SP2023 Week 04 • 2023-02-16

Pentesting I

Minh and Emma

Announcements

- WiCyS Palentines Day Social (2023-02-20)
  - Make crafts, eat snacks, meet friends!

- Cyber Tractor Challenge (application due 2023-03-13)
  - Travel to Des Moine to learn how to secure John Deere equipment

- ICSSP Informational Meeting (2023-03-02)
  - Scholarship and government internship opportunity

ctf.sigpwny.com

sigpwny{this_is_a_quality_pen}

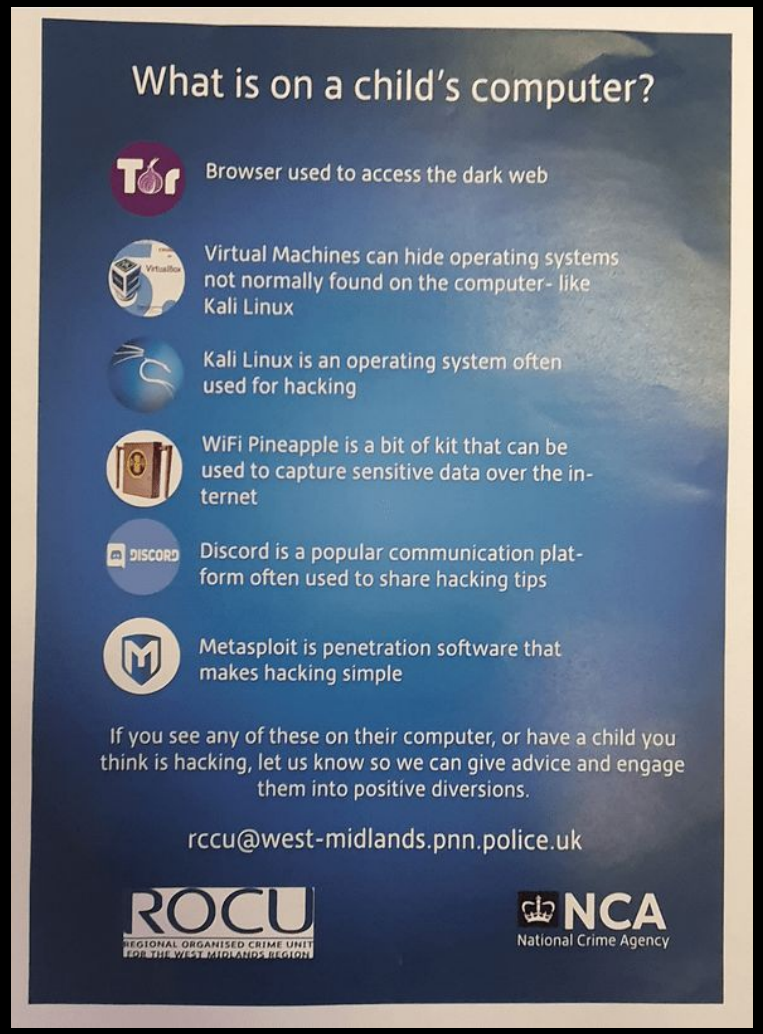


Table of Contents

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"
- Can be employee-based (traditional) or contractor-based (modern)

The Process

<u>Before the Pentest</u>
- Meeting with the firm
- Scoping and scope documents
- Legal agreements
- Initial security audit from client

<u>During the Pentest</u>
- Technical
  - Reconnaissance
  - Enumeration
  - Exploitation
  - Post-Exploitation
- Non-Technical
  - Meetings with clients
  - Continuous documentation
  - Human testing

<u>After the Pentest</u>
- Report writing
- Debrief meetings
- Client will implement patches

Before the Pentest

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, and actions that list what you can and cannot do.

Devices

- Printers, servers, computers

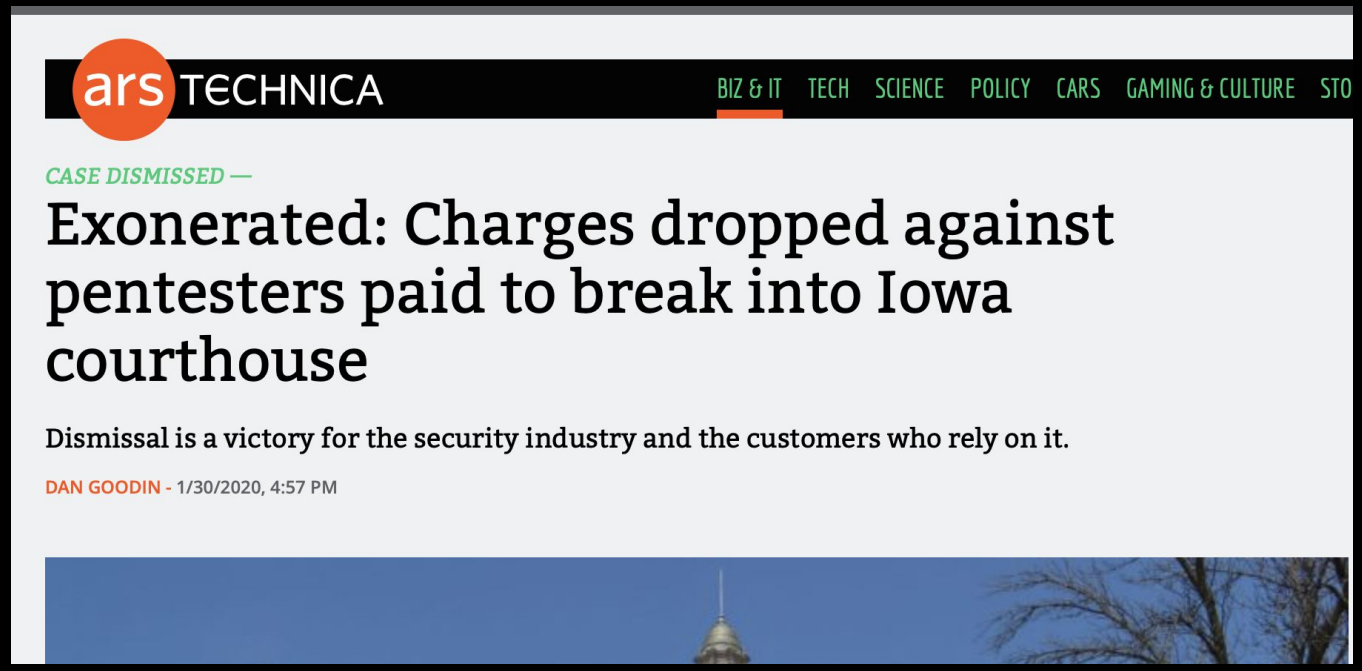
IPs and Subnets

- IP address can be either internal or external
- Groups of IPs are represented with CIDR notation (192.168.1.0/24 == 192.168.1.0 - 192.168.1.255)

Actions

- "You are only allowed to connect to port __ on __ server"

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

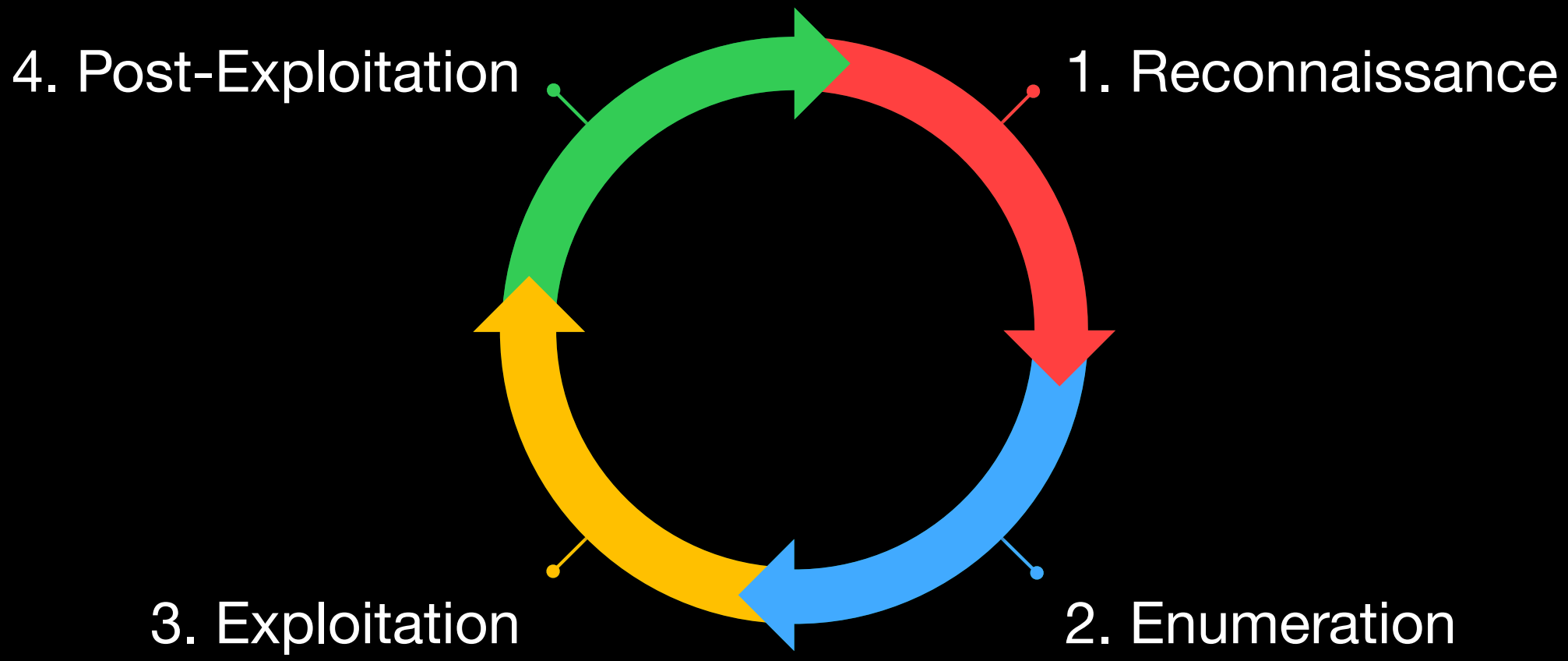
Dismissal is a victory for the security industry and the customers who rely on it.

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

Legal

- NDA
- Standard contract to avoid suit
- Written permission
- It is a bit tedious/boring, but it is the only defense you have in the case of legal action taken against you

During the Pentest


4. Post-Exploitation
1. Reconnaissance
3. Exploitation
2. Enumeration

1. Reconnaissance

- Reconnaissance ≈ OSINT `Google Dorks`
  - Google + using relevant tools
- Finding the target `nslookup` `dnsrecon`
  - WHOIS domain lookup
- Looking for subdomains `crt.sh` `sublist3r`
  - What services are related to the domain?
- Identifying website technologies `builtwith.com` `wappalyzer` `whatweb`
  - What technologies do they use? Are they outdated?
- Finding previous attacks `hunter.io` `shodan.io` `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

- Ports → Services → Vulnerabilities
- Port Scanning
  - What ports are open? What services are running? `nmap`
- Service Scanning
  - Example: HTTP
    - What paths are available? Login pages? `dirb` `gobuster` `nikto`
  - Example: FTP
    - Is anonymous login allowed?
    - If the filesystem read-only or writable?
  - Example: SMB
    - Useful for host information (OS version, usernames)
    - Has a notorious history of vulnerabilities

Enumeration is *active* information gathering!

You are scanning the targets for open ports and services.

This could get you in trouble!

Port Scanning

Running a full nmap TCP port scan:

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

`-Pn` specifies the scan will skip a ping check

`-sC` means that nmap will run some default script scans to enumerate more information from a port

`-sV` will have the scan perform version checking

`-sS` will perform a SYN stealth scan

`-p $PORT` will scan specified ports (omitting will scan top 1000 ports)

`-p-` will scan every single port from 1-65535

`-v` will enable verbose output

Service Scanning

Running HTTP directory brute force scan with gobuster:

```
gobuster dir -u http://target.site/ -w /usr/wordlists/dirb/common.txt
```

Handy directory wordlists:
https://github.com/danielmiessler/SecLists/tree/master/Discovery/Web-Content

3. Exploitation

- The goal is to get remote code execution (RCE)
- You can use version information look up possible exploits
  - 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 which 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`

Exploitation is Just CTF

- Web, PWN, reverse engineering - you have already been doing exploitation!
- Instead of trying to find a flag, you are trying to gain more access or a larger foothold into a system
- Some services run custom application code and require more thought to exploit them (as opposed to just trying to find CVEs or public exploits)

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 (persistence)
  - Sometimes, exploits can only be used once or the exploit is patched while you are trying to attack a system
  - Use scheduled tasks or cron jobs which run at time intervals to re-establish access

Useful Resources

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

https://github.com/swisskyrepo/PayloadsAllTheThings - contains many different attacks on various services and payloads to use against targets

Non-technical Stuff

- Meetings with the client to update on current progress
- Taking notes, documenting findings, reporting vulnerabilities
  - Some clients or bug bounty firms enforce a "stop-and-report" policy, meaning the moment you find a vulnerability, you must cease enumeration/exploitation and report it

After the Pentest

Reporting Your Findings

- Without a report, what's the point?
- Report format
  - Executive Summary
  - Summary of suggestions
  - Overview of each service offered
  - Summary of each finding
  - Detailed analysis of each finding (including mitigations)
  - Appendices
- List of every finding should be kept somewhere you can go back to

Next Meetings

2023-02-19 - This Sunday

- PWN IV: Heap with Kevin
- Learn about heap PWN

2023-02-20 - This Monday

- WiCyS Palentines Day Social
- Make crafts and eat snacks with Women in Cybersecurity

2023-02-23 - Next Thursday

- REV III with Richard
- Learn about VM obfuscation and side channels

HackTheBox

How HackTheBox Works

- HackTheBox provides a virtual network to practice pentesting
- Machines are systems that you can exploit
  - `user.txt` - contains the flag for gaining user-level access
  - `root.txt` - contains the flag for gaining system-level access
  - Flag files are usually stored in home directories (Linux) or desktop folders (Windows)
- To connect to machines, you first need to connect to HTB's VPN (only a small subnet of IPs are routed through it)
  - Only connect through your warstation virtual machine
  - Alternatively, you can use HTB's virtual desktop service
- They also have Challenges, which is just traditional CTF

Setup Steps

- Set up HackTheBox
  - Create an account and join the university team (https://app.hackthebox.com/universities/overview/785)
- Set up Kali Linux virtual machine
  - Install VMware (or VirtualBox or QEMU)
    - M1 users should install UTM
  - Download the prebuilt Kali Linux VM from kali.org
    - https://www.kali.org/get-kali/#kali-virtual-machines
    - You may need to install 7-Zip to extract the virtual machine files
    - M1 users will need to follow these instructions: https://docs.getutm.app/guides/kali/
- Set up HTB VPN in Kali
  - Log in to HTB on Kali, click Labs, Starting Point
  - Download OpenVPN profile, `sudo openvpn ~/Downloads/starting_point_USERNAME.ovpn`

Important Tips

- **DO NOT CONNECT TO THE VPN DIRECTLY FROM YOUR PERSONAL MACHINE**
- Only connect through your Kali virtual machine, otherwise you risk attacks against your personal device

Home
My Profile
My Team
Labs
Rankings
Battlegrounds
Academy
Job Board
Universities
Social

OVERVIEW
ACTIVITY
MEMBERS

University of Illinois Urbana-Champaign

REQUEST TO JOIN
RESPECT

University of Illinois Urbana-Champaign - Rankings Growth
1 MONTH

—
Points Gained (1 month)

0% growth
In contrast with last month.

+1 ranks earned
In contrast with last month.

Rank Progress

—
Points needed for next rank bracket

— RANK BRACKET
— RANK BRACKET

University Best Ranking
1 YEAR

#
University Best Rank
Achieved on

23	23	3	0
USER OWNS	ROOT OWNS	RESPECTS	FIRST BLOODS

University Machine Statistics

Average stats of all university members

University Challenge Statistics

Average stats of all university members

Prebuilt Virtual Machines

Kali Linux VMware & VirtualBox images are available for users who prefer, or whose specific needs require a virtual machine installation.

These images have the default credentials **"kali/kali"**.

Virtual Machines Documentation ›

64-bit 32-bit

VMware

2.6G torrent docs sum

Recommended

VirtualBox

2.6G torrent docs sum

Recommended

QEMU

2.6G torrent docs sum

Recommended

HTB University

- The more machines we solve, the higher our university ranking
- We'd like to start competing against other universities and gaining experience so we can participate in more penetration-testing based competitions
- We will give LOTS of Pwny CTF points for people to continue playing HackTheBox

Starting Point Track

HackTheBox → Labs → Starting Point
sudo nmap -Pn -sC -sV -sS -p- -v $IP

Meow

telnet $IP $PORT

Fawn

ftp $IP

Dancing

smbclient -L $IP

smbclient \\\\$IP\\ShareName --no-pass

redis-cli

sigpwny{this_is_a_quality_pen}

SIGPwny