock down the lab boxes very well
  - you will be able to attack others’ laptops and attack boxes, and you will have sudo/root on attack/target boxes respectively
  - don’t break the attack boxes, don’t change things on the target boxes, we’re all adults here!
  - if you aren’t sure if you should be running a command, please ask me first!
  - this is for everyone to learn, not for you to show off… no king-on-the-hill on target boxes!

first, get connected and set up

- everyone has a little paper with a hostname/username/password?
- SSH in (you CAN sudo but please [!!!] DO NOT) (`ssh username@hostname` then enter password at prompt)
- run `nmap` to make sure it's installed okay
- run `msfconsole`, hit "`n`" when prompted about the database, you may get some errors but that is ok, these are for setting up features we aren't using. make sure it looks like this when you're done then hit ctrl-D to exit back to a terminal.



```
       =[ metasploit v5.0.70-dev-                         ]
+ -- --=[ 1960 exploits - 1093 auxiliary - 336 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 >
```

nmap

- nmap == “network map”
    - first released in the legendary phrack magazine as a c file >22 years ago
- finds computers/their open ports/services they are running
- can be extended with scripts to tell you about vulns on services
    - (also try --script vuln)
- how does it work?
    - Ping, SYN, ACK scanning
    - OS/service fingerprinting
- important things to know: (more in this cheat sheet)
    - basic scan: `nmap 10.0.7.0/24`
    - check what hosts exist super quickly: `nmap -sn IP_RANGE`
    - scan specific ports with -p option, skip reverse DNS resolution with -n
    - -sV to get specific service information
    - -A -T4 to get reasonably fast & detailed OS/service info

let’s try nmapping

- hack-talk-box-1: 10.0.7.0/24 hack-talk-box-2: 10.0.63.0/24
- find the box: start with `nmap -sn IP_RANGE`, get `IP_ADDR`
- find services on it: `nmap -sV IP_ADDR`, get `PORT_LIST`
  - Ports should be formatted like 80,443,60-63
  - This would be ports 80, 443, 60, 61, 62, 63
- do more intensive service identification on the ports you found:
  - `nmap -sV --version-all -T4 -p PORT_LIST IP_ADDR`
- do OS recognition on the box: `nmap -O IP_ADDR`
- Check the cheat sheet for more info, let me know if you have questions
- Take notes of the services, what ports, what IP.

metasploit

- ok so u found services on the box
- time to metasploit them
- https://sourceforge.net/projects/metasploitable/
-