

Cyber@UC; Meeting 28

Cyber Kill Chain

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

- **Babyhack Saturday Oct 7.**
 - CTF360.com scenarios
 - NSA Codebreaker challenge
 - Starts at 10:00 AM to 10:00 AM Sunday
 - Food provided throughout
 - [Sign-up Roster](#)
- **Cyber Range**
 - Delayed Date TBD
- **October 27/28th ACM** programming challenge
- **P&G cybersecurity center** tour is still in the planning phase
- **National Collegiate Cyber Defense Competition** prepping will begin soon

COINs and LOGO



Ida Pro


Questions?




The background is a solid pink color. In the top right corner, there are several overlapping geometric shapes: a dark pink square, a medium pink square, and a light pink square, all partially cut off by the edge of the image.

Weekly Info Session

Yahoo Data Breach

- The largest hack of user data till date.
 - 3 billion accounts compromised in the August 2013 data breach.
 - The hack exposed user information including names,email addresses,telephone numbers,date of births,hashed passwords and in some cases security questions.
 - Yahoo immediately notified the affected users about the stolen data.
 - Change passwords , security questions and enabling 2FA.
 - Deleting the account might not help as Yahoo takes 30 days to recycle the deleted accounts.
- 

Vehicle Tracking Device breach

- Login credentials of more than half a million records belonging to SVR Tracking have leaked online.
 - The company used a misconfigured Amazon Web Server S3 cloud storage to store the data.
 - The cloud storage bucket had a cache which was accessible to everyone for an unknown period.
 - The leaked cache contained 540,000 SVR accounts including email addresses ,passwords and vehicle data like VIN, IMEI number of GPS devices.
 - The database also contained information about the location of the tracking unit.
- 

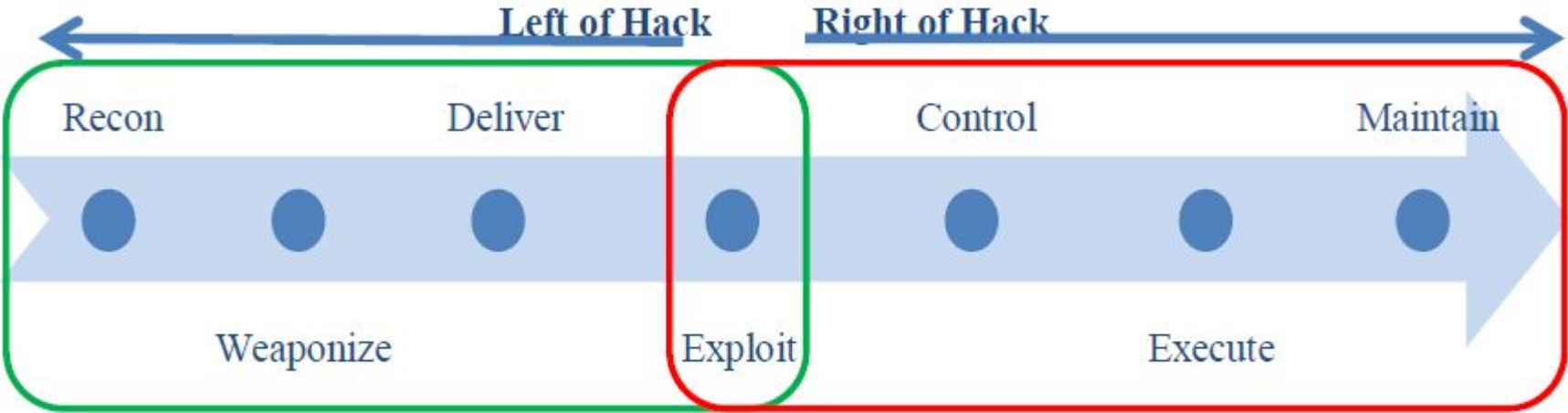
Changing trends in ransomware

- The primary ransomware defense is backups backups backups
- A rising trend in the latest ransomware malwares is the targeting of backups
- Newer versions of Cryptolocker and wannaCry have been doing this
- This has been happening to mac since the first mac ransomware in 2015
- Now ransoms are target windows shadow files
- <https://www.darkreading.com/endpoint/ransomware-will-target-backups-4-ways-to-protect-your-data/a/d-id/1330029?>
- https://en.wikipedia.org/wiki/Shadow_Copy



Cyber Kill Chain

Cyber Kill Chain



Example Cyber Kill Chain

Reconnaissance

- Methods determined by situation and/or target.
- Primary goal is to obtain sufficient information to enable exploitation.
 - Operating system
 - System services
 - Communication protocols
- Secondary goal may be to evade detection.
 - IP address spoofing
 - Escalation of scanning methods
 - Pivoting



Weaponization

- Once target operating system, services, or protocols are known:
 - Determine a suitable payload
 - Payload configuration
- A typical configuration may include:
 - Payload encoding
 - Programming language changes
 - No Op sledding



Delivery and Exploit

- Delivery:
 - Determine the delivery method and time
 - Decide on passive and active delivery
 - Passive may include listeners that perform packet injection
 - Active means you “run” the exploit
- Exploitation generally occurs on the target system:
 - May activate Anti-Virus
 - Have varying degrees of reliability
 - Generally allow you to execute some code.
 - May be configured to occur slowly over time.



Control and Execute

- This is where the real damage happens.
- This is when you have control of the system you have attacked.
 - Control you install or modify programs in on the victim
 - Execute performs commands on victim
- Targeted data is extracted or programs are inserted.
 - Keylogger can be inserted
 - etc/shadow file removed
 - Sensitive documents taken



Maintain

- Battle Damage Assessment (BDA) for DDOS
 - Similar to Recon phase
- Update code (It is still software)
 - More difficult attack style
 - Maintain codebase
 - Perform data dumps periodically for collection platforms



Background – Policy

Successful intrusion detection depends on policy and management as much as technology

Security Policy (defining what is acceptable and what is being defended) is the first step

Notification

Who, how fast?

Response Coordination



Intro to Snort

Snort is a multi-mode packet analysis tool

Sniffer

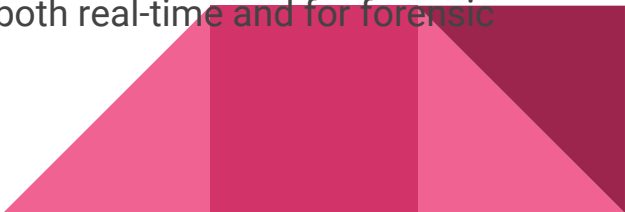
Packet Logger

Forensic Data Analysis tool

Network Intrusion Detection System

Where did it come from?

Developed out of my evolving need to perform network traffic analysis in both real-time and for forensic post processing



Snort Design

Packet sniffing “lightweight” network intrusion detection system

Libpcap-based sniffing interface

Rules-based detection engine

Plug-in system allows endless flexibility



Uses for Snort

Standard packet sniffing NIDS

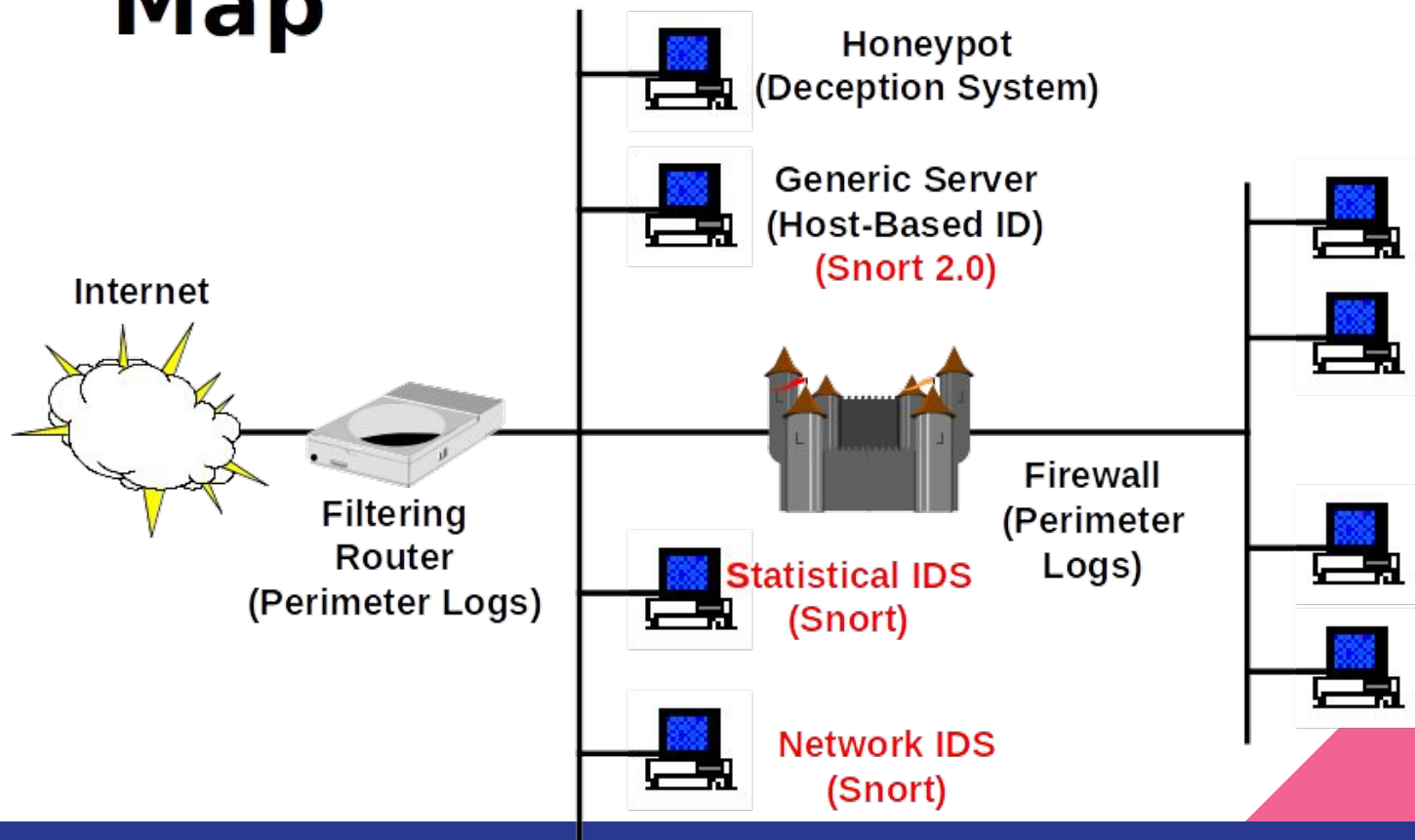
Policy Enforcement

Honeypot monitor

Scan detection/traps



IDS Implementation Map



Packet Logger Mode

Gee, it sure would be nice if I could save those packets to disk...

Multi-mode packet logging options available

Flat ASCII, tcpdump, XML, database, etc available

Log all data and post-process to look for anomalous activity



NIDS Mode

Uses all phases of Snort + plug-ins to analyze traffic for both misuse detection and anomalous activity

Can perform portscan detection, IP defragmentation, TCP stream reassembly, application layer analysis and normalization, etc

