Computer Network Security

COMP 178 | Spring 2022 | University of the Pacific | Jeff Shafer

Penetration Testing: Reconnaissance

Stages of "Cyber Kill Chain"

Abnormal DNS reverse lookup requests

Brute Force Attack

Unusual amount of data uploaded to external websites

Activity from blacklisted geolocationn

Unusual number of GDPR files deleted

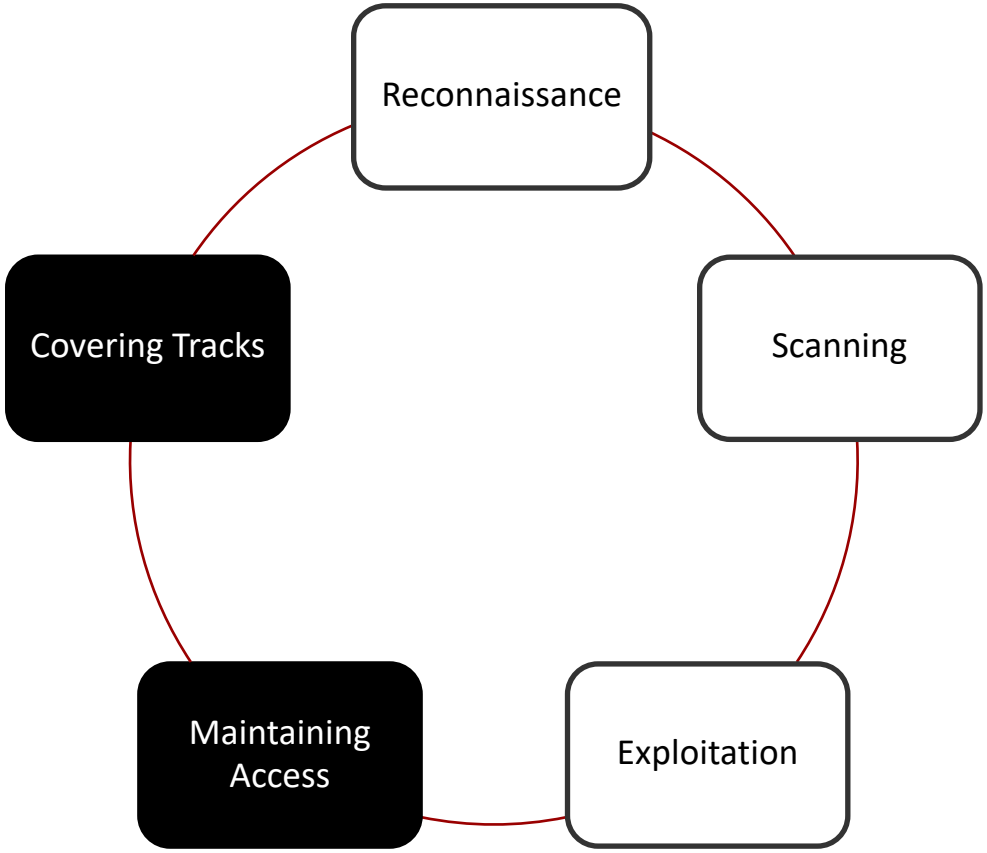
Failed privilege escalation detected

Unusual number of messages marked as unread

A dormant service account was reactivated

https://www.varonis.com/blog/cyber-kill-chain/

Stages of an Attack



Stages of an ~~Attack~~ Pen Test

Pen Testing

- Reconnaissance – Investigate the target
  - Public sources
- Scanning
  - Searching for systems and vulnerabilities to target
- Exploitation

Real Attackers

- *Maintaining Access*
- *Covering Tracks*

Reconnaissance Stage

- Spend a day gathering information about the target from **public sources**
  - Not *necessarily* technical! (tech-lite?)
  - Not doing scans of their network (that comes next)
  - Google, LinkedIn, myriad public databases
- Put yourself in the shoes of the target and better understand them
  - What business are they in?
  - Where are their facilities located?
  - Who works there? (names, titles, emails, …)
    - Bonus points if you can find names & emails of executives and IT administrators – Would be *very* helpful to get their logins later!
  - What kind of technology do they claim to use?

Reconnaissance Stage

- Benefits
  - Improves your chances of success during the rest of the pen test
  - Reporting documents (of threats, risks, …) can be tailored to the customer instead of being generic

Resources

- **Penetration Testing Framework**
- Detailed checklist of common pen-test areas of interest
  - Reconnaissance
  - Discovery & Probing (Scanning)
  - Password Cracking
  - Network Testing
  - Penetration
  - Physical Security

http://vulnerabilityassessment.co.uk/Penetration%20Test.html

Resources

- **Open-Source Intelligence** (OSINT)
  - Gather information from free databases and resources
  - ***Deeper than just "Google it!"***
- Applied during pentest reconnaissance stage
  - Take a small piece of information and leverage it to learn more
  - Example: Given a domain name, what can I learn?
    - Whois records to check ownership
    - Enumerate (guess/lookup) subdomains
    - Check for SSL certificates
    - …

Resources

- OSINT Framework - https://osintframework.com/
- Skip Tracing Framework - https://makensi.es/stf/
  - *Last updated in 2012, so some of the tools are broken, but the ideas are still useful*

System Inventory

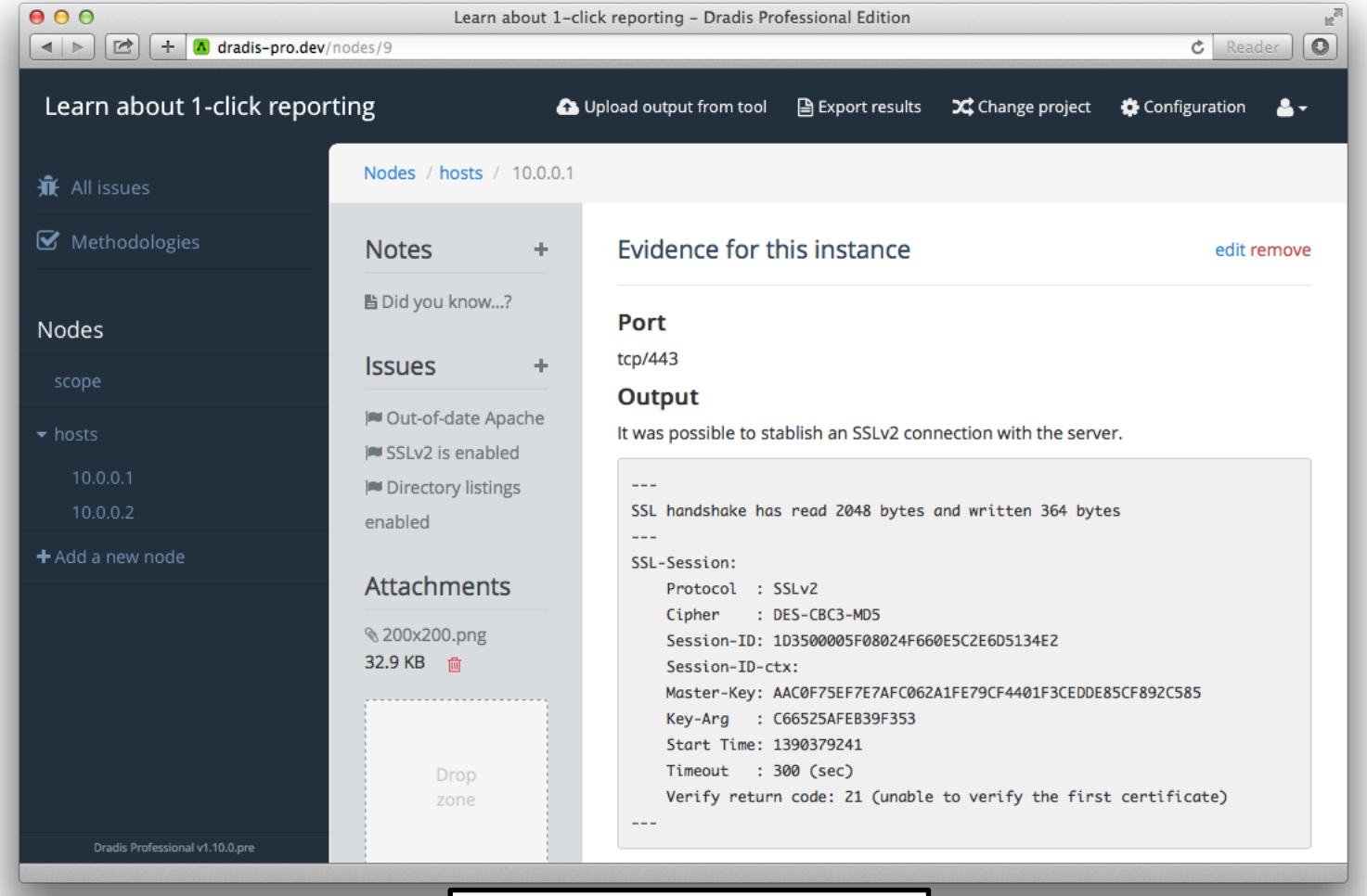
- You won't remember everything you discover during reconnaissance and scanning! Need an organized method to document your discoveries
- One suggestion: **System Inventory**

IP Addr	Hostname	OS	Discovery Method	Open Ports	Vulns?	Accounts & Passwords	Notes

Discovery Method

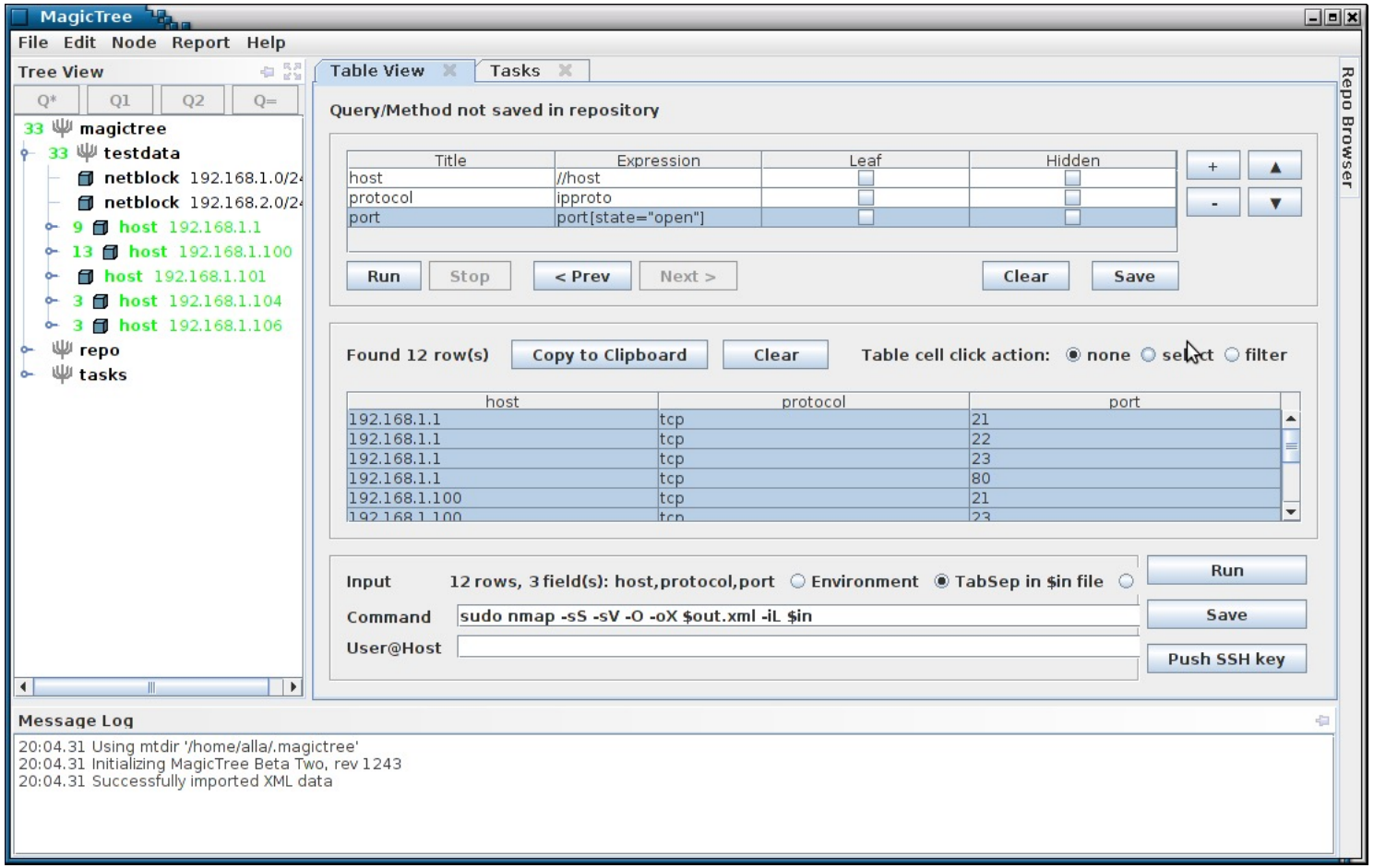
- **Discovery Method** is particularly important to document thoroughly – it makes your results *reproducible*
  - Provided by customer? (during scoping discussions)
  - Google search?
  - DNS? (zone transfers, reverse lookups, etc…)
  - Network scans? (ICMP, TCP, UDP, …)
  - Physical access?
  - Pivoting through another host? (which host?)

Automated Documentation - Dradis



https://dradisframework.com/

Automated Documentation - MagicTree



https://www.gremwell.com/what_is_magictree

Google

- Google is your friend!
  - All kinds of data is intentionally (or unintentionally) placed online
  - Search for interesting files?
    - `site:example.com filetype:.pdf`
  - Search for Unix passwd file?
    - `site:example.com intitle:index.of passwd`
    - (Password is hashed but usernames are present)

Google Dorks

- Google Hacking Database, aka “Google Dorks”
  - Simple Google queries to pull up potentially vulnerable systems or interesting information
- Categories
  - Files Containing Juicy Info
  - Sensitive Directories
  - Vulnerable Servers
  - Network or Vulnerability Data
  - ….

https://www.exploit-db.com/google-hacking-database

Google Dorks

- Example – Pfsense login pages
  - Pfsense is a firewall – do you have an exploit handy and are looking for targets?
  - `intitle:"Pfsense - Login"`
  - https://www.exploit-db.com/ghdb/5671
- Example – Cacti Monitoring
  - Cacti is a network monitor, and might show servers that the enterprise thinks are important enough to monitor
  - `intitle:"Cacti" AND inurl:"/monitor/monitor.php"`
  - https://www.exploit-db.com/ghdb/5600

https://www.exploit-db.com/google-hacking-database

Class Presentations

Class Presentations

- **Topic**: Anything related to computer security, network security, etc…
- **Scope**: **15 minutes of technical content w/slides**
- **Timeline**
  - **Proposal due – Tue Feb 8th**
  - Video & slides due – Tue Mar 1st
  - Peer Reviews due (3) – March 11th

Class Presentation

- Ideas for inspiration?

https://cyberlab.pacific.edu/resources/security-and-privacy-news