Cybersecurity Engineering

Samuel

+1 (281) 965 1140

info@delojik.com

www.delojik.com

DELOJIK CONSULTING

Contents

Chapter One

INTRODUCTION TO CYBERSECURITY

Chapter 1: Introduction

General Introduction

Virtualization

Installation of Tools/Software

Q & A Session

1a. General Introduction

1. *General Introduction*
2. *Class Schedule / Class Structure*
3. *What is Cybersecurity and why it is needed?*
4. *Certifications*

General Introduction

What is your Name?

Where are you currently located?

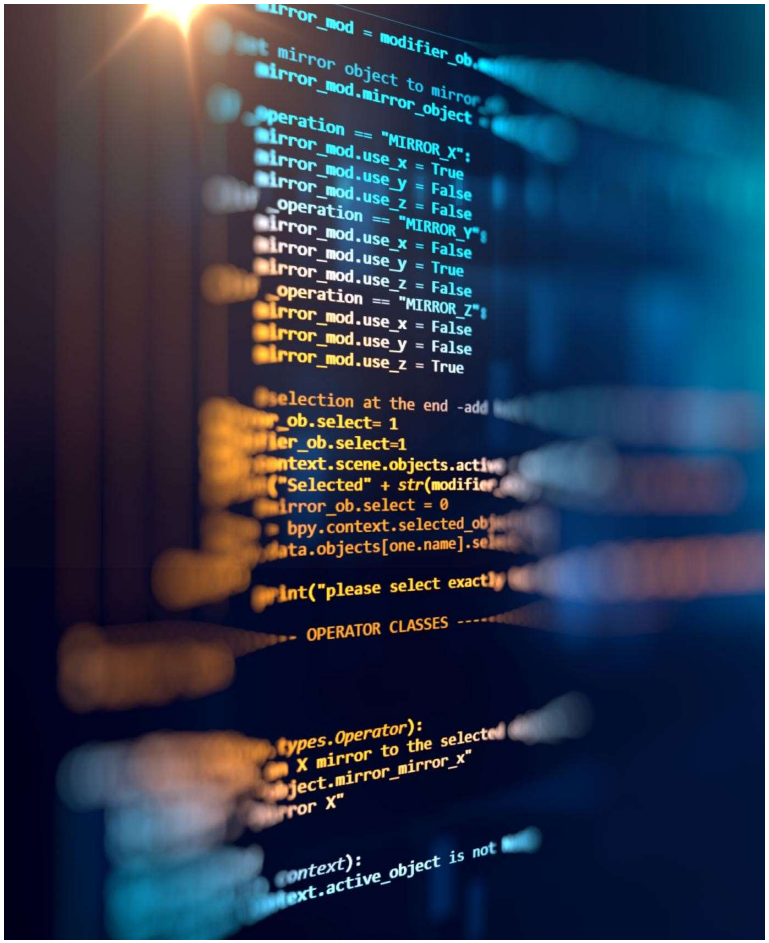
Your Current Job?

What do you know about Cybersecurity?

Where do you see yourself in the next 5 years?

Class Schedule

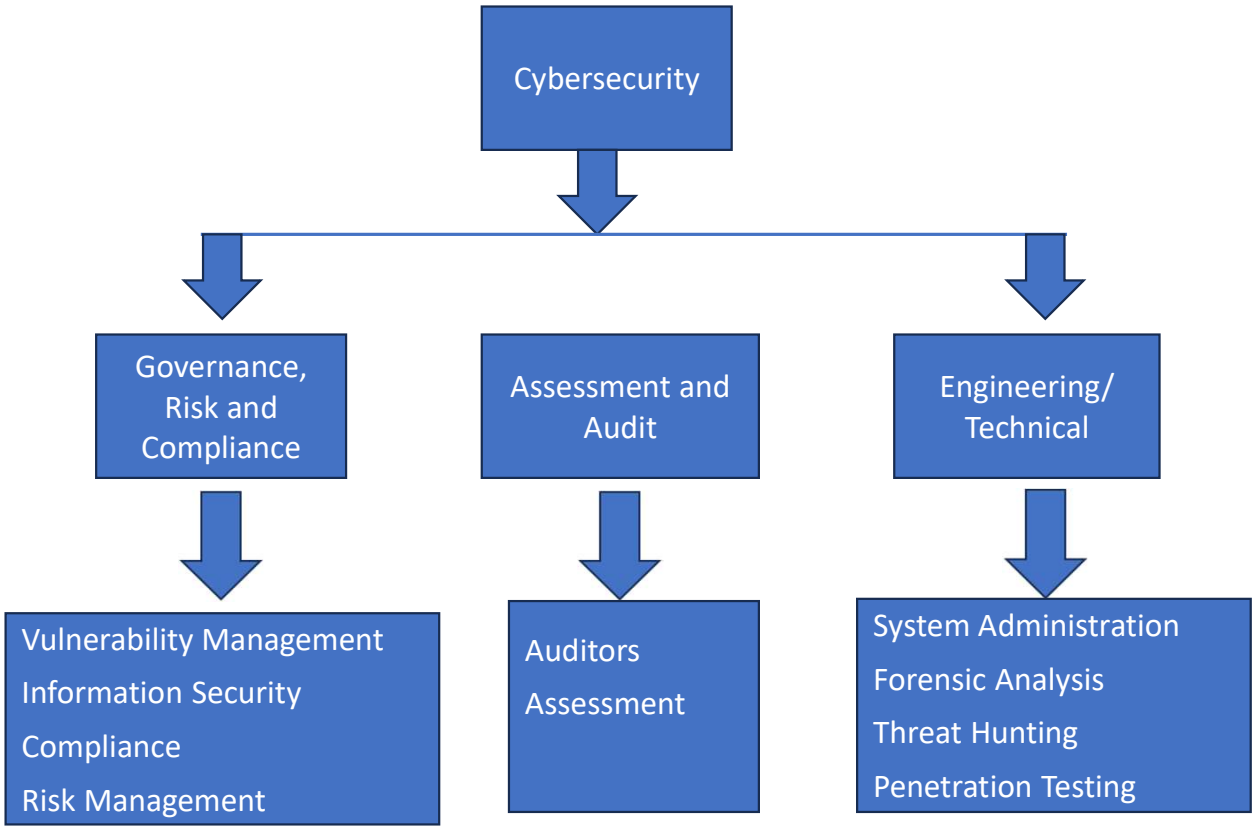
- Weekly once a week
- Saturdays 11am – 1pm US CT; 6pm – 8pm Nigerian time
- End date : Tentative March 31st, 2025.
- 15 minutes break per hour.



Class Structure

- Domain 1: Introduction to Cybersecurity
- Domain 2: Governance, Risk and Compliance
- Domain 3: Cybersecurity Engineering
- Domain 4: Resume Review and Certifications

Cybersecurity Structure



What is Cybersecurity

- Cybersecurity Definition: Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks.

- Why Cybersecurity: Cybersecurity is important because it protects all categories of data from theft and damage. This includes sensitive data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property, data, and governmental and industry information systems.

- Cybersecurity Job Market: It is expected that by 2025 there will be 3.5 million unfilled cyber security jobs due to a lack of skilled professionals and a growing need to secure more and more systems.

Certifications

- CompTIA Security Plus
- Certified Information Systems Auditor
- Certified Ethical Hackers
- Certified Information Systems Security Professional

The End

1b. Virtualization

Distributed storage	Scalability	Resource pooling
Access from any location	Measured service	Automated management

Cloud deployment models

1

Public cloud: Open for public use

2

Private cloud: Used just by the client organization

3

Community cloud: Shared between several organizations

4

Hybrid cloud: Composed of two or more clouds

IaaS, PaaS, and SaaS

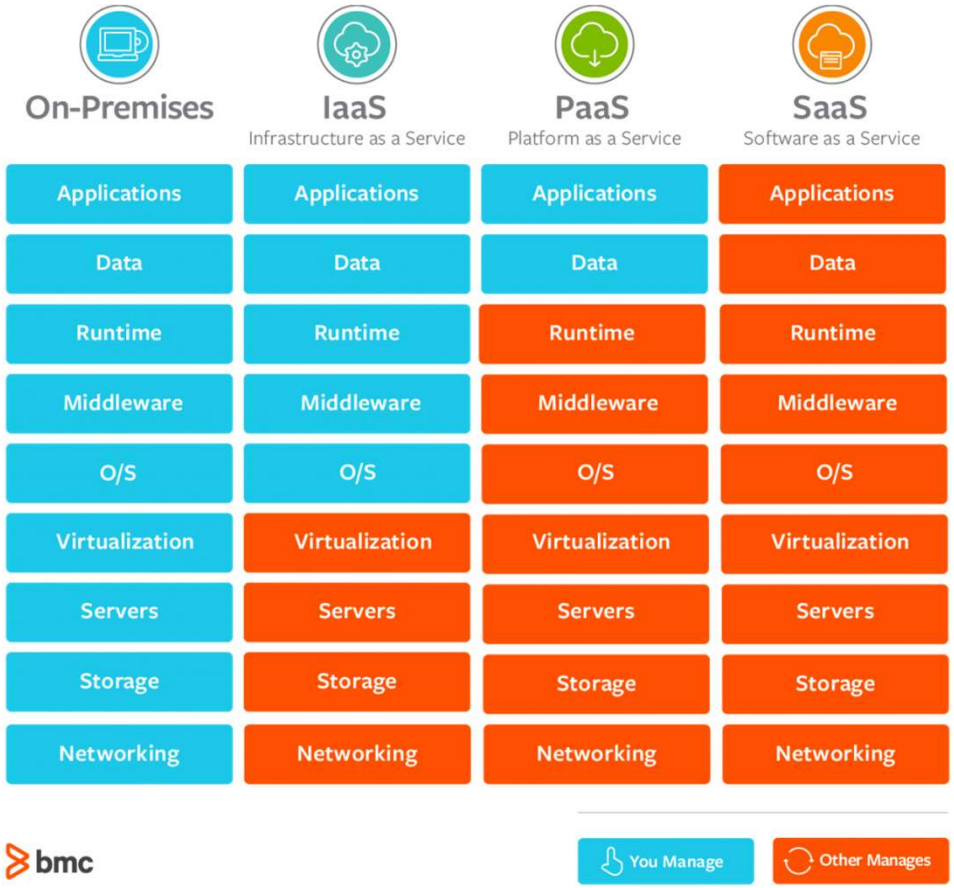
Infrastructure as a Service (IaaS) delivers the hardware for cloud services, including servers, networking, and storage.

Platform as a Service (PaaS) gives you everything that comes with IaaS, plus the operating system and databases.

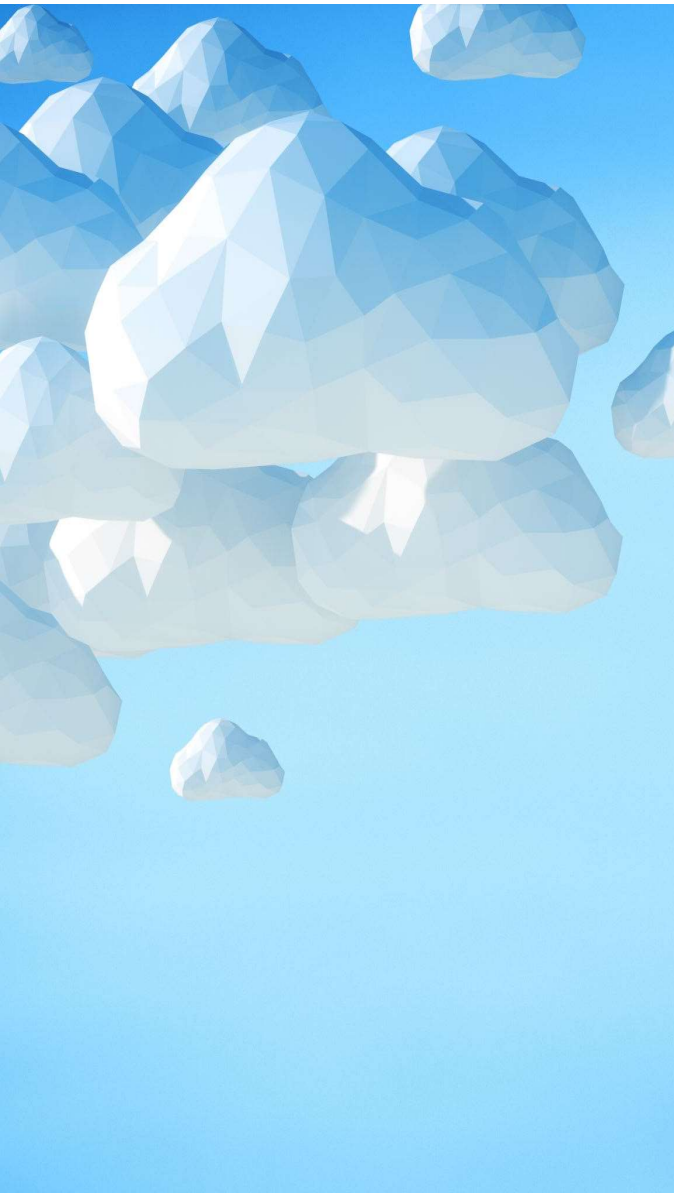
Software as a Service (SaaS) offers the most support, providing your end users with everything except for their data.

Cloud services

- Make sure you know:
- The difference between IaaS, PaaS, and SaaS.
- What is their security responsibility vs yours.



Good Questions to ask your cloud provider



The NIST SP-500-292 Cloud Computing Reference Architecture

- Provides a reference point to describe the overall framework for cloud computing in the federal government.
- It describes five major components with their roles & responsibilities
- The five major participating actors are the Cloud Consumer, Cloud Provider, Cloud Broker, Cloud Auditor and Cloud Carrier.
  - For example, a **Cloud Consumer** is an individual or organization that acquires and uses cloud products and services.
  - The seller of products and services is the **Cloud Provider**.
  - The **Cloud Broker** acts as the intermediate between consumer and provider and will help consumers through the complexity of cloud service offerings.
  - The **Cloud Auditor** provides a valuable inherent function for the government by conducting the independent performance and security monitoring of cloud services.
  - The **Cloud Carrier** is the organization who has the responsibility of transferring the data akin to the power distributor for the electric grid.

FedRAMP

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

This approach uses a “do once, use many times” framework that saves cost, time, and staff required to conduct redundant Agency security assessments.

Cloud Computing Security

Regardless of the model used, cloud security is the responsibility of both the client and the cloud provider. These details will need to be worked out before a cloud computing contract is ever signed.

The contracts will vary depending on the given security requirements of the client. Considerations include disaster recovery, SLAs, data integrity, and encryption.

As an example, is encryption provided end to end or just at the cloud provider? Also, who manages the encryption keys: the cloud provider or the client? Overall, you will want to ensure that the cloud provider has the same layers of security (logical, physical, and administrative) in place that you would have for services you control.

The difference is that you have to worry about the provider's security and your security.

Virtual machines vs containers

Virtual Machines vs. Containers

Think of a VM as a neighborhood of single-family houses, whereas a container would be one apartment building.

Every single family houses (in the single-family has its own separate infrastructure (i.e. one HVAC system), that supports multiple rooms.

- Each VM has a single infrastructure (i.e. O/S), that supports multiple guest O/S, with multiple applications on each guest operating system. Each VM has guest multiple O/Ss. Each guest O/S is equivalent to one single family house.

An apartment building has a single infrastructure (i.e. one HVAC system), that supports multiple apartments, each apartment has multiple rooms.

- A container has one infrastructure (i.e. O/S), that supports multiple **GROUPS** of applications. However, the container has only one operating system.

A VM supports multiple groups of O/Ss, whereas a Container support multiple groups of applications.

The End

1c. *Installation of Tools/Software*

- Virtual Box
- Kali Linux
- Wireshark
- NMAP
- FTK Imager
- HXD

Virtual Box 7.0.20

VirtualBox is a hypervisor used to run operating systems in a special environment, called a virtual machine, on top of the existing operating system.

https://www.virtualbox.org/wiki/Downloads

Kali Linux

Kali Linux, known initially as Backtrack Linux, is a free and open-source Linux-based operating system geared at advanced penetration testing and security auditing.

https://www.kali.org/get-kali/#kali-installer-images

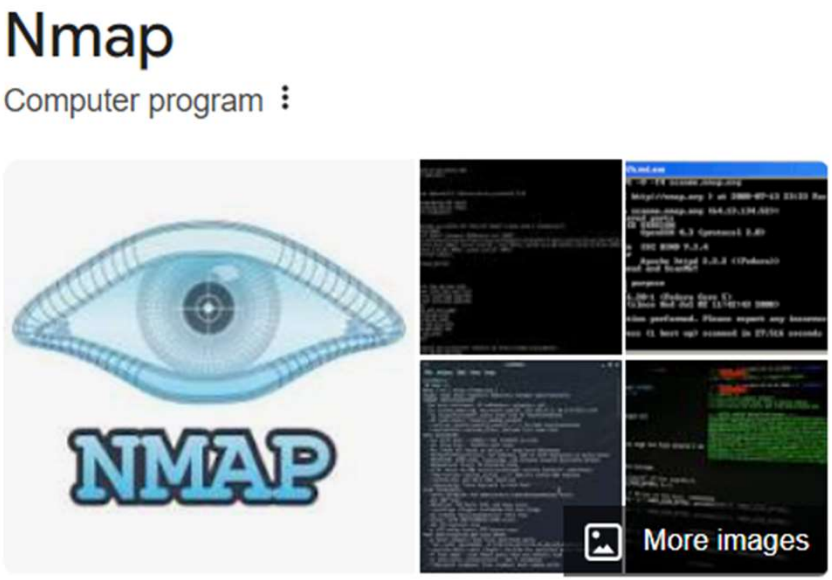
Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education

- https://www.wireshark.org/download.html

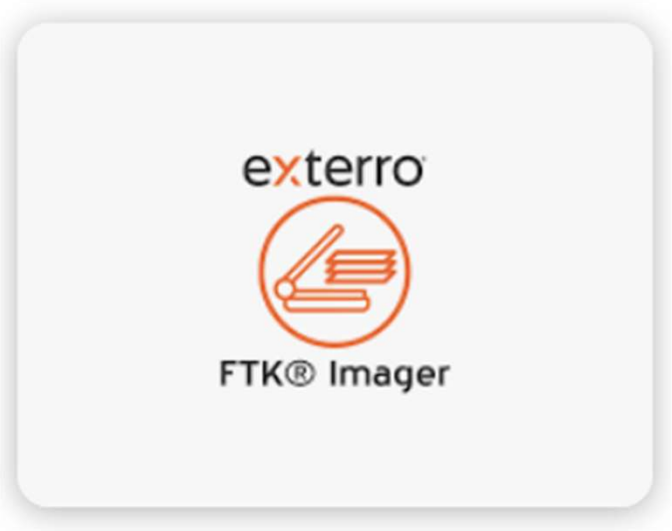
NMAP

Nmap (Network Mapper) is a network scanner used to discover hosts and services on a computer network by sending packets and analyzing the responses.

- https://nmap.org/download



FTK Imager



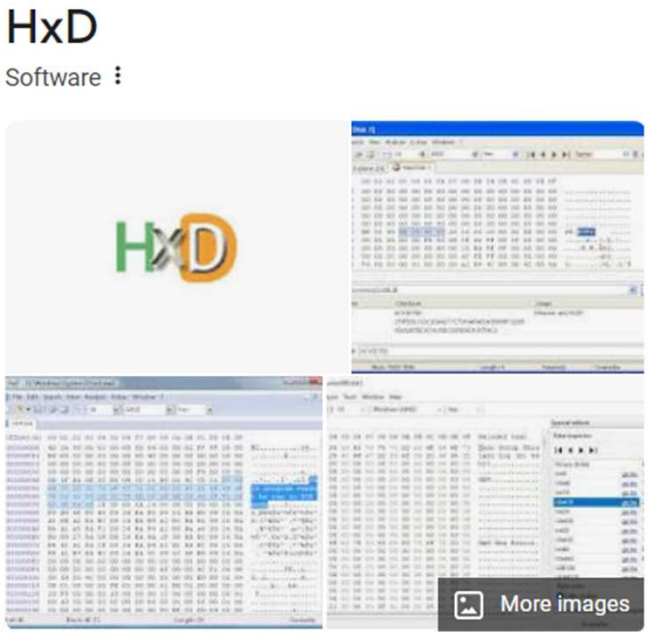
FTK Imager is a digital forensic tools used to mount and explore forensic images.

- https://accessdata-ftk-imager.software.informer.com/download/#downloading

HXD

HxD is a freeware hex editor, disk editor, and memory editor developed. It can open files larger than 4 GB and open and edit the raw contents of disk drives, as well as display and edit the memory used by running processes.

- https://mh-nexus.de/en/downloads.php?product=HxD20



- 1d. *Q & A Session*

The End

Chapter Two

Characteristics of Red, Blue & Purple Teams using command prompt

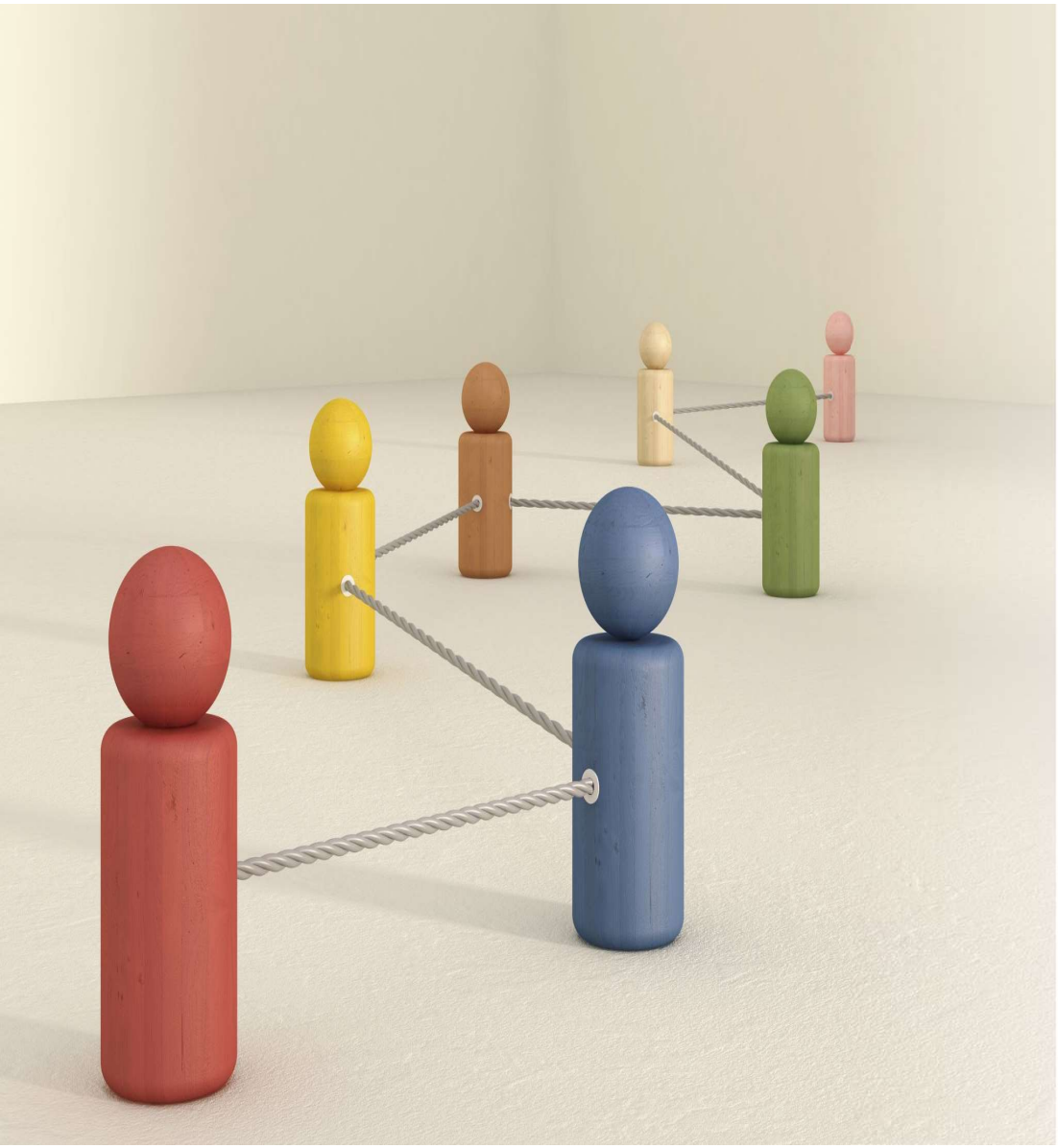
Contents

Session 2: Characteristics of Red, Blue & Purple Teams using command prompt

***Red Team**: The red team is in charge of the offensive. They must figure out creative ways to attack the company and to infiltrate it. The red team must do everything (within certain parameters) possible to succeed.*

***Blue Team**: The blue team oversees defending the company. They have to do everything they can to fend off the red team's attacks, including checking infrastructure, updating software, and preventing social engineering attempts from succeeding.*

***Purple Team**: The purple team is a mix of some characteristics of the red and blue teams. In other words, the purple team is a mixture of the other two teams: they join forces after the campaign is over, so they can figure out where the vulnerabilities are and what needs to be improved.*



Red, Blue and Purple team

From the characteristics on the last slide, you will notice that the Red Team has a unique way of looking at simple activities that are performed on a target. In this lab, we would use a few footprinting exercises to demonstrate how to think as part of a red team

*What is **Footprinting***

Footprinting is the technique used for gathering information about computer systems and the entities they belong to. To get this information, a hacker might use various tools and technologies. This information is very useful to a hacker who is trying to crack a whole system.

Labs

Lab 1: ***Using PowerShell to Find IP Address, DNS and DHCP***

Lab 2: ***Differentiating Characteristics of Blue, Red & Purple Teams Using Footprinting Techniques from Ping, Fragmentation, Tracert, NSLookup,***

1.Analyze the CNAME results for both servers. What does the default TTL results as a Red Team?

2.With regards to the entire lab, how would you explain the way a red team approaches simple system and network results in comparison to a blue team?

Lab 3: **Using PowerShell to Find Active & Listening Ports**

Lab 1: Using PowerShell to Find IP Address, DNS and DHCP

- An IP address (Internet Protocol address) is a unique numerical label assigned to every device connected to the internet, essentially acting like an online address that allows data to be sent to the correct location on the network; it's a string of numbers that identifies a device so it can communicate with other devices online.

- Domain Name Server DNS is a system that translates domain name into IP address which are used by devices to locate each other on the internet. DNS works when a user enters a domain name into their browser, the browser queries a DNS server DNS server returns the IP address for the domain name, The browser uses the IP address to load the requested web page.

- Dynamic Host Configuration Protocol DHCP: A network protocol that automatically assigns IP addresses to devices on a network. DHCP also provides other configuration information, such as subnet masks and default gateways.

- Classes of IP address. Class C: 255.255.255.0, Class B: 255.255.0.0, Class A: 255.0.0.0. Every IP has two sections, Network portion and Host portion.

Lab 2: Differentiating Characteristics of Blue, Red & Purple Teams Using Footprinting Techniques from Ping, Fragmentation, Tracert, NSLookup,

Characteristics of Red, Blue & Purple Teams

Red Team: The red team oversees the offensive. They must figure out creative ways to attack the company and to infiltrate it. The red team must do everything (within certain parameters) possible to succeed.

Blue Team: The blue team oversees defending the company. They have to do everything they can to fend off the red team's attacks, including checking infrastructure, updating software, and preventing social engineering attempts from succeeding.

Purple Team: The purple team is a mix of some characteristics of the red and blue teams. In other words, the purple team is a mixture of the other two teams: they join forces after the campaign is over, so they can figure out where the vulnerabilities are and what needs to be improved.

Lab 3: *Using PowerShell to Find Active & Listening Ports*

- A port is a physical docking point, which an external device can be connected to the computer. It can also be a programmatic docking point through which information flows from a program to the computer or over the Internet.

- A network port which is provided by the Transport Layer protocols of Internet Protocol suite, such as Transmission Control Protocol (TCP) and User Diagram Protocol (UDP) is a number which serves endpoint communication between two computers.

- To determine what protocol incoming traffic should be directed to, different port numbers are used. They allow a single host with a single IP address to run network services. Each port number has a distinct service, and each host can have 65535 ports per IP address. **Internet Assigned Numbers Authority (IANA)** is responsible for managing the uses of these ports. There are three categories for ports by IANA − 0 to 1023 – well known ports or system ports.

Lab 3: *Using PowerShell to Find Active & Listening Ports*

Some well-known ports are −

Port number	Transport protocol	Service name
20,21	TCP	File Transfer Protocol
23	TCP	Telnet
25	TCP	Simple Mail Transfer Protocol(SMTP)
53	TCP and UDP	Domain Name System(DNS)
110	TCP	Post Office Protocol(POP3)
123	UDP	Network Time Protocol(NTP)

- **1024 to 49151** – registered ports assigned by IANA to a specific service upon application by a requesting entity.
- **49152 to 65 535** – dynamic (private, high) ports range from 49,152 to 65,535. Can be used by private or customer service or temporal purposes.

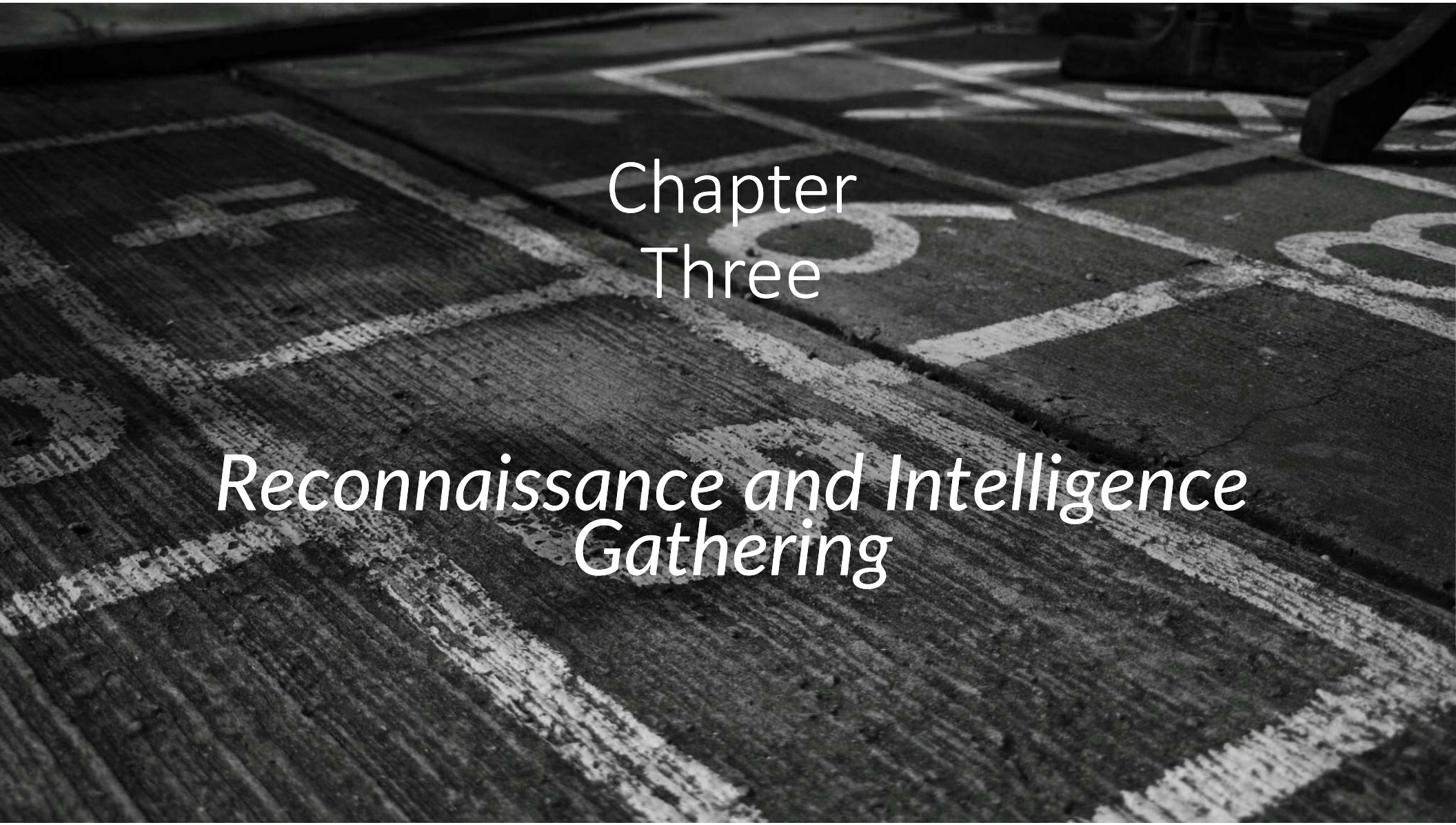
Lab 3: *Using PowerShell to Find Active & Listening Ports*

Transport Protocols

- **Transmission Control Protocol (TCP):** Communications standard for delivering data and messages through networks. TCP is a basic standard that defines the rules of the internet and is a common protocol used to deliver data in digital network communications.
  - More secured
  - Uses three-way handshake
  - Less fast than UDP

- **User Datagram Protocol (UDP):** Communication protocol that sends data packets over the internet. It's often used for time-sensitive applications like video streaming and online gaming.
  - Faster than TCP because it doesn’t wait to establish a connection
  - Suitable for applications that can tolerate some data loss

- *Q & A Session*



Chapter Three

Reconnaissance and Intelligence Gathering

Contents

What is Reconnaissance?

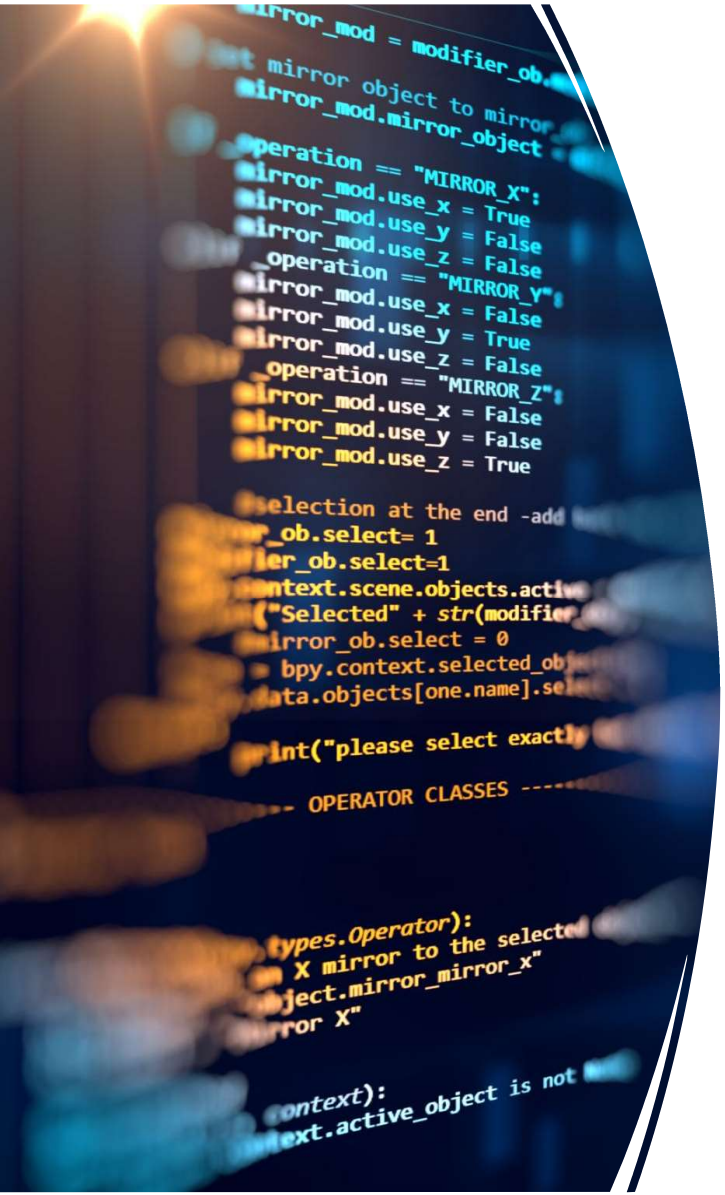
Cybersecurity reconnaissance is the preliminary phase of a cyber attack. It involves the systematic surveying or scanning of systems, networks, or web applications to gather information about potential vulnerabilities that can be exploited.

Two different tools used for reconnaissance which will be covered in this class.

- *Shodan*
- *VirusTotal*

Log Review

- **Logs** are records of events that happen in your computer, either by a person or by a running process. They help you track what happened and troubleshoot problems.
- Why are logs so cryptic?
  - The output format could be very cryptic, and in such a format that only the developers will truly understand because they created it. They generally have no interest in generating output for the common user, nor do they have any mandate or standard that tells them to.
  - This creates problems for security professionals or computer administrators who are trying to investigate an incident or failure that may have occurred within their infrastructure.



Security Information and Event Management (SIEM) and Log Management

- SIEMs and Log Management are two examples of software tools that allow IT organizations to monitor their security posture using log files, detect and respond to Indicators of Compromise (IoC) and conduct forensic data analysis and investigations into network events and possible attacks.
- The easiest way to think of a SIEM is that it is part IDS and part Log management tool.
- Syslog is a logging system that has been standardized so that any flavor of UNIX/Linux operating system will output the same log format.
- Windows operating systems support the Eventlog format, and all events output to a standardized event log format.

Watch these videos to learn about reading logs	
Find out what users are doing on your network https://www.youtube.com/watch?v=nv0uHGKXAkQ Understanding audit logs https://www.youtube.com/watch?v=iR8GjOwTOrQ Syslog a logging system that monitors events on devices https://www.youtube.com/watch?v=2jDYd5RkAl8 Deciphering Log Files (Using Syslog) https://www.youtube.com/watch?v=C4JLuatkRvQ	Searching Through Logs: Where Do I Start? https://www.youtube.com/watch?v=48f_TFkZ5EA Basic Approach: Analyzing Files Log For Attacks (2020) https://www.youtube.com/watch?v=-T6oue5E4KQ Log Analysis - CompTIA Security+ SY0-401: 1.2 https://www.youtube.com/watch?v=fGVFCaVQnWw Real-Time Log Analytics using Splunk | Basic Searching Log File https://www.youtube.com/watch?v=EPfz82XRQFk

Reconnaissance

Passive Reconnaissance **They can just search on the Internet**	**Active Reconnaissance** **Who is touching our systems**
Open Source Intelligence (OSINT)	Scanning
Review Website	Banner grabbing
Is the company directory online	Searching Regional Internet Registries (RIR)
Financial database (EDGAR)	Vulnerability scanning
What does your Email give away	
What do Job boards give away	
What are your employees saying on social media	
Google Dorking	
Searching Regional Internet Registries (RIR)	

Open Source Intelligence (OSINT)

- Data collected from publicly available **sources** to be used in an **intelligence** context. In the **intelligence** community, the term "**open**" refers to overt, publicly available **sources** (as opposed to covert or clandestine **sources**).

Open Source Intelligence (OSINT)

- https://traversals.com/blog/osint-tools/

- There are many online services for gaining information about a website's technology. The two most popular are:
- BuiltWith
- Wappalyzer

Recon 101

Examine the company's website using

Wayback machine: The Wayback Machine is a digital archive of the web, created in 1996 by the Internet Archive. It lets users see past versions of websites

Company Directories

These usually identify key employees or departments . By combining this information with a little social engineering, an attacker can call the help desk, pretend he works for one of these key employees, and demand that a password be reset or changed. He could also use biographical information about a key employee to perform other types of social engineering trickery.

Send an email that will bounce from the site.

If the site is www.xyz.com , send a mail to badaddress@xyz.com . It will bounce back to you and give you information in its header, including the email server IP address and email server version.

Information Gathering Tools

- Shodan
  - https://www.shodan.io/
  - Shodan is the world's first search engine for Internet-connected devices. ... Use Shodan to discover which of your devices are connected to the Internet.
- The Harvester
  - https://github.com/laramies/theHarvester/
  - This tool is intended to help Penetration testers in the early stages of the penetration test in order to understand the customer footprint on the Internet. It is also useful for anyone that wants to know what an attacker can see about their organization.
- Maltego
  - Maltego is an interactive data mining tool that renders directed graphs for link analysis. The tool is used in online investigations for finding relationships between pieces of information from various sources located on the Internet.

What is running on this machine

- There are approximately 65,535 port numbers; they are divided into
  - Well-known ports (0–1023),
  - Registered ports (1024–49151), and
  - Dynamic ports (49152–65535)

- **A port number is used to uniquely identify an application or processes running on a single computer.**

- A port number allows applications on your machine to communicate over the Internet.
  - Example,
    - Your machine can have many applications that need to communicate over the Internet, they can do so by assigning each application a port number. Each of these applications with their assigned port number can then share can share one IP address.

Finding Open Ports and Access Points

- Port scanning is the process of connecting to TCP and UDP ports for the purpose of finding what services and applications are running on the target device.

- After running applications, open ports, and services are discovered, the hacker can then determine the best way to attack the system.

- **WARNING**
- Scanning someone's network can be considered **ILLEGAL**.

- 20-21 FTP
- 22 SSH
- 23 Telnet
- 25 SMTP
- 53 DNS TCP/UDP
- 67/68 DHCP UDP
- 69 TFTP UDP
- 79 Finger
- 80 HTTP
- 88/464 Kerberos TCP/UDP
- 110 POP3 TCP
- 111 RPCBind
- 135 MSRPC
- 137/138/139 NetBios
- 143 IMAP

- 161/162 SNMP UDP
- 389 LDAP TCP
- 443 SSL/TLS TCP
- 445 SMB TCP/UDP
- 993 IMAPS
- 995 POP3S
- 1701 L2TP
- 1723 PPTP
- 3306 MYSQL
- 3389 RDP
- 5900 VNC
- 8080 HTTP-Proxy
- **You need to learn these port numbers and programs!!!!**

DNS Harvesting

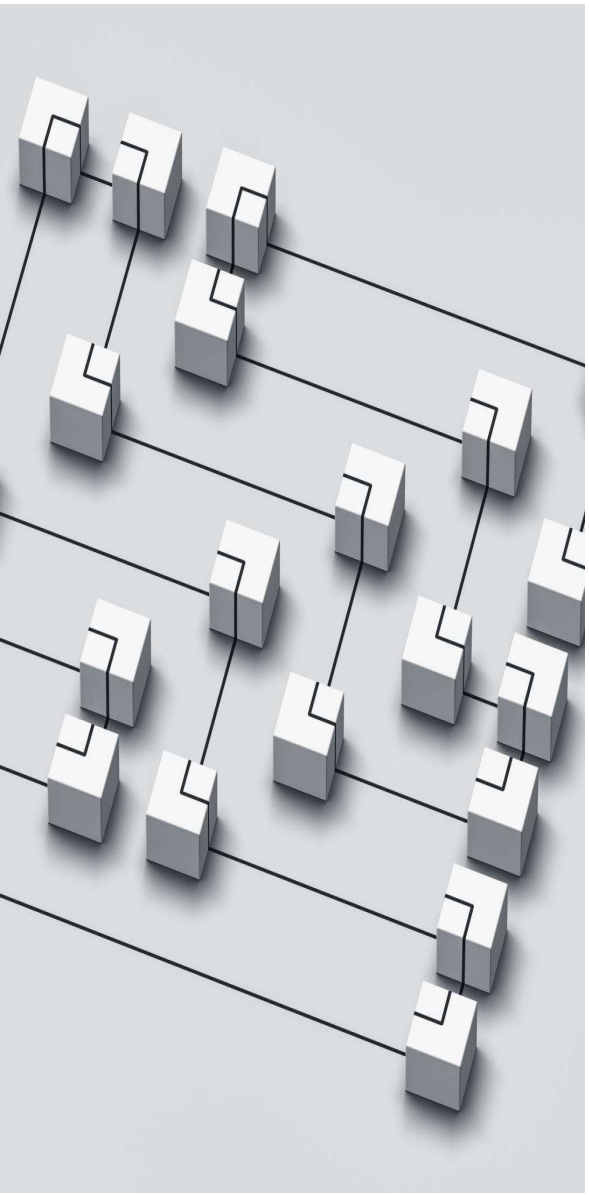
- DNS harvesting enables hackers to gain access to the DNS records of an organization, which can then be used to map the organization's network.

- DNS harvesting methods include exploiting Whois, unauthorized zone transfers, Windows Tracert, or the UNIX traceroute tool. These harvesting methods transfer data from servers which have not been setup standards.

- A Security Analyst can control unauthorized transfers by specifying the DNS servers where zone transfers can take place.

Practice DNS harvesting

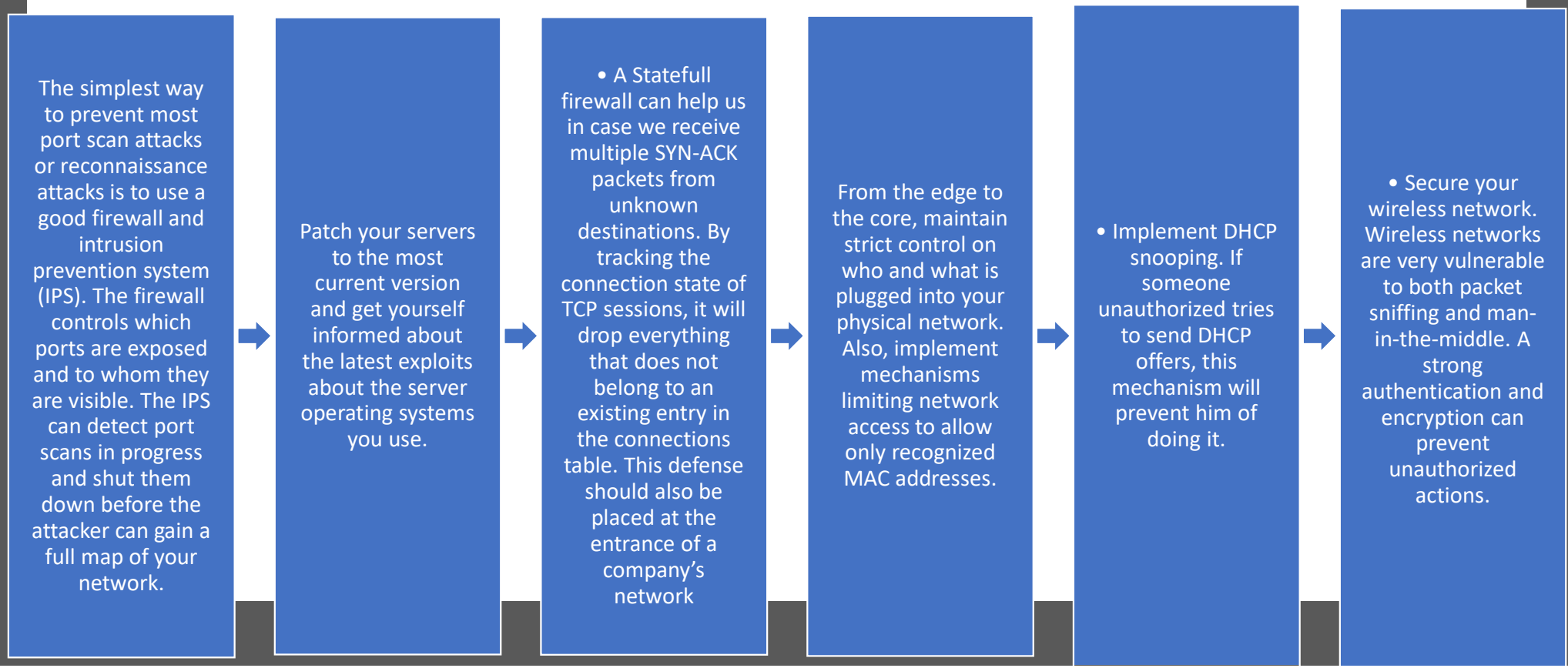
https://digi.ninja/projects/zonetransferme.php



DNS Enumeration

- Is the process of locating all information about DNS.
- This can include identifying internal and external DNS servers and performing lookups of DNS records for information such as usernames, computer names, and IP addresses of potential target systems and performing zone transfers.
- The most straightforward way is to use **Nslookup** Tools for DNS enumeration.
- Other tools include the following:
  - DigDug
  - WhereIsIP
  - NetInspector
  - Men and Mice Management Console

Preventing reconnaissance



Shodan Tool

Shodan – Search engine for Internet-connected devices. Web search engines, such as Google and Bing, are great for finding websites.

Shodan gathers information about all devices directly connected to the Internet. If a device is directly hooked up to the Internet, then Shodan queries it for various publicly-available information. The types of devices that are indexed can vary tremendously: ranging from small desktops up to nuclear power plants and everything in between

Network Security: keep an eye on all devices at your company that are facing the Internet.

Market Research: find out which products people are using in the real-world

Cyber Risk: include the online exposure of your vendors as a risk metric

Internet of Things: track the growing usage of smart devices

Tracking Ransomware: measure how many devices have been impacted by ransomware

Shodan Lab Exercise

- *In this lab, we would be using Shodan to carry out reconnaissance activities.*
- *Requirements:*
  - *High Speed Internet*
- *Estimated Time*
  - *Varies*

VirusTotal Tool

VirusTotal is an online tool launched in June 2004 and acquired by Google in September 2012. The company's ownership switched in January 2018 to Chronicle, a subsidiary of Google.

VirusTotal inspects items with over 70 antivirus scanners and URL/domain blocklisting services, in addition to a myriad of tools to extract signals from the studied content. Any user can select a file from their computer using their browser and send it to VirusTotal.

VirusTotal Lab Exercise

- *In this lab, we would be using VirusTotal to carry out reconnaissance activities.*
- *Requirements:*
  - *High Speed Internet*
- *Estimated Time*
  - *Varies*

- *Q & A Session*

The End

Contents