



Applied Cyber Security Industry Led-Course

Instructor: XYZ

Lab Instructor: Moez Javed

Lab 2: Network Scanning, Reconnaissance, and Vulnerability Analysis

Availability:

Monday to Friday: 9 AM – 5 PM (at CUST)

After 5 PM: Please drop a message instead of calling.

Lab Instructor Contact Details:

Phone: +92 333 8744696

Email: moezjavedmj@gmail.com

Introduction:

In the field of cybersecurity, understanding how networks function and how to assess their security is crucial. This lab focuses on using **Nmap (Network Mapper)**, a powerful network scanning tool, to identify devices, services, and vulnerabilities within a network. Additionally, we explore reconnaissance techniques using **Open Source Intelligence (OSINT) tools**, as well as **Google Hacking Database (GHDB) queries** for information gathering.

By the end of this lab, participants will gain hands-on experience in **network scanning, vulnerability detection, and reconnaissance** techniques, preparing them for real-world cybersecurity assessments.

NMAP:

Nmap (Network Mapper) is a free, open-source network scanning tool that helps identify devices, services, and operating systems on a network. It's used for security, troubleshooting, and network diagnostics.

How Nmap works ?

Uses IP packets to identify devices connected to a network
Analyzes packet responses to determine if ports are open, closed, or filtered
Supports many port scanning mechanisms, including TCP and UDP
Can perform OS detection, version detection, and ping sweeps

Why use Nmap?

- Security: Identify nodes and operating systems, and audit the security of a device or firewall
- Troubleshooting: Identify unexpected ports and systems
- Network diagnostics: Understand network devices and services
- Network inventory: Map networks, manage assets, and perform maintenance

Who uses Nmap?

Network administrators, Security professionals, Penetration testers, and Red and blue team exercise participants.

Nmap is available for Linux, macOS, and Windows. It's scriptable and can be integrated into DevSecOps pipelines. You can use Nmap via the terminal (command-line console) or through a graphical user interface (GUI).

Why Windows 10 and Nmap?

Windows 10:

Windows 10 is one of the most widely used operating systems in enterprise environments.

Many security tools and penetration testing frameworks are designed to work with Windows.

Virtual machines running Windows 10 allow for safe, controlled testing environments for cybersecurity assessments.

Nmap:

Free & Open-Source: Nmap is widely used for **network discovery, security auditing, and troubleshooting**.

Port Scanning & OS Detection: It helps identify **open ports, running services, and operating systems** on a network.

Security & Vulnerability Assessment: Nmap can detect potential vulnerabilities by analyzing open ports and system configurations.

Versatile & Cross-Platform: It runs on **Windows, macOS, and Linux** and can be integrated into **DevSecOps pipelines**.

First Download Window 10 ISO File:

Create Windows 10 installation media

To get started, you will first need to have a licence to install Windows 10. You can then download and run the media creation tool. For more information on how to use the tool, see the instructions below.

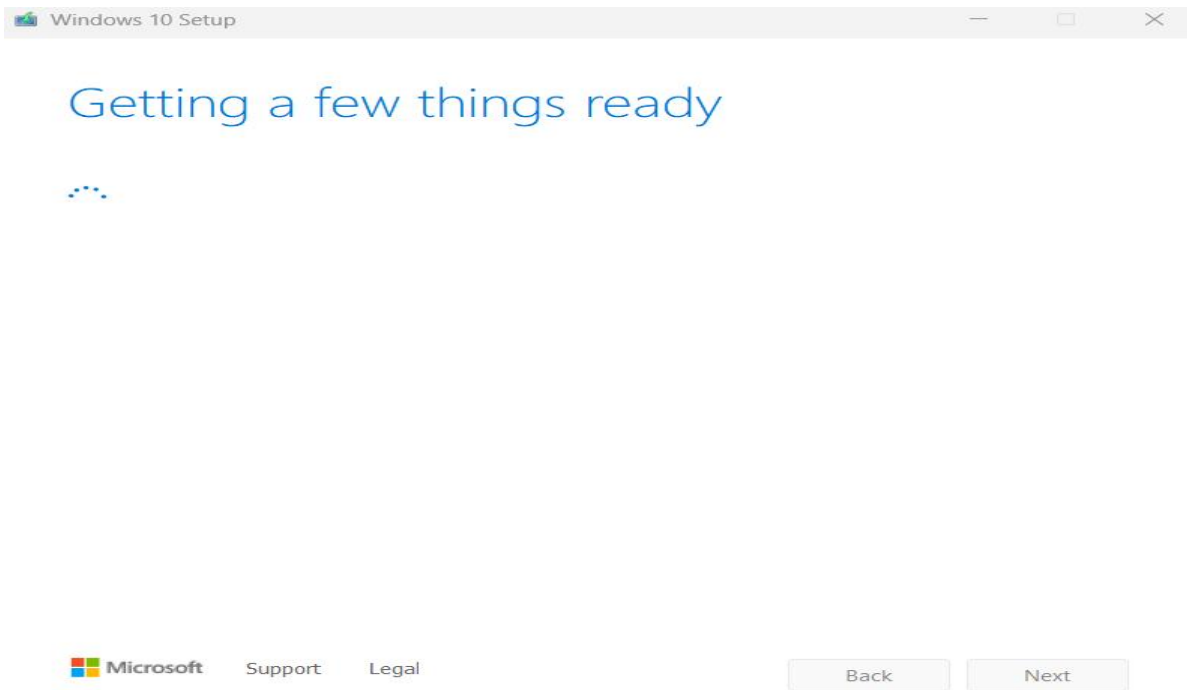
[Download Now](#)



> [Using the tool to upgrade this PC to Windows 10 \(click to show more or less information\)](#)

> [Using the tool to create installation media \(USB flash drive, DVD, or ISO file\) to install Windows 10 on a different PC \(click to show more or less information\)](#)

Then Click on Next:



Click Accept:

Applicable notices and license terms

Please read this so you know what you're agreeing to.

NON-INFRINGEMENT.

13. LIMITATION ON AND EXCLUSION OF DAMAGES. IF YOU HAVE ANY BASIS FOR RECOVERING DAMAGES DESPITE THE PRECEDING DISCLAIMER OF WARRANTY, YOU CAN RECOVER FROM MICROSOFT AND ITS SUPPLIERS ONLY DIRECT DAMAGES UP TO U.S. \$5.00. YOU CANNOT RECOVER ANY OTHER DAMAGES, INCLUDING CONSEQUENTIAL, LOST PROFITS, SPECIAL, INDIRECT OR INCIDENTAL DAMAGES.

This limitation applies to (a) anything related to the software, services, content (including code) on third party Internet sites, or third party applications; and (b) claims for breach of contract, warranty, guarantee, or condition; strict liability, negligence, or other tort; or any other claim; in each case to the extent permitted by applicable law.

It also applies even if Microsoft knew or should have known about the possibility of the damages. The above limitation or exclusion may not apply to you because your state, province, or country may not allow the exclusion or limitation of incidental, consequential, or other damages.

[Privacy statement](#)



Microsoft

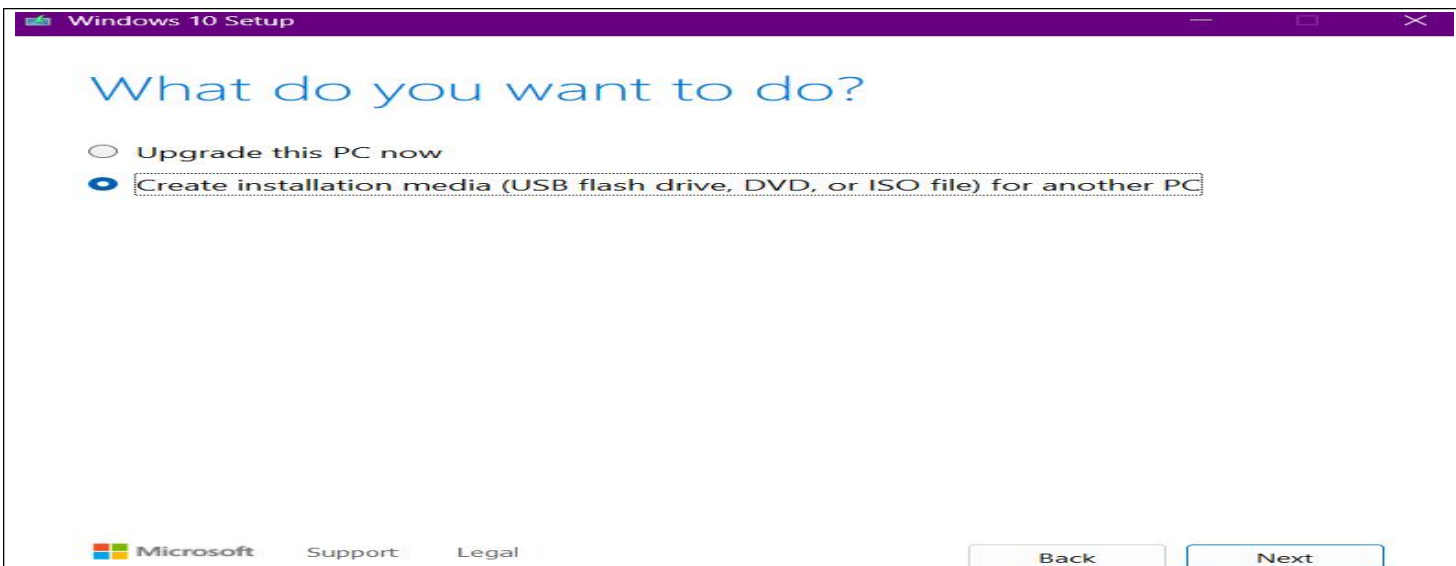
[Support](#)

[Legal](#)

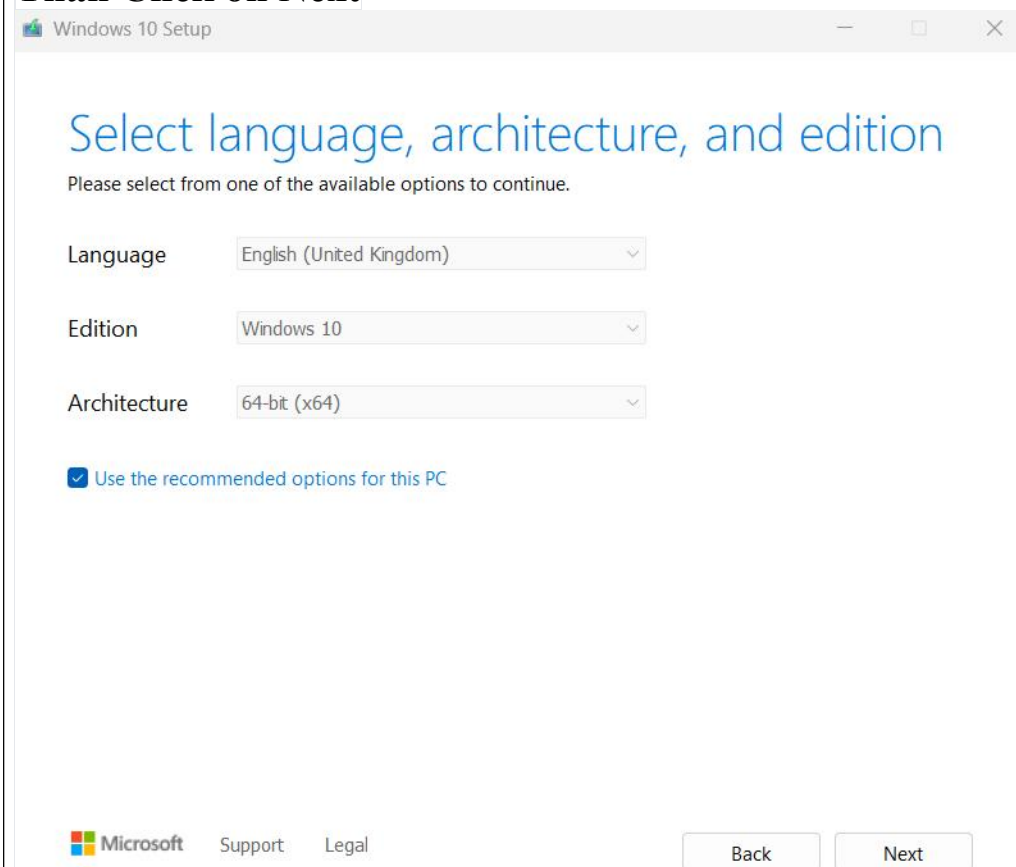
Decline

Accept

**After that first select Create Installation Media:
than click on Next**



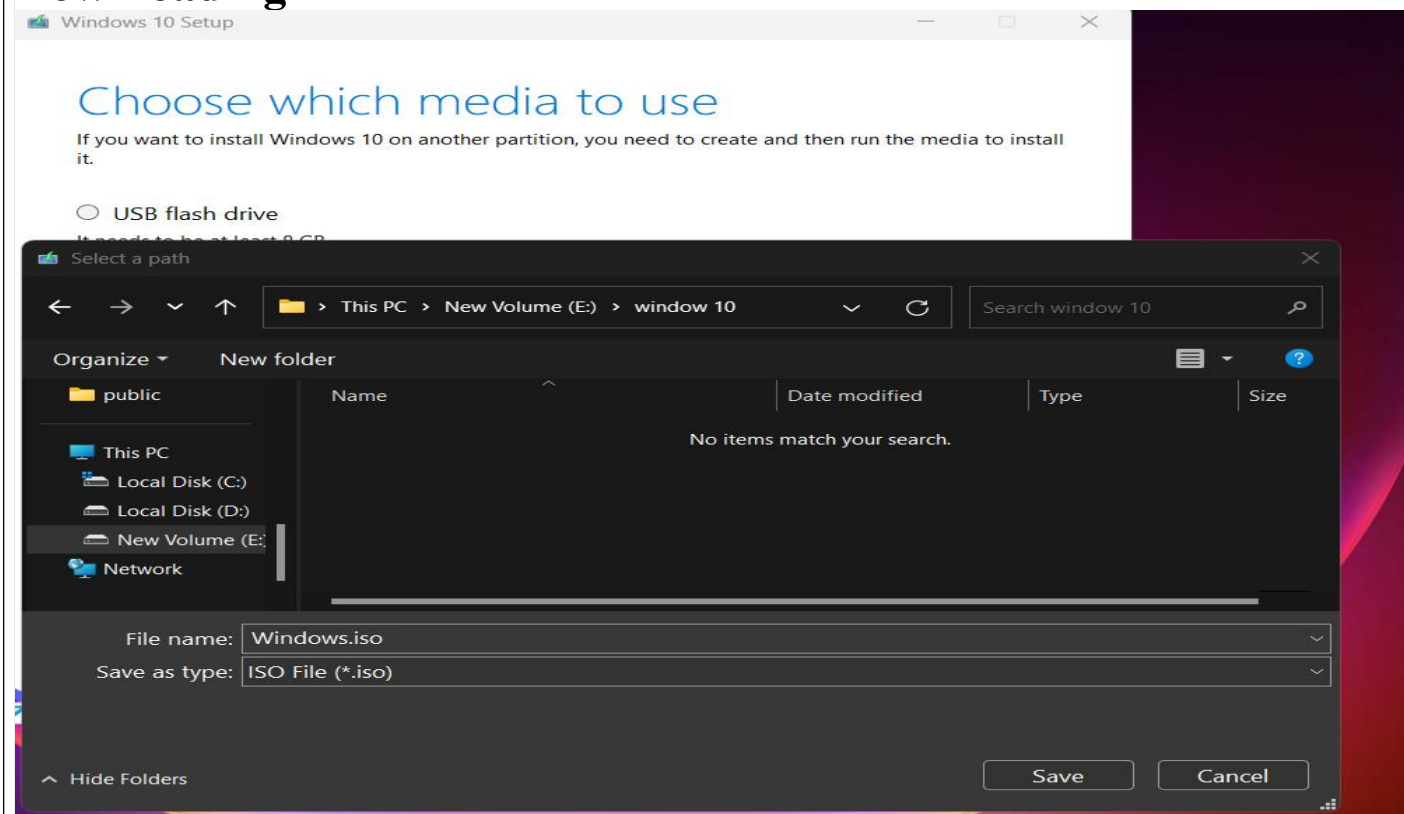
Than Click on Next



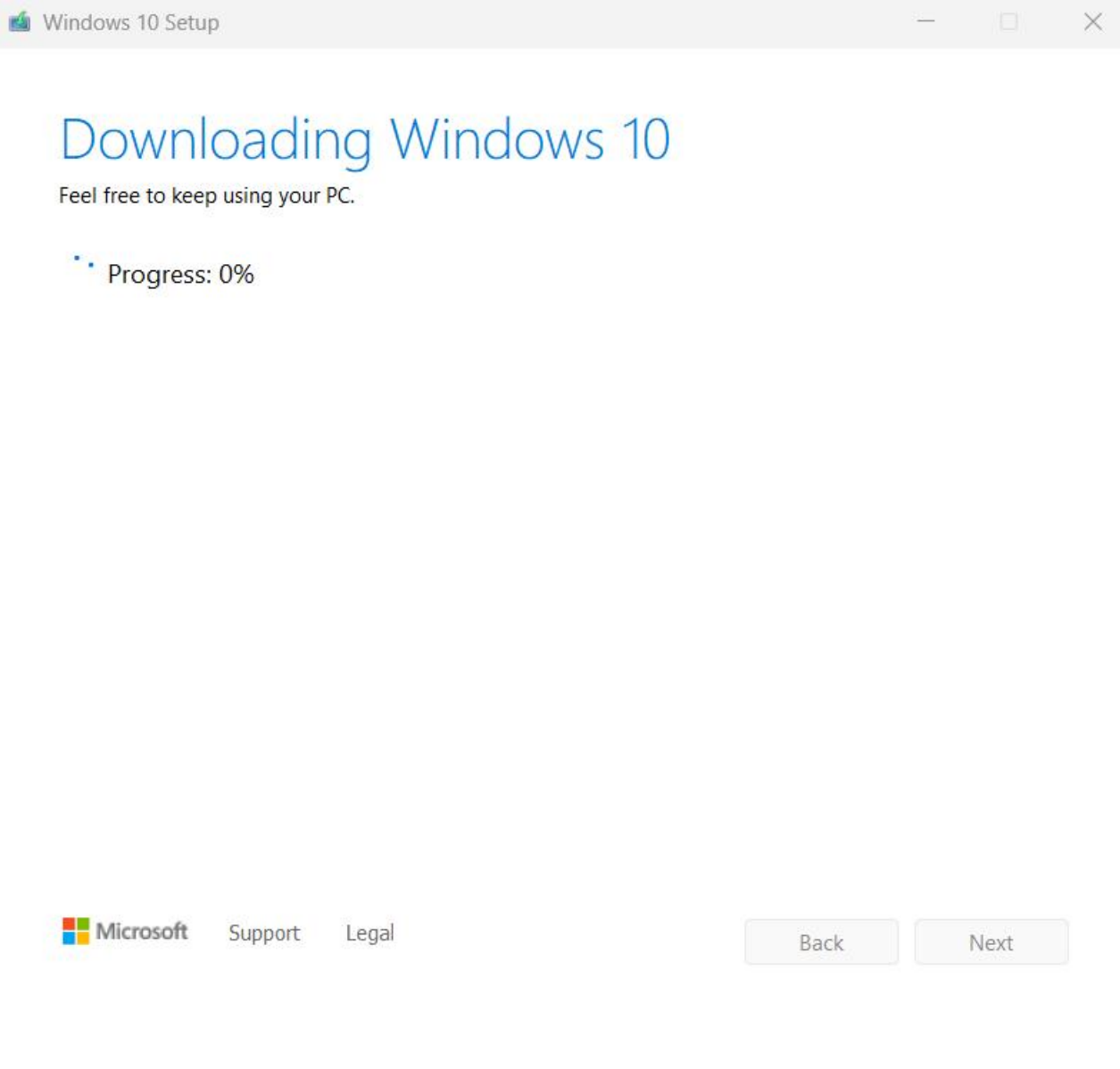
Select ISO File and Click Next:



Than Click on Next after that select location of iso file and start Downloading



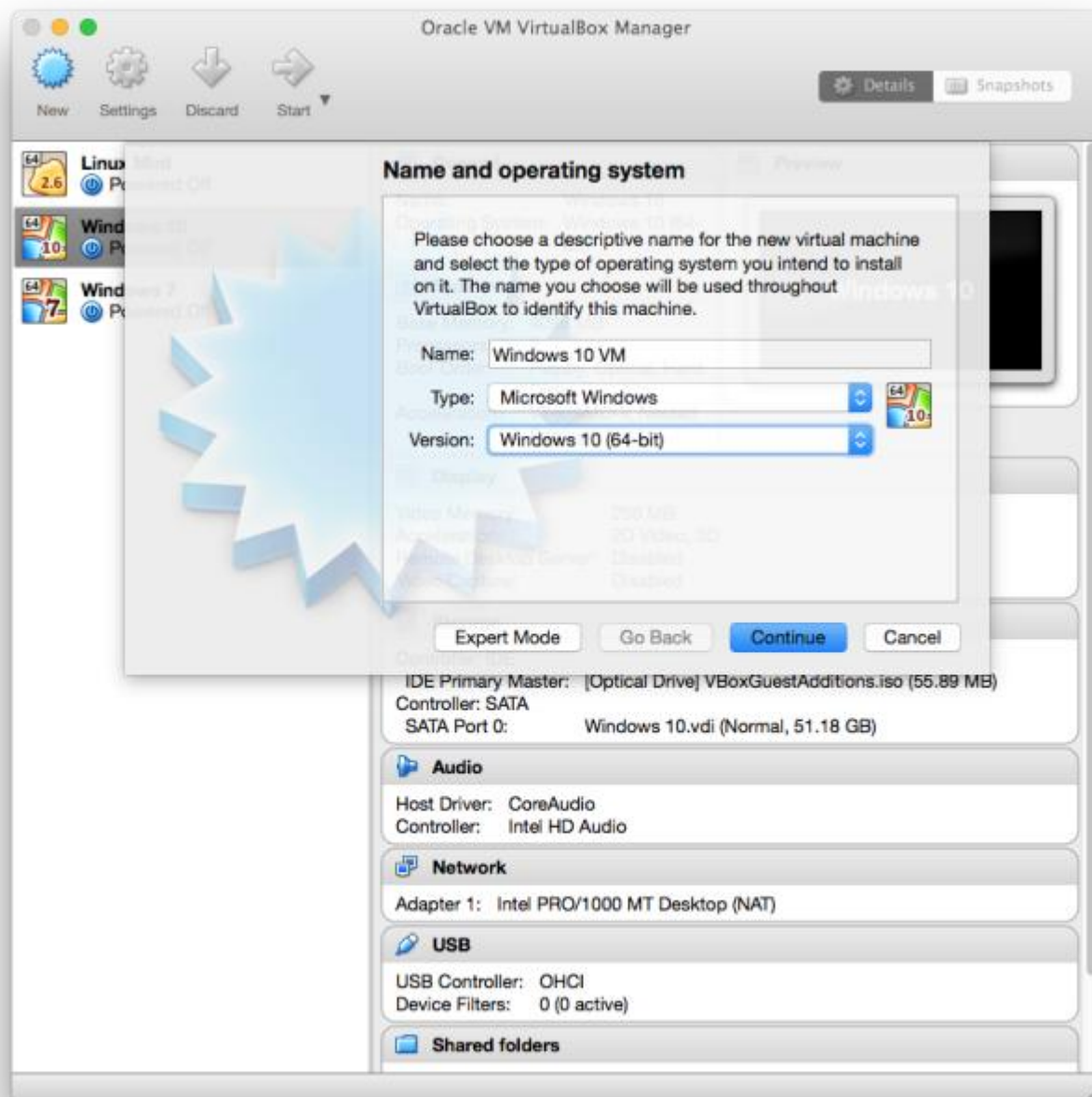
Than



VirtualBox Installation

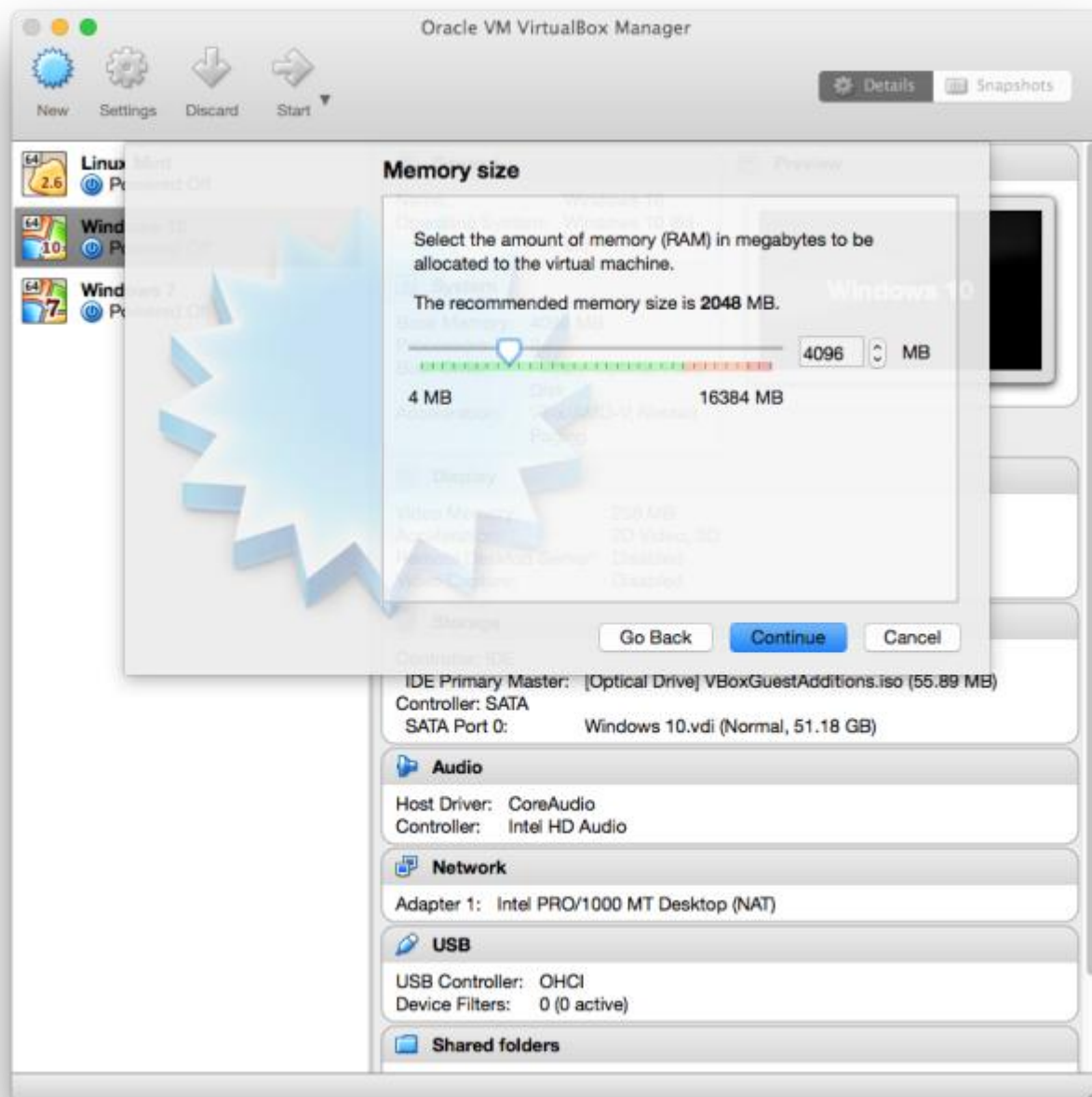
1. Download the Windows 10 ISO

First, head over to the Windows 10 download page If you are a Windows user. Microsoft will prompt you to download the Media Creation Tool before allowing you to download an OS image. You can use this tool to create an ISO file locally, or you can follow these additional instructions to download the ISO manually without being forced to grab the tool first.



2. Create a New Virtual Machine

Go to the VirtualBox website and download the latest version of Oracle's free, open-source software. Go through the installation process, and then launch the application. Press the "New" button, and name your virtual machine. Make sure your "Type" is set to "Microsoft Windows" and your "Version" is set to "Windows 10." Make sure you match the x64 version with a 64-bit VM and the x86 version with a 32-bit VM.



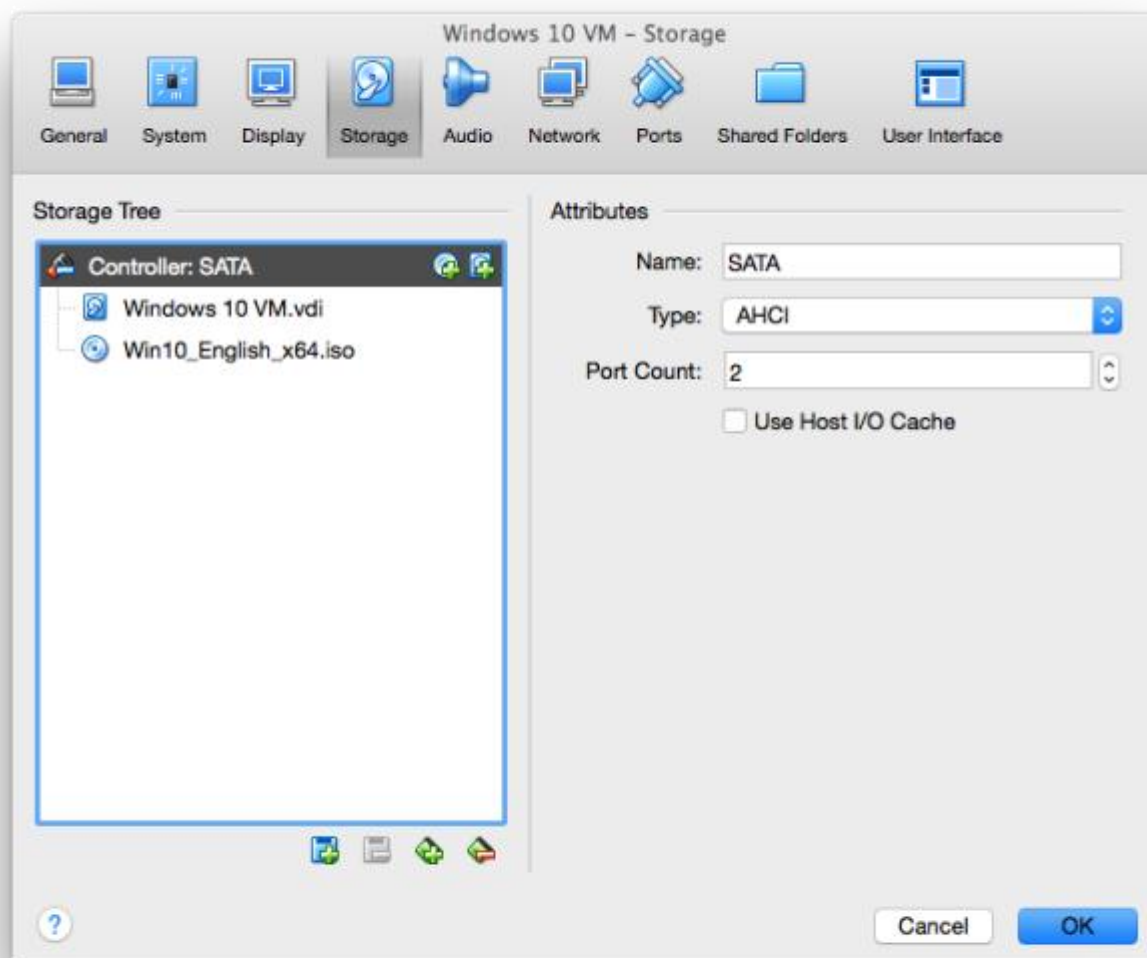
3. Allocate RAM

Now, you must decide how much RAM you want to allocate for this VM. For the x86 version, you'll need at least 1GB of RAM. For the x64 version, you'll need 2GB. Whatever you decide, just make sure you stay in the green. If you allocate too much RAM, you'll end up with serious performance issues.



4. Create a Virtual Drive

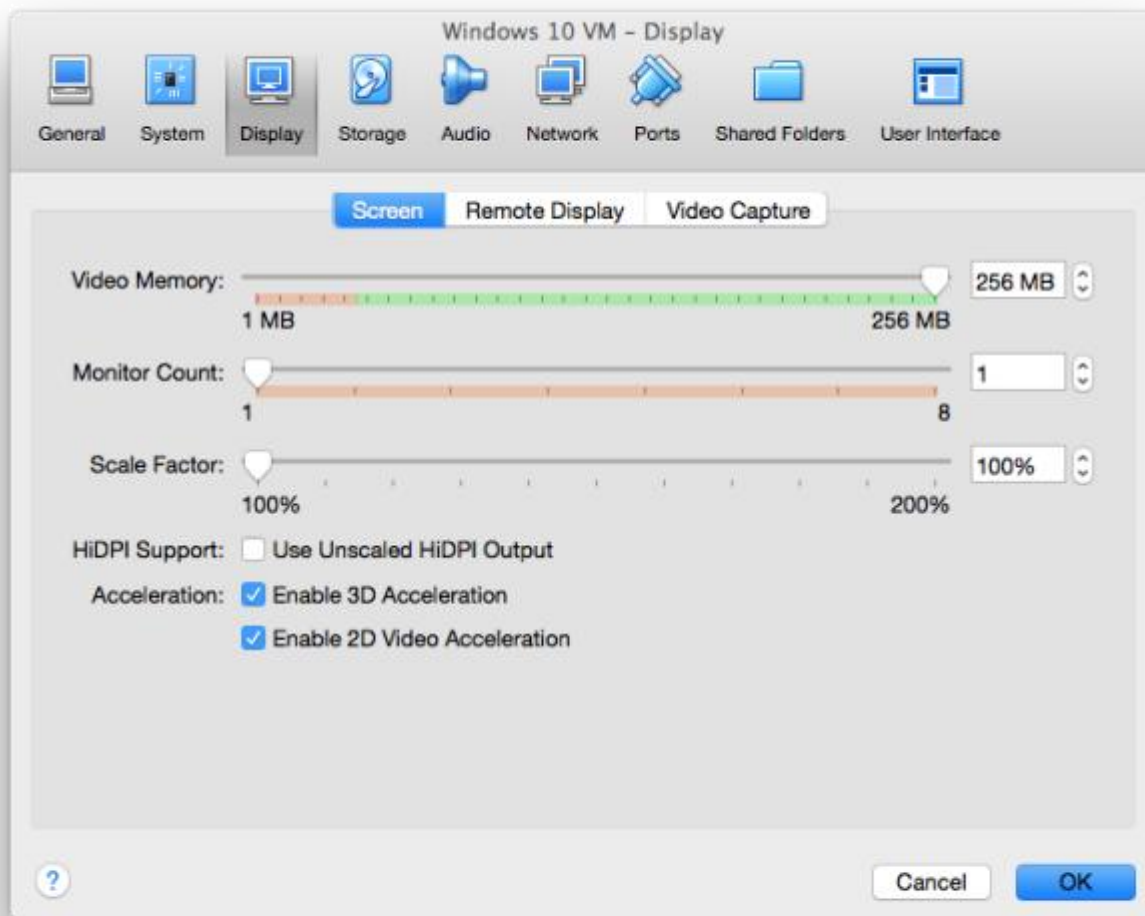
Next, you need to create a virtual drive. Microsoft says that 16GB is the minimum space needed for the 32-bit version, but 20GB is required for the 64-bit version. A 50GB can be a good virtual desktop, but feel free to make it as large as you need. Just be sure you have enough space on your actual hard drive to handle the size of your virtual drive. Depending on what you intend to do with the OS, you may want to allocate more or less storage. Applications installed to a VM should be assumed to require the same amount of "real" storage that their standard installations would.



Credit: Microsoft

5. Locate the Windows 10 ISO

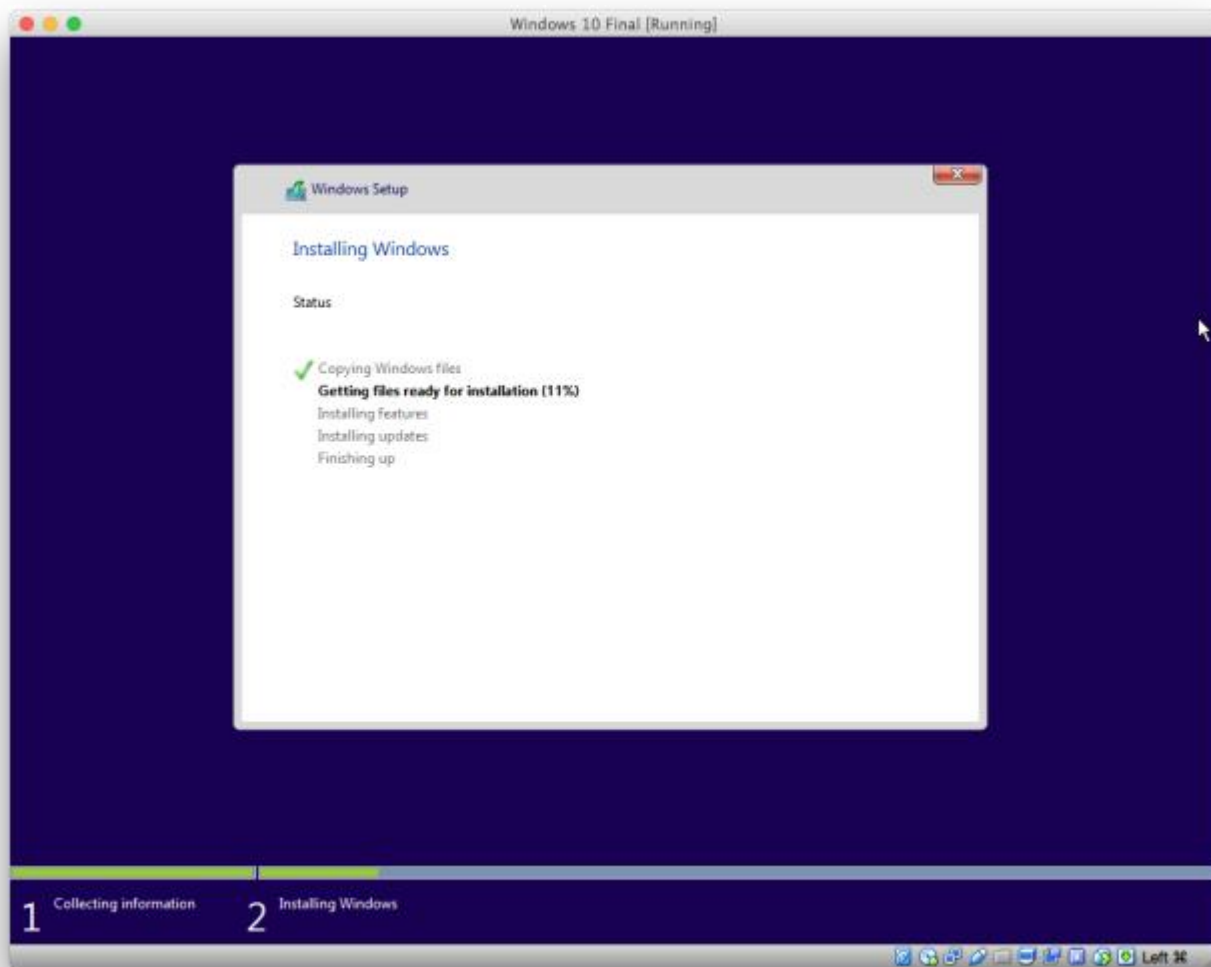
Now, go into the settings for this virtual machine and navigate to the "Storage" tab. Click the disc icon with a green plus next to "Controller: SATA." Click "Choose disk" and locate the Windows 10 ISO you downloaded earlier.



Credit: Microsoft

6. Configure Video Settings

Before you jump in and start installing Windows 10, move over to the "Display" tab. You can configure how much video memory you will allocate to the virtual machine, but stay in the green. You can also toggle on 3D acceleration if you like.



Credit: Microsoft

7. Launch the Installer

After that setup, press the "Start" button in VirtualBox and begin the Windows 10 installation process. Follow the instructions on the screen, and you're well on your way.

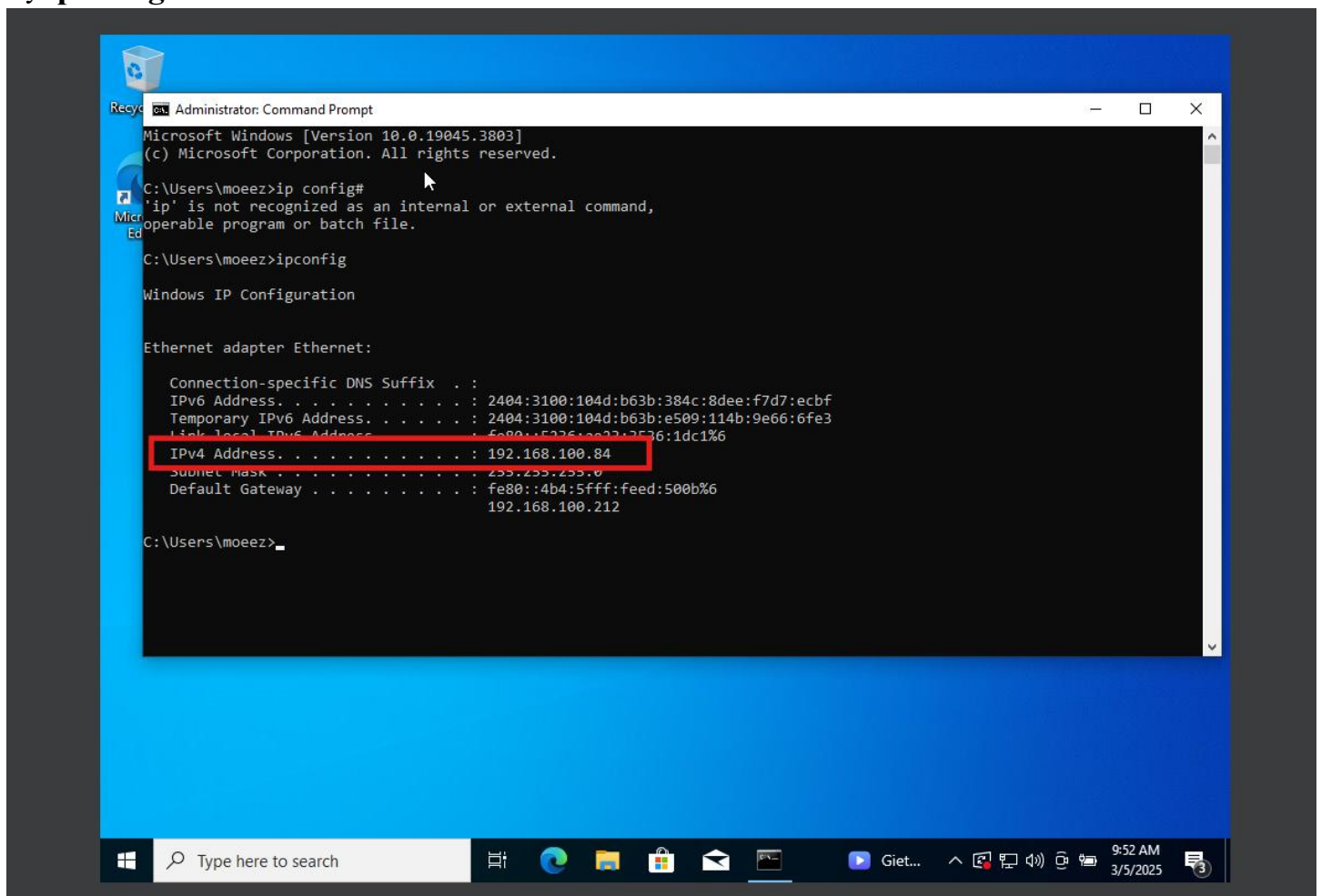
Nmap for Scanning

When you perform a penetration test, the team will provide you a subnet, or a list of IP addresses for scanning. Scanning outside of the allowed list will cause issues such as bringing down production servers, affecting the performance of production servers. Scanning is to help you discover vulnerabilities on each of the scanned servers. You need to consider what arguments you should use for scanning. Even you are provided with the IP list, scanning them all at once may introduce unexpected problems (the router/switch or IPS/IDS cannot bear the load you deliver).

Before attacking any device, you will need to know the detail information of the device. Knowing the OS will help you find what vulnerabilities are available on that OS; knowing opened ports will help you know what services the device is offering.

First See your Ip address in Window ISO file:

By **ipconfig**



1. To find all live hosts in a network, use the below command and **take a screenshot of your findings**. This only uses the **ping** scan to discover the hosts; therefore, it is not too penetrative.

Replace the network with your Kali's network

```
root@UMBkali:~# nmap -sP 192.168.1.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2018-
```

2. If you want to scan the whole network segment and exclude a specific IP address, use the

```
root@UMBkali:~# nmap -sS -PS --exclude 192.168.1.154 192.168.1.1/24
```


following command and **take a screenshot** of your result. Replace the network with your Kali's network, and exclude your Win7 out of the scan

3. When having the result of live hosts, you are taking the next step to find more information. To find the OS version, run the following command with your target IP address, and **take a screenshot** of your findings. Make sure include the scanned time in your screenshot (in seconds)

```
root@UMBkali:~# nmap -sV 192.168.1.152
Starting Nmap 7.70 ( https://nmap.org )
```

4. If you want to set the amount of probes to use, you can use the argument **--version-intensity**. The more probes you use, the higher chance you will be discovered. **Take a screenshot** and note how many seconds **nmap** used to scan this

time? Is it shorter or longer than the previous step?

```
root@UMBkali:~# nmap -sV --version-intensity 2 192.168.1.152
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-23 15:20 EST
```

5. Another way to hide the **nmap** scan from being discovered is using the scan with random data. Packets generated by **nmap** scans usually just have the protocol headers set. To decrease the detection by security tools, **nmap** uses random data as payloads. Execute the following command and **take a screenshot of the result**

```
root@UMBkali:~# nmap -sS -PS --data-length 300 192.168.1.154
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-23 16:22 EST
Nmap scan report for 192.168.1.154
Host is up (0.00089s latency).
```

6. When using **ping** scan, it does not perform port or service scan. Sometimes, the penetration tester knows what port he/she wants to scan for a specific vulnerability. To do that, execute the following command and **take a screenshot** of your result. This is to find if the device is offering direct TCP/IP network access service. This can be used for hacking at a later time.

```
root@UMBkali:~# nmap -p445 192.168.1.154
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-23 15:54 EST
Nmap scan report for 192.168.1.154
Host is up (0.00030s latency).
```

7. If you want to include more than 1 port in the scan, use the following command, and **take a screenshot of your result**

```
root@UMBkali:~# nmap -p445,80,443,139 192.168.1.154
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-23 16:22 EST
Nmap scan report for 192.168.1.154
Host is up (0.00078s latency).
```

8. If you want a wider range, use the following command and **take a screenshot of your result**

```
root@UMBkali:~# nmap -p[1-1024] 192.168.1.154
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-23 16:22 EST
Nmap scan report for 192.168.1.154
Host is up (0.00038s latency).
```

Exercise 2: **nmap** with external vulnerability scanning script and database.

The default configuration of **nmap** provides the capability to check multiple flaws of the server. However, if we want to look further into what vulnerabilities the server is having, we will need to download additional **nse** scripts. The script was written by Marc Ruef to facilitate the vulnerability checking. Follow the below procedure to achieve the task.

1. Copy the **vulscan** folder from your Kali **/opt/vulscan** to the directory **/usr/share/nmap/scripts/vulscan**. If you practice on your own Kali, download the source from **github**:

a.

```
# git clone https://github.com/scipag/vulscan.git
```

- b. Copy the whole folder to the following directory and **take a screenshot of your directory**

```
root@UMBkali:/usr/share/nmap/scripts/vulscan# ls
_config.yml  exploitdb.csv  README.md      securitytracker.csv
COPYING.TXT  openvas.csv   scipvuldb.csv  vulscan.nse
cve.csv      osvdb.csv     securityfocus.csv xforce.csv
```

2. Go to the directory and run the following command. **Take a screenshot of the success**

```
root@UMBkali:/usr/share/nmap/scripts/vulscan# nmap -sV --script=vulscan/vulscan.nse --script-args vulscandb=securitytracker.csv 192.168.1.154 | more
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-25 16:06 EST
```

3. List all the vulnerabilities that you can find as following (the screenshot is one of many found vulnerabilities)

```
|
|_
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
| vulscan: securitytracker.csv:
```

4. This list will help you know what vulnerabilities you can plan for attacks.
5. The last step in this exercise is running the script in the vulnerability category to see what we can attack. Run the following command and **take a screenshot** of your findings (replace the IP address with your Windows 7 IP address)

```
root@UMBkali:/usr/share/nmap/scripts# nmap -sV --script vuln 192.168.1.154
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-25 16:45 EST
Nmap scan report for 192.168.1.154
```

Zenmap exercise

1. Logon to your Kali, go to **Application, Information Gathering**, and select **Zenmap**
2. In the target box, put in your **Win7** IP address, select **Intense Scan** and click **Scan**
3. **Take a screenshot** of all open port the tool found
4. Go to **Host Details**, and **take a screenshot** of the information the tool discovered
5. Go back to the profile box, and select **Slow comprehensive scan**

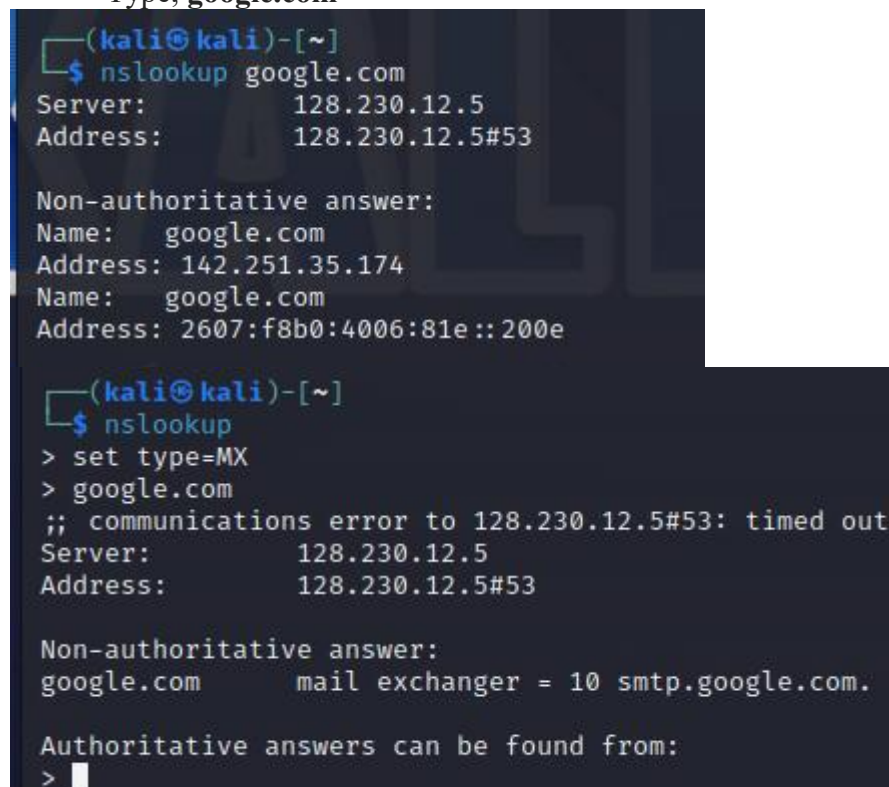
6. What differences can you see between the intense scan and comprehensive scan? The scan will take a few minutes. When it finishes, the high risk ports should be listed in **green**. **Take a screenshot of the green list**
7. Look into the detail and **take a screenshot** of the **smb** version this device uses

Reconnaissance Tools:

1. nslookup:

nslookup is a network administration command-line tool available in many computer operating systems for querying the Domain Name System(DNS) to obtain domain name or IP address mapping, or other DNS records. The name “nslookup” means “name server lookup”.

- In the terminal, type **nslookup <Domain name>**
- Example: **nslookup google.com**
- Then type, **nslookup**
- Type, **set type=MX**
- Type, **google.com**



```
(kali㉿kali)-[~]
$ nslookup google.com
Server:      128.230.12.5
Address:     128.230.12.5#53

Non-authoritative answer:
Name:   google.com
Address: 142.251.35.174
Name:   google.com
Address: 2607:f8b0:4006:81e::200e

(kali㉿kali)-[~]
$ nslookup
> set type=MX
> google.com
;; communications error to 128.230.12.5#53: timed out
Server:      128.230.12.5
Address:     128.230.12.5#53

Non-authoritative answer:
google.com   mail exchanger = 10 smtp.google.com.

Authoritative answers can be found from:
>
```

1. Open Source Intelligence Framework (<https://osintframework.com/>)

Use the OSINT tools to gather information about 3 domains of your choosing not in any of the previous exercises.

2. Sign Up For a Free Account Under Shodan.io

Perform a query to list all public ip addresses that have a Telnet service on port 23.

The screenshot shows the Shodan search interface. At the top, the search bar contains the query "telnet port:23 country:US". Below the search bar, the total number of results is 4,473. The page is divided into several sections: "TOTAL RESULTS", "TOP CITIES", "TOP ORGANIZATIONS", and "TOP PRODUCTS".

TOTAL RESULTS

4,473

TOP CITIES

- New York ... 118
- Richmond 109
- Los Angeles 97
- Houston 76
- Owensboro 76

TOP ORGANIZATIONS

- Charter Co...698
- CenturyLi... 667
- Comcast C...345
- Service Pr... 122
- Verizon Bu... 114

TOP PRODUCTS

- Broadcom ...569
- Microsoft ... 104
- HP JetDirec... 54
- Synchronet ...46
- ZyXEL ZyW... 25

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using [InternetDB](#)

104.244.150.114 2023-07-19T13:49:20.486251

host-104-244-150-114.ustc-online.net Important

ROPIR INDUSTRIES Web username/password is configured to admin/password.

United States, Union Springs Enable and **Telnet** passwords are configured to "password". Please change them immediately.

The ethernet 0/1 interface is enabled with an address of 10.10.10.1

Telnet/SSH access is also enabled. ...

24.229.38.6 2023-07-19T13:41:45.068897

cpe-static-ma-nmicrotel-rtt.cmts.man2.ptd.net

PenTeleData House Account

United States, Mansfield

69.243.15.181 2023-07-19T13:32:05.898156

c-69-243-15-181.hsd1.va.comcast.net

Comcast Cable Communications, Inc

United States, Marlow Heights

Synchronet BBS for Win32 Version 3.19 Copyright 2022 Rob Swinc

Google Hacking Database

What is the Google Hacking Database (GHDB)?

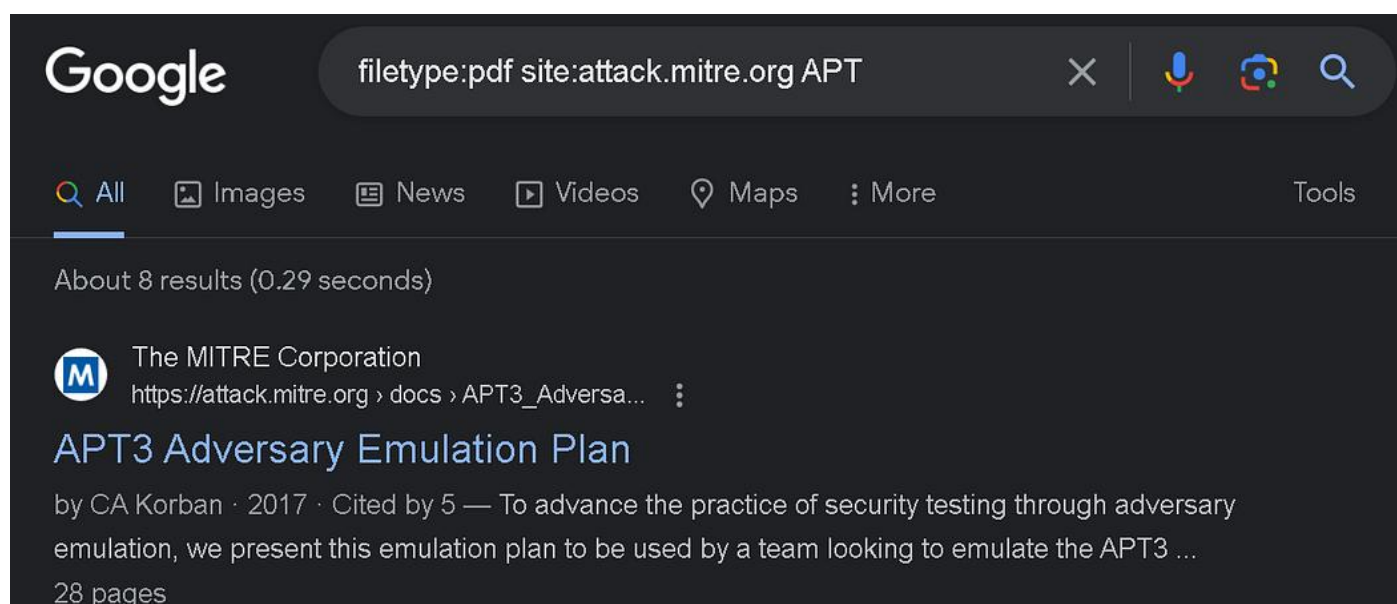
The Google Hacking Database (GHDB), also known as Google Dorks or Google Hacking, is a collection of advanced search queries and techniques to uncover hidden, vulnerable, or sensitive information that may be inadvertently exposed on the web. It is used to discover specific information via Google searches, using specialized search parameters and operators to pinpoint data that is not typically indexed by standard search engines. It is often used by cybersecurity professionals, ethical hackers, and security researchers to identify

security vulnerabilities and raise awareness about the importance of data protection. GHDB serves as a resource for both offensive and defensive purposes in cybersecurity.

How Does Google Hacking Database (GHDB) Work?

Google Hacking Database (GHDB) operates by using specialized search queries, often called “dorks” or “Google dorks.” These dorks are specifically designed to identify vulnerabilities and confidential data that could be accessed on websites, servers, or online platforms. The queries can range from basic searches for specific file types, including PDFs or Excel spreadsheets, to more advanced searches for login pages with default credentials. Here is an example of a simple Google dork query:

filetype:pdf site:attack.mitre.org APT



In this example, the query instructs Google to search for PDF files on the website “attack.mitre.org” that contain the word “APT.”

Another Example:

openSIS 9.1 - SQLi (Authenticated)

<input type="checkbox"/> Verified	<input type="checkbox"/> Has App						Filters	Reset All
Show	15			Search:				
Date	D	A	V	Title	Type	Platform	Author	
2024-11-15	↓	×		SOPanning 1.52.01 (Simple Online Planning Tool) - Remote Code Execution (RCE) (Authenticated)	WebApps	PHP	cybersploit	
2024-10-01	↓	×		reNgine 2.2.0 - Command Injection (Authenticated)	WebApps	Multiple	Caner Tercan	
2024-10-01	↓	×		openSIS 9.1 - SQLi (Authenticated)	WebApps	PHP	Devrim Diragumandan	
2024-10-01	↓	×		dizqueTV 1.5.3 - Remote Code Execution (RCE)	WebApps	JSP	Ahmed Said Saud Al-Busaidi	
2024-08-28	↓	×		NoteMark < 0.13.0 - Stored XSS	WebApps	Multiple	Alessio Romano (sfoffo)	
2024-08-28	↓	×		Gitea 1.22.0 - Stored XSS	WebApps	Multiple	Catalin Iovita, Alexandru Postolache	
2024-08-28	↓	×		Invesalius3 - Remote Code Execution	WebApps	Python	Alessio Romano (sfoffo), Riccardo Degli Esposti (partywave)	

After Clicking on the Link:

openSIS 9.1 - SQLi (Authenticated)

EDB-ID:

52080

CVE:

N/A

EDB Verified:

×

Author:

DEVTRIM DIRAGUMANDAN

Type:

WEBAPPS

Exploit:

↓ / {}

Platform

:

PHP

Date:

2024-10-01

Vulnerable App:

←

→

we get the data about the exploitation.

After executing this query, it will provide you with detailed information about threat groups associated with Advanced Persistent Threats (APTs).

Importance of Google Hacking Database (GHDB)

Below are some vital points highlighting the significance of the Google Hacking Database (GHDB):

1. **Security Auditing:** Valuable tool for security professionals to discover vulnerabilities and weaknesses in web applications and websites
2. **Reconnaissance:** Crucial for security professionals to perform reconnaissance and footprinting activities to understand an organization's online presence and identify potential security vulnerabilities
3. **Penetration Testing:** Valuable tool for ethical hackers to evaluate the security posture of systems and help organizations strengthen their defenses
4. **Education and Awareness:** Raises awareness about the importance of data protection and the potential consequences of failing to secure sensitive information
5. **Vulnerability Discovery:** Assists in identifying and resolving security vulnerabilities, which can help prevent data breaches and cyberattacks
6. **Data Protection:** Highlights the importance of securing data and encourages organizations and individuals to take data protection seriously
7. **Mitigating Risks:** Helps reduce the risk of data breaches and associated legal, financial, and reputational damage by proactively detecting and resolving vulnerabilities
8. **Incident Response:** Security teams can use GHDB to search for leaked or exposed data to mitigate risks proactively
9. **Resource for Researchers:** Valuable resource for researchers and academics delving into the realm of cybersecurity and information security practices
10. **Compliance and Regulation:** Assist organizations in adhering to data protection regulations and compliance standards by identifying potential areas of data security vulnerability

How can InfosecTrain Help?

If you want to learn more about the Google Hacking Database (GHDB) and how it relates to cybersecurity, enrolling in InfosecTrain's CEH v12 Training and CompTIA Security+ training courses can be an excellent choice. These courses provide comprehensive education on various aspects of cybersecurity, including understanding tools like GHDB and practical skills. CEH, for instance, focuses on ethical hacking techniques and methodologies, while CompTIA Security+ covers a wide range of cybersecurity concepts and practices. Both can help you acquire a deeper understanding of GHDB and how to use it responsibly in the context of cybersecurity.

Task 1: Nmap Scanning

Live Host Discovery:

1. Use **Nmap** to find all live hosts on the network.
2. Take a screenshot of the results.

OS and Port Scanning:

1. Identify the **operating system** and **open ports** of a specific target.
2. Include the scanned time in your screenshot.

Evasion Techniques:

1. Use --version-intensity to control probe levels.
2. Run a scan using **random data payloads** to avoid detection.
3. Compare the scan time with previous scans.

Multi-Port Scanning:

1. Scan for multiple ports and a **wider range of ports** on the target system.
2. Take screenshots of your findings.

Task 2: Vulnerability Assessment using Nmap Scripts

Vulnerability Scanning:

1. Copy the vulscan script to the Nmap directory.
2. Run an **Nmap vulnerability scan** on a target system.
3. List all vulnerabilities found.

Exploitable Services:

1. Identify **high-risk services and ports**.
2. Take a screenshot of the service details.

Task 3: Reconnaissance using OSINT Tools

NSLookup Usage:

1. Use nslookup to find the **IP address** of a given domain.
2. Check **mail server records (MX records)** for the domain.

OSINT Data Collection:

1. Use **OSINT Framework (osintframework.com)** to collect intelligence on **three different domains**.
2. List the key details found.

Shodan Search:

1. Sign up on **Shodan.io** and perform a search to list all **public IP addresses running Telnet on port 23**.
2. Submit a screenshot of your query and findings.

Task 4: Google Hacking Database (GHDB)

Using Google Dorks:

1. Use **Google dork queries** to find sensitive files (e.g., PDFs, login pages, or exposed databases).
2. Submit **three different queries** and explain their results.

Identify Potential Vulnerabilities:

1. Run a GHDB query related to **SQL Injection** or **exposed credentials**.
2. Describe what kind of data you found.

Submission Guidelines

- Submit a **document (PDF or Word)** containing:
 - Screenshots of all scans and queries.
 - A brief explanation of findings for each task.
- Ensure all scans are conducted in a **controlled environment** (e.g., your own virtual machines).
- Unauthorized scanning of external networks is **not allowed**.