

Introduction to Pentesting

Make sure you have Kali ready :)

DISCLAIMER

All content covered is purely for educational/informative purposes!
Please don't utilize anything learned here to do anything stupid.

AND ILLEGAL.



What is Pentesting?

Ethical Hacking: A company hires you to simulate being an attacker, in order to find, exploit, and report vulnerabilities.

- “Pretending to be evil”.



Network



Web



Mobile

\$Career\$

- Consulting
- Red Teaming
- Security Engineer
- Security Researcher
- Bug Bounty



Stages of Pentesting

Open Source Intelligence (OSINT)

- Gather publicly available information on target before the pentest

Enumeration

- Run scanning tools, and gather information company machines

Exploitation

- Use the previously gathered information to exploit a vulnerability you found to gain control over the system

Post Exploitation

- Escalate privileges and pivot to other machines in the network to gain more control over the entire network

Report Writing

Some Essential Networking Knowledge: IP

- **IP Address:** identifies device on network or the internet so data can be routed to correct destination.
 - **IPv4:** 4 numbers (each between 0 to 255) separated by dots.
 - **localhost:** 127.0.0.1
 - ***ifconfig*:** Linux command to get IP address

123.89.46.72

IPv4 IP Address example

Some Essential Networking Knowledge: Ports

Port: Each IP address has 65535 ports that help with sorting network traffic.

- Different network protocols happen different at port numbers (0-1023 are well defined)

Network Protocol	Port Number(s)
SSH	22
HTTP/HTTPS	80/443
SMB	139/445

Netcat

A powerful networking tool to send and receive information over different protocols.

- Main tool used to catch reverse shells

> Demo Time!

Netcat Demo

Try it yourself! See if you can connect to yourself as localhost and then connect to our device on:

IP - 34.136.6.142

Port - 12345

Listener - **nc -lvp <PORT #>**

Client - **nc <IP Address> <PORT #>**

Some More Essential Knowledge: Server

A specialized device or software that provides functionality for other devices.

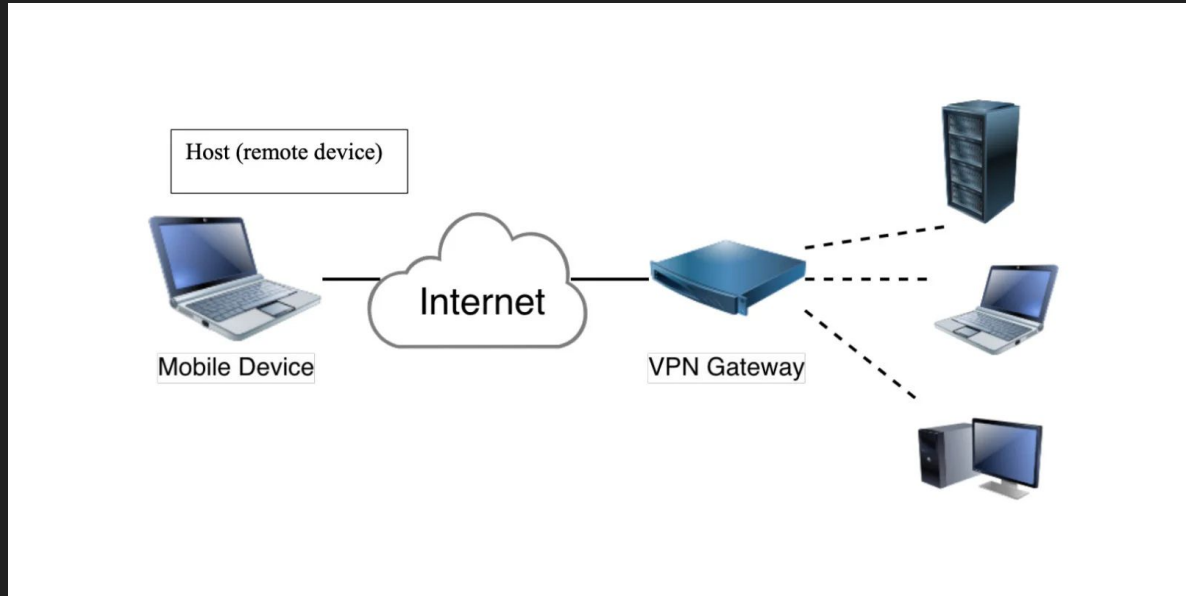
Example: web servers, email servers, Minecraft servers, etc.

Client - requests services/information from server



Virtual Private Network - VPN

Creates a tunnel between us and another network.



Nmap

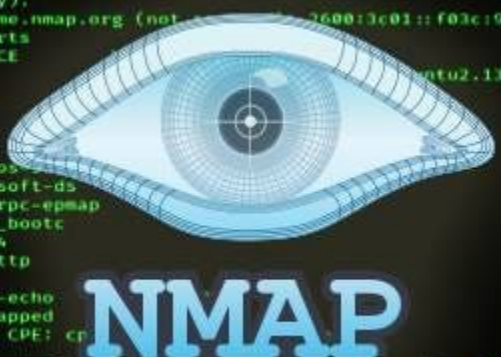
Mostly wide used port scanner used to get information about targets

Provide an IP address and will identify ports and their service version

Includes a scripting engine for finding specific exploits

```
root@kali:/home/spect# nmap -sV scanme.nmap.org -oX /home/spect/scanResults.xml
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-18 23:25 +01
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.21s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 987 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    filtered smtp
80/tcp    open  http
135/tcp    filtered msrpc
139/tcp    filtered netbios-ssn
445/tcp    filtered microsoft-ds
593/tcp    filtered http-rpc-epmap
1068/tcp   filtered instl_bootc
4444/tcp   filtered krb524
5800/tcp   filtered vnc-http
5900/tcp   filtered vnc
9929/tcp   open  nping-echo
31337/tcp  open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:Ubuntu:Ubuntu2.13 (Ubuntu Linux; protocol 2.0)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 39.35 seconds
```



Nmap Flags

- -sC: Scan with default NSE scripts
- -sV: Attempts to determine the version of the service running on port
- -p-: All ports
- -O: OS detection
- -sU: UDP port scan
- -sn: Host discovery (Useful for network sweep)
- -Pn: Disables ping and only scans for open ports
- DO NOT RUN -A: Aggressive detection mode
- <https://www.stationx.net/nmap-cheat-sheet/>

Nmap Practice

Try doing a nmap scan on **34.136.6.142** and discuss the following with the people around you:

- **Number of services open**
- **Port numbers**

Then try doing it with the `-sV` for service enumeration and discuss what happens.

Finding Exploitable Services

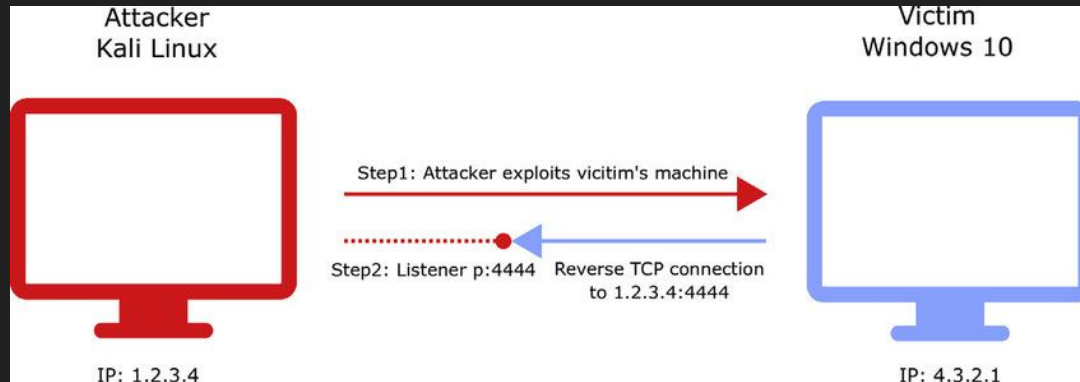
- Use Google to search for versions of service and look for vulnerabilities
 - **Example:** Apache 2.2.11 exploit
- Large public database - exploit-db.com
- **Searchsploit** - search for exploits using enumerated info
 - [manual](#)
- Online cheat sheets - Google: *hacktricks* <service name>

Shell and Reverse Shell

Shell: program that can execute commands that interact with your computer's operating system

Reverse Shell: a shell connection that allows you to make commands to a remote machine (revshells.com - DEMO on netcat)

- essentially the same as ssh-ing into the victim, but stealthier



Metasploit!

Multifunctional Pentesting tool used to automate process of running and finding exploits

> **DEMO TIME!!!** EternalBlue

Open by typing in Kali terminal: **msfconsole**

[Cheatsheet](#)

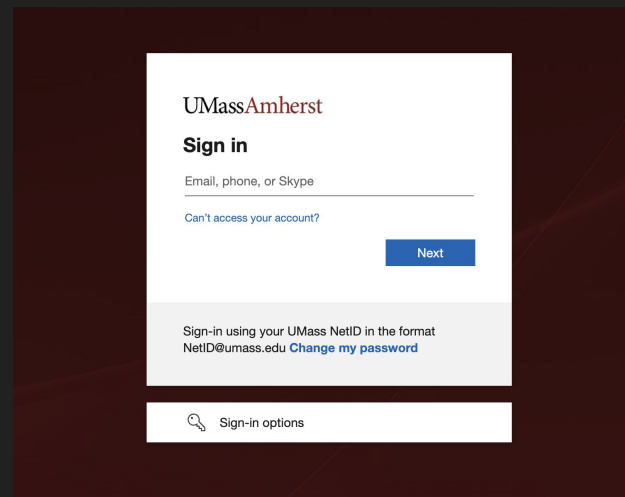
Active Directory

What is Active Directory?

- Keeps track of many resources on a corporate network as objects
- Ex: schools, companies
- Examples of Active Directory objects:
 - User Accounts
 - Computers
 - Groups
 - Services (DNS, Database access, etc)

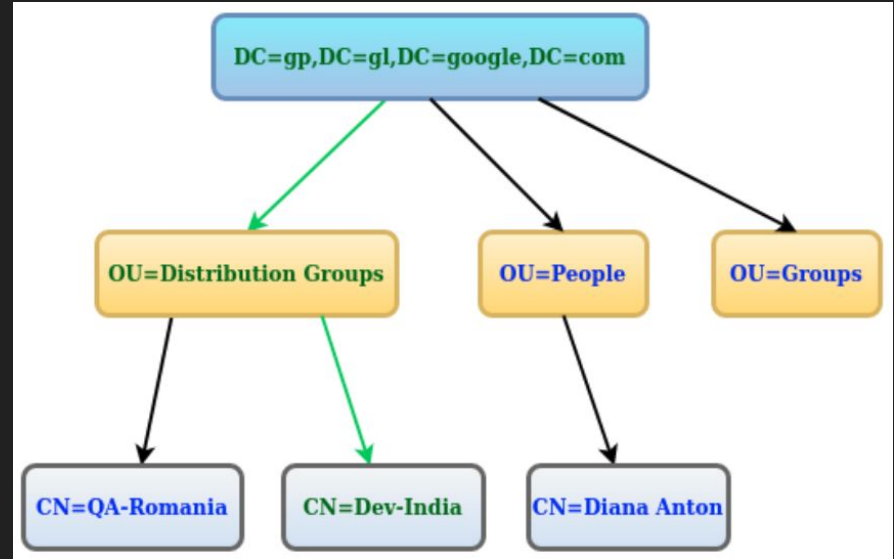


Microsoft
Active Directory

A screenshot of the UMassAmherst sign-in page. The page has a white background with a dark red border. At the top, it says "UMassAmherst" in red and black. Below that is "Sign in" in bold. There is a text input field for "Email, phone, or Skype". Below the field is a link "Can't access your account?". A blue "Next" button is to the right. Below the input field, it says "Sign-in using your UMass NetID in the format NetID@umass.edu" followed by a link "Change my password". At the bottom, there is a magnifying glass icon and the text "Sign-in options".

LDAP - Lightweight Directory Access Protocol

- Protocol for authenticating and accessing directory services
- Effectively how you find things in AD
- You query by where things are. For example, to query the Diana Anton user:



"CN=Diana Anton,OU=People,DC=gp,DC=gl,DC=google,DC=com"

SMB - Server Message Block

- a network protocol used to share files, printers, and other resources between devices on a network
- also allows computers to communicate and access shared data
- provides remote access to resource management
- goldmine for enumeration

BloodHound

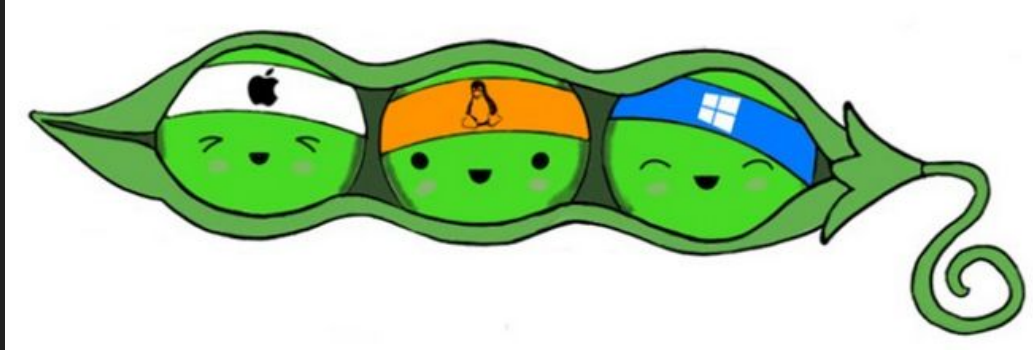
- A tool to find hidden/often unintended relationships, security misconfigurations within Active Directory
- Uses queries to find privilege escalation and lateral movement paths
- One of the most used AD pentest tools



> Demo Time!

winPEAS

- Privilege Escalation tool to find paths and security misconfigurations in Windows machines



AD Mindset

- Enumeration
 - nmap, smb, ldap, http
- Initial Access
 - Exploits
- Privilege Escalation
 - BloodHound, winPEAS
- Lateral Movement/Persistence
 - BloodHound, backdoor, metasploit

A brief overview of

Web/Linux

Brief background on web

Client - Server model:

- everything is a computer
- client will ask server for resources, server will respond

HTTP

- the “language” web clients (your browser) and servers ([google.com](https://www.google.com)'s computer)
- contains method, endpoint, headers, and body

Demo of client server model

I can run my own server on my own computer and make requests to it!

```
python3 -m http.server
```

Feel free to follow along!

Burp Suite and HTTP Proxies

- Burp Suite is a pentesting tool to find, enumerate, and exploit vulnerable web applications
- Burp Suite is a proxy that receives all HTTP/s traffic on local port 8080 and forwards or intercepts based on settings
- **In simple words - we can intercept and modify our requests**



Burp Suite demo

Now let me modify my requests and see what happens.

```
python3 -m http.server
```

CTF Web vs Pentesting Web

More differences than you'd expect:

- no source code
- no flag/no simple goal
- larger scope
- less complex vulnerabilities

Pentesting is more “real world”: what issues/vulnerabilities you'd see in companies

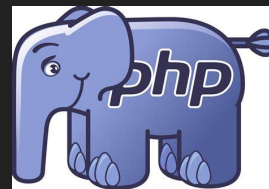
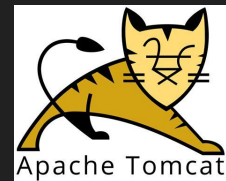
However, many concepts from CTF Web are transferable to pentesting

Linux

Similar to AD - **mainly enumeration of services and utilization of known exploits**

However, linux services aren't all "centralized" - there are way more different/unrelated linux services than windows

- Thus **there is no tool like bloodhound** that can tie many vulnerabilities together
- **You'll need to search** for service specific exploits on exploit-db, google, hacktricks, etc



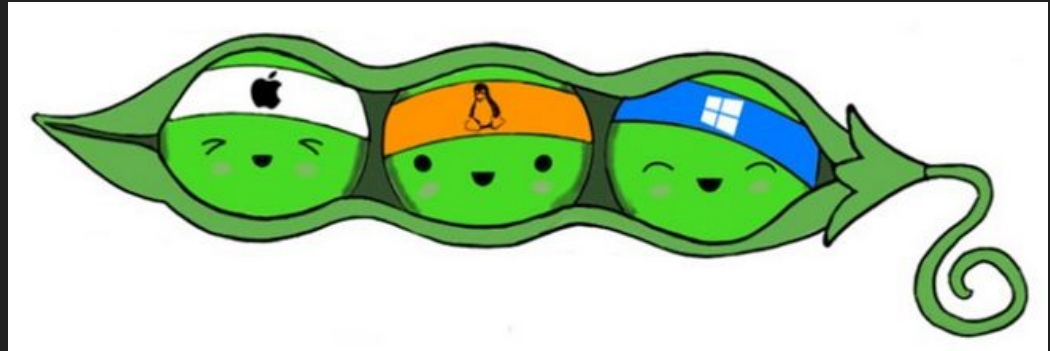
Linpeas

Privilege escalation tool:

- *Requires you to already have remote shell on the victim machine*
- Helps with becoming administrator/root on machine from a non-privileged user
 - Identifies any misconfigurations in the system (relaxed permissions, exposed passwords, etc)

Why do we want root?

- **access other user data**
- **pivot to other machines**
- control over the system
(dos, botnet, crypto miner)



Overall web/linux flow

- **Emumeration:** nmap, Burp Suite
- **Initial access/exploitation:** exploit-db, web RCEs
- **Privilege escalation:** LinPEAS, GTFObins
- **Lateral movement/persistence:** Rootkits, Command+control

Sometimes you can stop at initial access/exploitation!

- eg SQL injection allows you to change the money in your bank account

Upcoming web talks to look out for

Intro to web security - 9/30

- More in depth intro to using burp suite
- Foundations of the web (what is the web, protocols, http details, etc)

Advanced web security - 9/30

- (almost) every way to get RCE from web exploitation

Collegiate Pentesting Competition (CPTC)

- Given fictional company infrastructure to hack and team that finds the most vulnerabilities
- Defending New England Champion



Cyber Defense Competition (CCDC)



How to Learn More?

- **Vulnerable machines to hack:** hackthebox.com
 - Write-ups for retired boxes can be found here: [lppSec](https://lppsec.com)
- **TryHackMe:** tryhackme.com
- **Red Team/Blue Team Simulations**
- **COMPSCI 561:** System Defense and Test
- **COMPSCI 564:** Cyber Effects

CTF Challenge Walkthrough

HTB FUN!