



SP2024 Week 02 • 2024-02-01

Intro to Pentesting

Ronan Boyarski

Announcements





- DiceCTF is tomorrow!
 - Come for free pizza and play great CTF challenges!



ctf.sigpwny.com


sigpwny{this_is_a_quality_pen}


What is on a child's computer?

-  Browser used to access the dark web
-  Virtual Machines can hide operating systems not normally found on the computer- like Kali Linux
-  Kali Linux is an operating system often used for hacking
-  WiFi Pineapple is a bit of kit that can be used to capture sensitive data over the internet
-  Discord is a popular communication platform often used to share hacking tips
-  Metasploit is penetration software that makes hacking simple

If you see any of these on their computer, or have a child you think is hacking, let us know so we can give advice and engage them into positive diversions.

rccu@west-midlands.pnn.police.uk

 **ROCU**
REGIONAL ORGANISED CRIME UNIT
FOR THE WEST MIDLANDS REGION

 **NCA**
National Crime Agency



What is Pentesting?

- Short for "penetration testing"
- Simulated attack by a company or person to test the strength of a computer system.
- Focus on finding and exploiting vulnerabilities rather than testing the effectiveness of a security response
- 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)



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"



Reporting

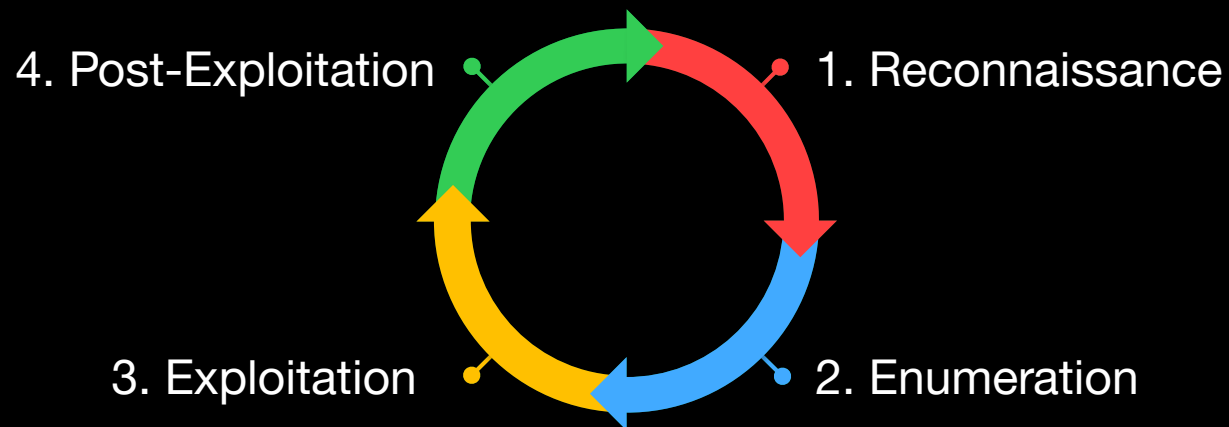
Typically, findings are documented in the form of a report

- 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
- Write it during the pentest, **not after**



Pentesting Process

- Focus on cyclical compromise rather than a one-off exploit
- Process is going to be dependent on the level of sophistication demanded by the target's security posture
- Since this is an introduction, the cycle can be simplified to:



Reconnaissance

- Similar to OSINT
- Focus on gathering exploitation-relevant information, such as:
 - Operating Systems/Tech Stack
 - Employees by position
 - Target mailing scheme
 - Hostnames by IP Address (Reverse DNS lookup)
 - Subdomain/VHOST "brute force" search
 - Past data breaches
 - Obviously outdated software
 - Target Active Directory Domains
- Nothing at this stage is illegal (but it is looking for trouble)

whatweb

wappalyzer

linkedin

nslookup

dig

dnsrecon

sublist3r

gobuster vhost

shodan.io

HaveIBeenPwned



Enumeration

- Active Information Gathering (interactive)
- Goal is to piece together a highly accurate model of the target computer(s)
- Scan ports -> Identify services -> Find Vulnerabilities
- Services are exposed software running on the target
- Typically start with **nmap** and use subsequent tools (this can be automated)
 - e.g. nmap -> feroxbuster & whatweb (port 80), enum4linux (port 445)
- Struggling with exploitation is **almost always** an enumeration issue



Port Scanning

- Port range: 0-65535, TCP & UDP
- `sudo nmap -Pn -F -sV -vv $IP -oN fast.txt`
- `sudo nmap -Pn -A -sV -p- -vv $IP -oN full.txt`
- `-A` means that nmap will run scripts and OS fingerprinting
- `-sV` will have the scan perform version checking
- `-p-` will scan every single port from 1-65535
- `-vv` will enable very verbose output
- `-oN` saves the result to a text file so you don't re-scan



Port Scanning

- Don't forget UDP services like SNMP!
- `sudo nmap -Pn -F -sU -vv $IP -oN udp.txt`
- `-sU` will have the scan check UDP ports
- `-F` will scan top 1000 ports (UDP scanning is **SLOW**)
- General workflow tip: make a directory for each target



Service Scanning: Web

- Now that you know what services are running, the goal is to extract as much information as theoretically possible from it
- Web
 - feroxbuster/gobuster: forcefully checks if directories exist
 - Can also be used to identify subdomains/vhosts
 - Great for finding admin panels, robots.txt, and git repos
 - nikto: scans for web vulnerabilities
 - Burp Suite: tools for manually finding web vulnerabilities
 - Can spider pages
 - sqlmap: automatically exploits SQL injection
 - Can be used to automatically get a shell when attacking MSSQL
 - Also can be used with a request file from Burp Suite



Service Scanning: SMB

- Server Message Block runs by default on all Windows computers
- If you know the password, you can view remote file shares `smbclient`
- If the target is running Windows Server or is AD joined, and you have Administrator credentials, **remote code execution is a feature**
`exploit/windows/smb/psexec` `psexec` `impacket-psexec`
- Windows computers prior to Windows 7 SP 6.1 are vulnerable to MS17-010 (SYSTEM RCE) `exploit/windows/smb/ms17_010_eternalblue`
- If SMB is not password protected, you can potentially read/write files



Service Scanning: Other services

- FTP: can be used to upload files or download sensitive files if left unsecured `ftpclient`
- SSH: if you have a password or id_rsa, get a shell as a feature
- SNMP: Simple Network Management Protocol, sometimes runs on Windows machines, allows viewing all of the running processes, usernames, and software versions, including command-line arguments `onesixtyone`
- SMTP: Simple Mail Transfer Protocol, you can send phishing emails from the command line `sendemail`
- Redis: Database, can **gain RCE as a feature**



Gaining Access: Exploitation

- Sometimes, when attacking vulnerable software, it's as easy as running **searchsploit** or the relevant metasploit module
- Other times, custom exploit development is necessary (think CTF web challenge)
- Example workflow:
 - nmap -> port 80 is open -> feroxbuster -> find gitlab instance
 - searchsploit gitlab
 - run exploit, hopefully get shell
- **ALWAYS** read exploit code before running it!



Gaining Access: Password Attack

- Lots of common software, like WordPress, doesn't rate-limit authentication, so you can go through an obscene amount of login attempts
- WordPress also allows username enumeration
- **Hydra** is a fantastic general-purpose password attack tool
- Example workflow:
 - `nmap -> port 443 -> feroxbuster -> /wp-admin`
 - `hydra -l Admin -P /usr/share/wordlists/rockyou.txt 10.10.230.209 http-post-form "/wp-login.php:log=^USER^&pwd=^PWD^:The password you entered for the username" -t 30`
- Use admin login to upload PHP reverse shell (feature)



Post-Exploitation

LinPEAS

WinPEAS

GTFobins

LOLBAS

- Arguably the most important part of the entire cycle (although enumeration is close)
 - This is primarily due to trust relationships in large networks, not so relevant for an introduction
- Usually need a way of escalating privileges, either vulnerability or misconfiguration
- Goal is to get root on Linux, or SYSTEM on Windows
- Use a C2 Framework for stealth & persistence



Linux Privesc Checklist

- Do manual and automated checks (not stealthy)
- LinPEAS: Linux Privilege Escalation Awesome Script
- My manual command checklist:

LinPEAS

GTFObins

- hostname
- id
- cat /etc/passwd
- uname -a
- ps aux
- ip a
- route
- ss -anp
- cat /etc/iptables/rules.v4
- ls -lah /etc/cron
- crontab -l
- grep "CRON" /var/log/syslog
- dpkg -l
- find / -writable -type d
2>/dev/null
- mount
- cat /etc/fstab
- lsblk
- find / -perm -u=s -type f
2>/dev/null



Windows Privesc Checklist

- Can Use PowerUp.ps1, or SharpUp, similar to LinPEAS

PowerUp.ps1

- My manual command checklist:

PowerView.ps1

- whoami
- whoami /groups
- Get-LocalUser
- Get-LocalGroup
- Get-LocalGroupMember <Target Group>
- systeminfo
- ipconfig /all
- Get-ItemProperty "HKLM:\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall*" | select displayname
- route print
- netstat -ano
- dir Downloads
- dir C:\Program Files
- Get-Process
- Get-ChildItem -Path C:\ -Include *.kdbx -File -Recurse -ErrorAction SilentlyContinue
- Get-ChildItem -Path C:\Users\ -Include .txt,*.*ini -File -Recurse -ErrorAction SilentlyContinue

ADPEAS.ps1



Post-Exploitation: Credentials

- Once you get root on one machine, your goal is to find any information on the machine that can be used to gain code execution on other machines
- Active Directory is out of scope for this meeting, but credential reuse is still a big deal even without AD
 - Linux
 - `cat /etc/shadow`
 - crack with hashcat
 - Look for RSA keys
 - Check `/var/www/html` config files
 - Pillage all of the user directories
 - Windows
 - Dump LSASS with Mimikatz
 - Look up the docs, use it to grab logonpasswords, wdigest, ntds.dit, anything that you can
 - Use PowerView's `Find-LocalAdminAccess`

mimikatz

PowerView.ps1



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



Setup

- Make a TryHackMe account
- Download a Kali VM ISO from OffSec
 - Use VMWare
 - Make sure to validate using sha256sum, since malicious Kali images are a "known issue"
- Download the TryHackMe VPN and run it from the Kali VM
 - Not advisable to run it from your host machine, it's insecure and also makes reverse shells fail
- You may need to set your network adapter to "bridged" if you want to catch shells for real / not through a VPN



TryHackMe

This is what I used to start learning pentesting. TryHackMe combines hands-on teaching with hands-off boot-to-root machines. All machines listed below are from the free tier.

Easy: Basic Pentesting, RootMe, Mr. Robot CTF, tomghost

- Learning Path: Junior Pentester, Web Fundamentals

Medium: Relevant, 0day, Road, Blog

- Learning Path: Offensive Pentesting

Hard: Ra, Internal, Daily Bugle,

- Learning Path: Red Teaming



Next Meetings

2024-02-01 • Tomorrow

- DiceCTF 2024 Quals
- Come join us for challenges and free pizza!
- No meeting this Sunday

2024-02-08 • Next Thursday

- Arm assembly



ctf.sigpwny.com

`sigpwny{this_is_a_quality_pen}`

Meeting content can be found at
sigpwny.com/meetings.

