TERMS, TOOLS AND CONCEPTS YOU NEED TO KNOW

OSINT = Gathering public info online.
whois lookup tool = Find website owner and registration details.
nslookup tool = Find a website's IP address.
Port Scanning = Check open "doors" on a server.
Nmap tool = A tool to scan ports safely and legally.

What is OSINT?

OSINT stands for Open Source Intelligence.

Think of it like being a detective, but instead of searching secret files, you only use publicly available information—like websites, online records, and public databases.

It's sometimes called information gathering or reconnaissance.

Why Learn OSINT?

- It's legal (when done ethically).
- It helps you understand what others can find about you online.
- It's the first step in securing systems.

OSINT Tools & How to Use Them

1. WHOIS LOOKUUP

Purpose: Find who owns a website, when it was registered, and where it's hosted.
How to practice:

- **Go to:** https://whois.domaintools.com

- Type in a website name (like example.com) in the search bar where it says "Enter a domain or IP address"
- **Look for:**
  - **Registrant:** Who owns it
  - **Registration Date:** When it was created
  - **Name Servers:** Where it's hosted/Country
  - **IP Address:** The server's IP address

Hands-On Exercise:

Look up these sites (from the case study) and note what you find:

- grandsquareng.com
- justriteonline.com

2. NSLOOKUP

Purpose: Find the IP address of a website.

How to practice (on Windows):

- Open Command Prompt (search for cmd in Start menu)
- **Type:**

```
nslookup justriteonline.com
```

- You'll see the IP address under "Address", in the Non-authoritative answer section.
- If you ping this IP address, you are pinging the host/server where justriteonline website's files are hosted.

On Mac/Linux:

- Open Terminal and type the same command.

Hands-On Exercise:

Run nslookup for:

- google.com
- grandsquareng.com

PORT SCANNING

What is Port Scanning?

Port scanning is like checking which doors and windows of a house are open.

Computers have “ports” (like doors) that services use to communicate. By scanning, we see which ports are open, closed, or filtered (blocked).

Why Scan Ports?

- To find security weaknesses
- To understand what services are running (like web servers, email, etc.)

Port Scanning with Nmap

What is Nmap?

Nmap is a free and powerful tool for scanning networks and ports.

Nmap is a tool that is already installed on Kali Linux. It comes pre-installed on kali linux

Hands-On Exercises with Nmap

Exercise 1: Scan a Virtual Machine (like Wazuh)

- Make sure your VM is running.
- Open Command Prompt or Terminal.
- **Type:**

```
nmap [IP-address-of-VM]
```

- Replace [IP-address-of-VM] with your VM’s IP e.g wazuh's IP (find it in your VM settings or through your VM's terminal)
- The command by default scans the top most important 1000 ports. You’ll see a list of open ports and services.
- For instance if wazuh's ip is 192.168.56.102 our command would be:

```
nmap 192.168.56.102
```

Exercise 2: Scan a Website's Server with nmap (Legally)

- Only scan websites you own or have permission to scan.
- Find the IP of the website using nslookup (as learned earlier) e.g. justrite
- **Scan it with:**

```
nmap [IP-address-of-JustRite]
```

- **Example for JustRite:**

```
Replace [IP-from-nslookup-justriteonline.com] with the
actual ip address of justriteonline.com you got earlier
```

- Note which ports are open (like 80 for HTTP, 443 for HTTPS).

Exercise 3: Use a Port Scanner Script

Beginners can use online tools to practice legally:

- **Go to:** https://pentest-tools.com/network-vulnerability-scanning/tcp-port-scanner-online-nmap
- Enter a target IP of the website and proceed with your scan
- Run the scan and review results.

Important Rules for Beginners

✅ **Do:**

- Only scan your own devices or VMs
- Use OSINT tools on public websites ethically
- Learn for educational purposes