Ethical Hacking & Penetration Testing

Assignment 1:

Objective: Use whois to gather information about a domain name of your choice. Perform a nslookup query on the same domain to obtain its IP address and DNS information.

What is WHOIS

- Purpose: WHOIS is a protocol and public database used to look up registration information for domain names and IP addresses.
- What it reveals: Domain registrant (name and contact details) when not redacted, registrar, registration and expiration dates, nameservers, and status. It can also indicate privacy protections or proxy services in use.
- How it's used in practice: You query a domain to confirm ownership details, see who manages the domain, and identify the authoritative name servers. It's commonly used for domain management, ownership verification, and basic reconnaissance in an approved lab setting.

I selected tryhackme.com website to get the information from WHOIS.

Here is the gathered information about tryhackme.com with the help of WHOIS.

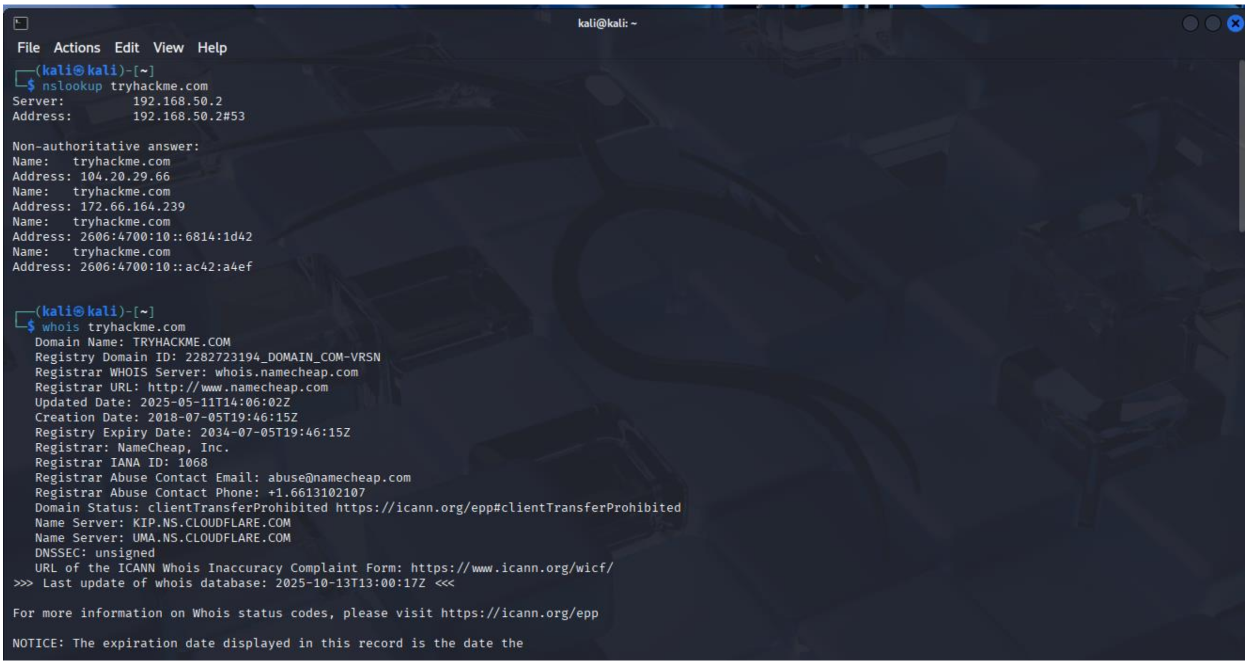
```
root@SunilVijay:~# whois tryhackme.com

  Domain Name: TRYHACKME.COM

  Registry Domain ID: 2282723194_DOMAIN_COM-VRSN

  Registrar WHOIS Server: whois.namecheap.com

  Registrar URL: http://www.namecheap.com

  Updated Date: 2025-05-11T14:06:02Z

  Creation Date: 2018-07-05T19:46:15Z

  Registry Expiry Date: 2034-07-05T19:46:15Z

  Registrar: NameCheap, Inc.

  Registrar IANA ID: 1068

  Registrar Abuse Contact Email: abuse@namecheap.com

  Registrar Abuse Contact Phone: +1.6613102107

  Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

  Name Server: KIP.NS.CLOUDFLARE.COM

  Name Server: UMA.NS.CLOUDFLARE.COM

  DNSSEC: unsigned

  URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/

>>> Last update of whois database: 2025-10-13T12:50:00Z <<<
```

What is nslookup

- Purpose: nslookup is a DNS query tool used to obtain information about DNS records for a domain.
- What it can fetch:
    - A records (IPv4 address)
    - AAAA records (IPv6 address)
    - NS records (name servers)
    - CNAME, MX, and other DNS records depending on options
- How it's used in practice: It helps verify the domain's DNS configuration, resolve domain names to IPs, and understand the domain's hosting setup. It is often used in labs to study how DNS responds to queries and to confirm network reachability.

Here is the result in nslookup

```
nslookup tryhackme.com

Server:         192.168.50.2

Address:        192.168.50.2#53



Non-authoritative answer:

Name:   tryhackme.com

Address: 104.20.29.66

Name:   tryhackme.com

Address: 172.66.164.239

Name:   tryhackme.com

Address: 2606:4700:10::6814:1d42

Name:   tryhackme.com

Address: 2606:4700:10::ac42:a4ef
```



```
┌──(kali㉿kali)-[~]
└─$ nslookup tryhackme.com
Server:         192.168.50.2
Address:        192.168.50.2#53

Non-authoritative answer:
Name:   tryhackme.com
Address: 104.20.29.66
Name:   tryhackme.com
Address: 172.66.164.239
Name:   tryhackme.com
Address: 2606:4700:10::6814:1d42
Name:   tryhackme.com
Address: 2606:4700:10::ac42:a4ef


┌──(kali㉿kali)-[~]
└─$ whois tryhackme.com
   Domain Name: TRYHACKME.COM
   Registry Domain ID: 2282723194_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.namecheap.com
   Registrar URL: http://www.namecheap.com
   Updated Date: 2025-05-11T14:06:02Z
   Creation Date: 2018-07-05T19:46:15Z
   Registry Expiry Date: 2034-07-05T19:46:15Z
   Registrar: NameCheap, Inc.
   Registrar IANA ID: 1068
   Registrar Abuse Contact Email: abuse@namecheap.com
   Registrar Abuse Contact Phone: +1.6613102107
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: KIP.NS.CLOUDFLARE.COM
   Name Server: UMA.NS.CLOUDFLARE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-10-13T13:00:17Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
```

Key differences

- Focus: WHOIS provides registration and ownership data; nslookup provides DNS resolution data (how the domain name maps to IPs and where those records are served from).
- Data exposure: WHOIS data can be restricted or redacted by privacy protections; DNS records (visible via nslookup) are typically publicly accessible.
- Use cases: WHOIS for ownership, contact, and registration details; nslookup for diagnosing DNS resolution, connectivity, and hosting configurations.

Assignment 2

I used a file in github, where I can't find any vulnerable windows xp machine.

I tried to get vm image file of windows xp vulnerable machine. But I couldn't make it.

But below is the process of same thing that how we need to perform a exploit in windows xp.

Question: Use the Metasploit Framework to exploit a known vulnerability on a virtual machine (such as the MS08-067 vulnerability in Windows XP). Document the exploitation steps.

Penetration Testing - MS08-067 Exploit

Overview:

In this project, I performed a full penetration testing workflow targeting a vulnerable Windows XP system on a simulated internal network. After discovering the machine through Nmap scanning, I identified an exploitable vulnerability (MS08-067) using Nessus, then leveraged Metasploit to gain remote code execution and extract key files from the system.

Tools & Technologies:

- **Nmap** - Network Scanning and OS detection
- **OpenVAS** - Vulnerability Assessment
- **Metasploit** - Exploitation and post-exploitation
- **Kali Linux** - Attacker machine
- **Windows XP SP3** - Target machine

Objective / Scenario:

The goal was to simulate a real-world penetration test by identifying a vulnerable system, performing reconnaissance and enumeration, scanning for vulnerabilities, exploiting one, and retrieving proof of access by retreiving specified flags in the system.

Target IP: 11.11.0.13 **Operating System:** Windows XP SP3

Methodology

1. Network Scanning with Nmap

I followed a standard netwrok scanning procedure using Nmap on a Kali Linux virtual machine. Commands are listed below:

```
Nmap -sS -O -v 11.11.0.1/24
```

I combed through the list that was returned until I found the IP that was associated with the target WIndows XP machine. Below is the full report for the Windows XP system, including the ports and statuses.

Nmap scan report for 11.11.0.13

Port	State	Service	Version
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows Netbios-ssn
445/tcp	open	Microsoft ds	Microsoft Windows XP Microsoft ds
3389/tcp	open	ms-wbt-server	Microsoft Terminal Services

Microsoft Windows XP SP3

2. Vulnerability Scanning with Nessus

Once I identified the system I wanted to exploit, I used Nessus to scan for vulnerabilities. There were 25 vulnerabilites on 11.11.0.13. I selected exploit: MS08-067 - Windows Server Service Crafted RPC Request Handling Remote Code. This vulnerability allows remote code execution by sending a specially crafted RPC request to the svchost.exe process on vulnerable Windows systems.

3. Exploitation with Metasploit

I started Metasploit and used the code below to begin the exploitation attempt:

```
use exploit/windows/smb/ms08_067_netapi
```

I specified the target IP I wanted to exploit:

```
set RHOST 11.11.0.13
```

then used the **Exploit** command to begin.

4. Post-Exploitation: File Retrieval

I navigated the file system using the shell commands listed below:

```
cd "Documents and Settings"
```

```
cd Administrator/Desktop
```

```
ls
```

Listed were three files:

flag0.txt

fruit.jpg

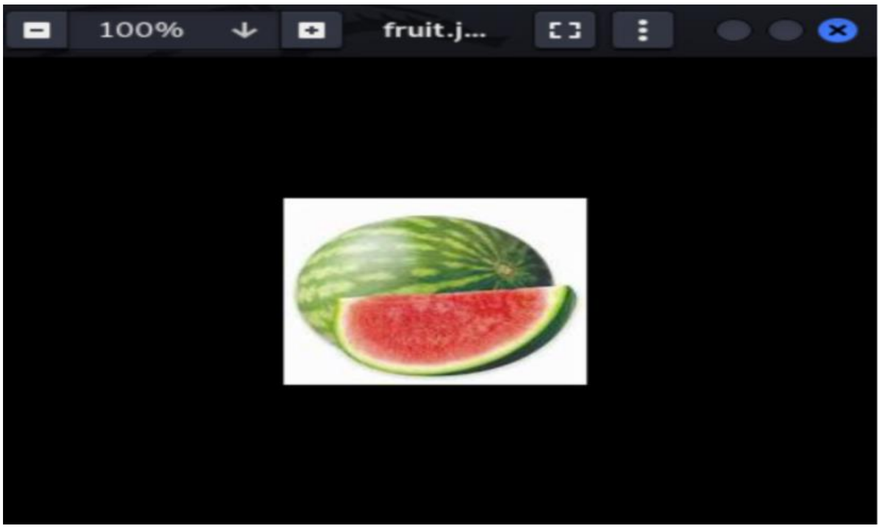
README.txt

I accessed all three using the cat command. The contents of the files will be listed below:

Flag0.txt: Gabaski

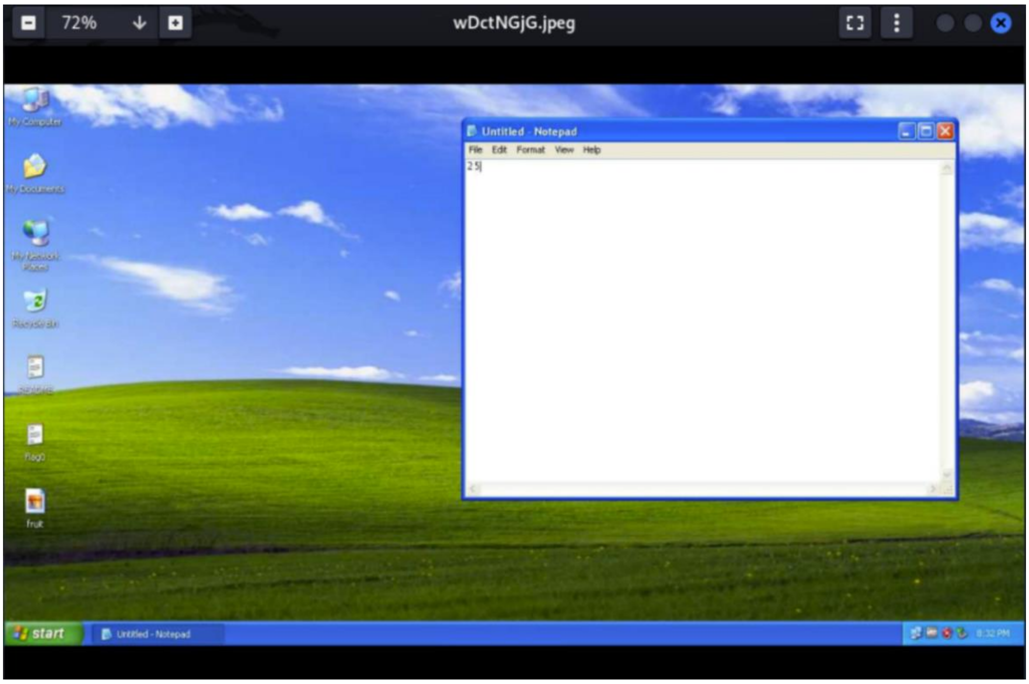
README.txt: Do not delete or add anything in this machine. Do not patch any vulnerabilites. Other people are using this machine for their project.

fruit.jpg:



I used the download command on the fruit photo and I used the screenshot command to take a screenshot of the

Administrator's desktop which is shown below:



```
25
```