Week 06
Pentesting I:
Intro to Pentesting

Thomas and Minh

Announcements

- TracerFIRE is this weekend!

- Spray paint social in April

sigpwny{but_i_use_pencils??}

What is pentesting?

- Short for "penetration testing"
- Simulated attack by a company or person to test the strength of a computer system.
- Companies will hire security firms to do pentesting
- Also referred to as "ethical hacking" or "white-hat hacking"

The Pentesting Process

Before the Pentest

- Meeting with the firm
- Scoping and scope documents
- Legal agreements
- Initial security audit from client

During the Pentest

- Technical
  - Reconnaissance
  - Enumeration
  - Exploitation
  - Post-Exploitation
- Non-Technical
  - Meetings with clients
  - Continuous documentation
  - Human testing

After the Pentest

- Report writing
- Debrief meetings
- Client will implement patches

Before the Pentest

This is here so you know what to do... don't get sued... and don't get arrested

Initial Meetings

Discuss Executive Goals

- Services Offered / Services Desired
- Will help determine scope roughly

Budgeting

- Pentesting is expensive
- Figure out budget → services offered

Expectations

- Given the budget, what do you want out of this engagement?

Scope

The exact list of things that you **can** and **cannot** do stuff on.

THIS IS REALLY IMPORTANT

THIS IS REALLY IMPORTANT DO NOT BREAK THE SCOPE!!!

Scope Documents

Typically a list of devices / IPs / Subnets for what you can / cannot do.

Devices
- Printers, Servers, Computers

IPs
- Most often internal, sometimes there are external IPs

Subnets
- Groups of IPs split by an ip and a / (192.168.1.0/24 == .1.0 - .1.255)

Why shouldn’t you violate scope?

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STO

CASE DISMISSED —

Exonerated: Charges dropped against pentesters paid to break into Iowa courthouse

Dismissal is a victory for the security industry and the customers who rely on it.

DAN GOODIN - 1/30/2020, 4:57 PM

Legal

Sign all the stuff and have all the stuff sent over to avoid legal troubles

Examples Of Stuff

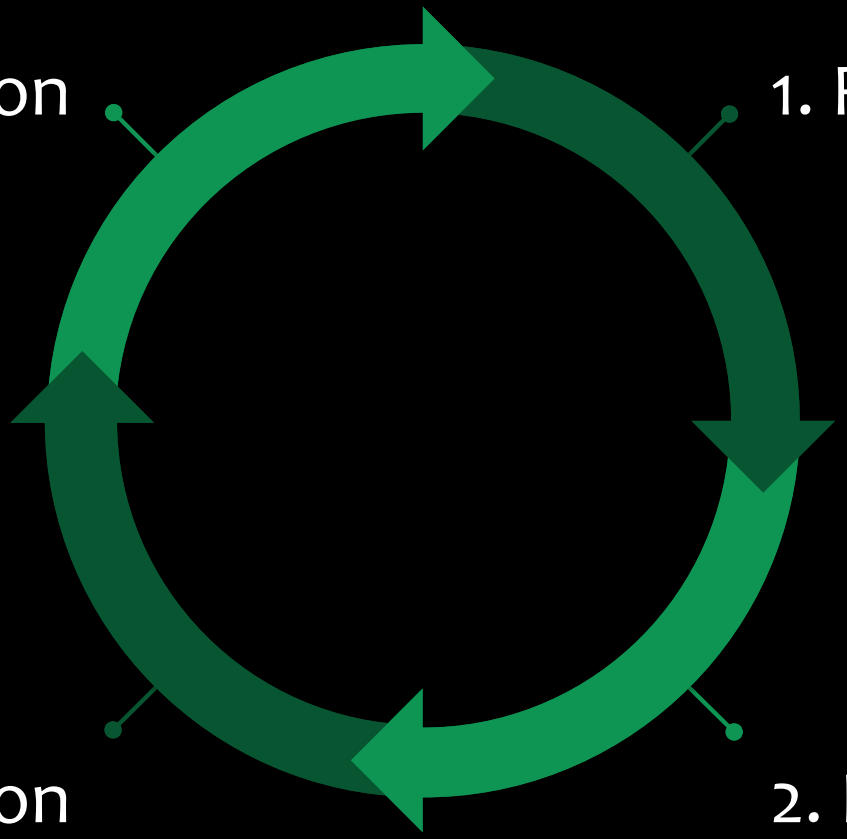
- NDA
- Standard Contract to avoid suit
- Written Permission etc

During the Pentest

Introducing the 4-step kill chain methodology!

4. Post-Exploitation

1. Reconnaissance



3. Exploitation

2. Enumeration

1. Reconnaissance

Reconnaissance ≈ OSINT

- Google + using relevant tools

Finding the target

nslookup dnsrecon

- WHOIS domain lookup

Looking for subdomains

crt.sh sublist3r

- What stuff is related to this domain?

Identifying website technologies

builtwith.com wappalyzer whatweb

- What technologies do they use? Are they outdated?

Finding previous attacks

hunter.io shodan HaveIBeenPwned

- Can we find leaked sensitive information online?

Recon is PASSIVE information gathering!

You are using publicly available information about the target.

You are NOT performing scans or probing the target directly.

2. Enumeration

- This is where you actively scan the network for entry points: Ports -> Services -> Vulnerabilities
- **Port Scanning**
  - What ports are open? What services are running on these ports? nmap
- **Service Scanning**
  - Each type of service is enumerated with different tools
  - Example: HTTP
    - What subdomains / URLs are visitable? dirb gobuster nikto
  - Example: FTP
    - Is anonymous login allowed?
    - Can I edit files, or is it read-only?
  - Example: SMB

Enumeration is ACTIVE information gathering!

You are scanning the targets for open ports and services.

This CAN get you in trouble!

Port Scanning

Running a full nmap TCP port scan:

```
sudo nmap -Pn -sC -sV -sS -p- $IP
```

Service Scanning

Running a HTTP directory brute force scan with gobuster:

```
gobuster dir -u http://example.com/ -w /usr/wordlists/dirb/common.txt
```

Wordlist:
https://github.com/danielmiessler/SecLists/blob/master/Discovery/Web-Content/common.txt

3. Exploitation

- The goal is to get remote code execution (RCE)
- If you know information about a certain service, you can lookup information to see if there is an exploit available
  - Example: After enumerating a web service, you figure out it is running Apache Struts version 2.5.16 from the nmap scan results.
  - A quick Google search will show that it has a critical vulnerability that allows RCE (CVE-2018-11776)
  - Find a public exploit for the CVE! https://www.exploit-db.com/exploits/45260
- Once you have RCE, you can get a shell!

searchsploit

github.com

4. Post-Exploitation

LinPEAS

WinPEAS

GTFObins

LOLBAS

- You're in, but you're not done yet
- Privilege escalation
  - Usually, we start as a low-privilege service account, such as `www-data`, or a low-privilege employee account
  - The goal is to get `root` or `Administrator`
- Maintaining access
  - Sometimes, exploits are one-shot and won't be exploitable afterwards OR the exploit is patched by a system administrator
  - Use scheduled tasks/cron jobs which run at time intervals to re-establish access (e.g. connect to the attacker server every 1 hour)

Useful Resources

https://book.hacktricks.xyz/ - quite possibly the most comprehensive guide on all stages of pentesting

https://github.com/swisskyrepo/PayloadsAllTheThings - contains common payloads you can use against targets

Nontechnical Stuff During the Pentest

Meetings…

Findings vs Notes, reporting, documentation

Human Testing

After the Pentest

Reporting!

Writing a report with all your findings

Very important

Pentest Reporting

Table of Contents

1. Executive Summary
2. Summary of suggestions
3. Overview of each service offered
4. Summary of each finding
5. Detailed analysis of each finding (including mitigations)
6. Appendices.

List of every finding should be kept somewhere like a spreadsheet or google doc.

Next Meetings

Sunday Seminar: **UIUCTF Planning (Unless someone has a mtg!)**

-

Next Thursday: **2022-03-10**

- TBD