Ethical Hacking

Meryem Jourhbiri
Raha Bahramizadeh

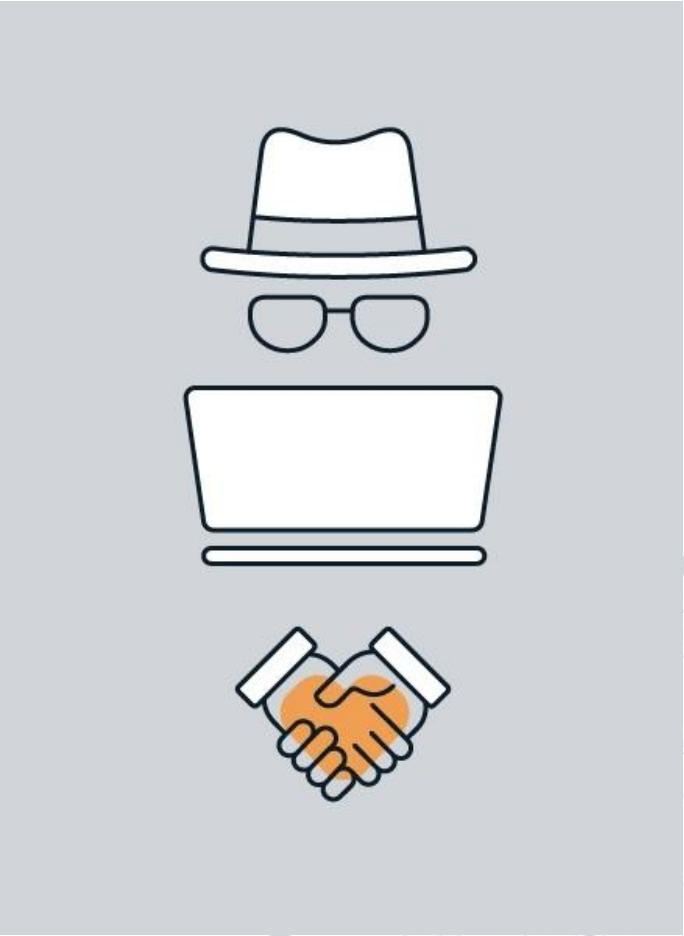
31.01.2025

Agenda

1. **Introduction**
2. **Case Studies: Why Ethical Hacking is Critical**
3. **The Ethical Hacking Process**
   3.1. Reconnaissance
   3.2. Scanning
   3.3. Gaining Access
   3.4. Maintaining Access
   3.5. Clearing Evidence
   3.6. Final Report
4. **Resources**

1. Introduction

- Definition
  - Ethical hacking is the use of **hacking techniques** by friendly parties in an attempt to **uncover**, **understand**, and **fix** security vulnerabilities in a network or computer system.



Ethical Hacking vs. Malicious Hacking

Find and fix vulnerabilities	Purpose	Exploit vulnerabilities for personal gain
Authorized and Legal	Legality	Unauthorized and Illegal
Improve cybersecurity posture	Impact	Breaches and Disruptions

2.

Case Studies: Why Ethical Hacking is Critical

The Equifax Data Breach (2017)	
Impact	More than **147 million** people
Cost	More than **$1.7 billion**

Source: Cobalt

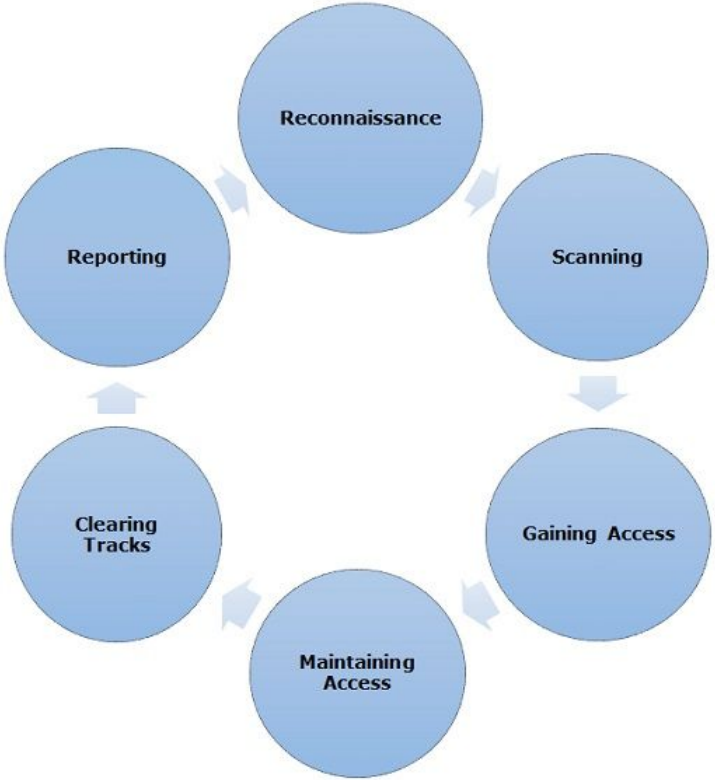
Playstation Network Hack (2011)	
Impact	**77 million** devices
Cost	**$171 million**

Source: pentestpeople

3.

The Ethical Hacking Process

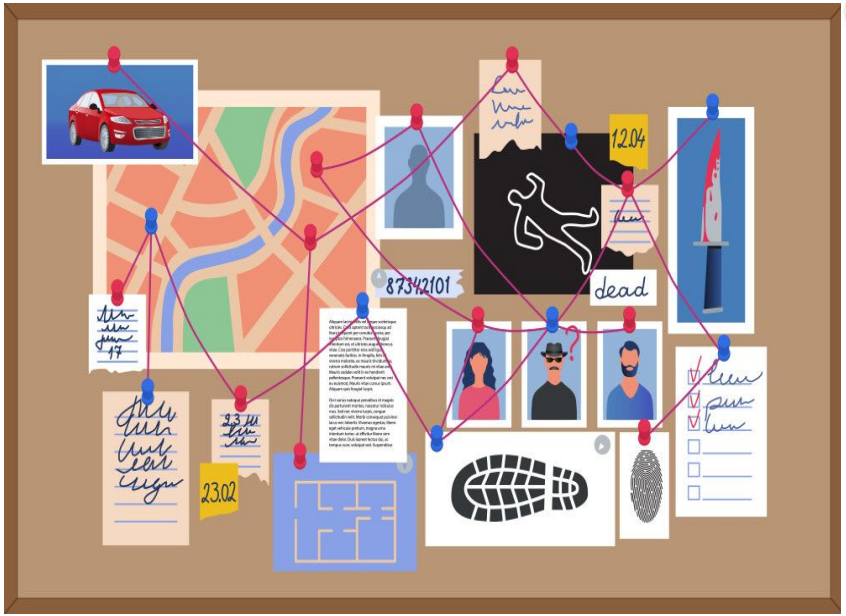
The Ethical hacking cycle process



Step 1.

Reconnaissance: Information Gathering

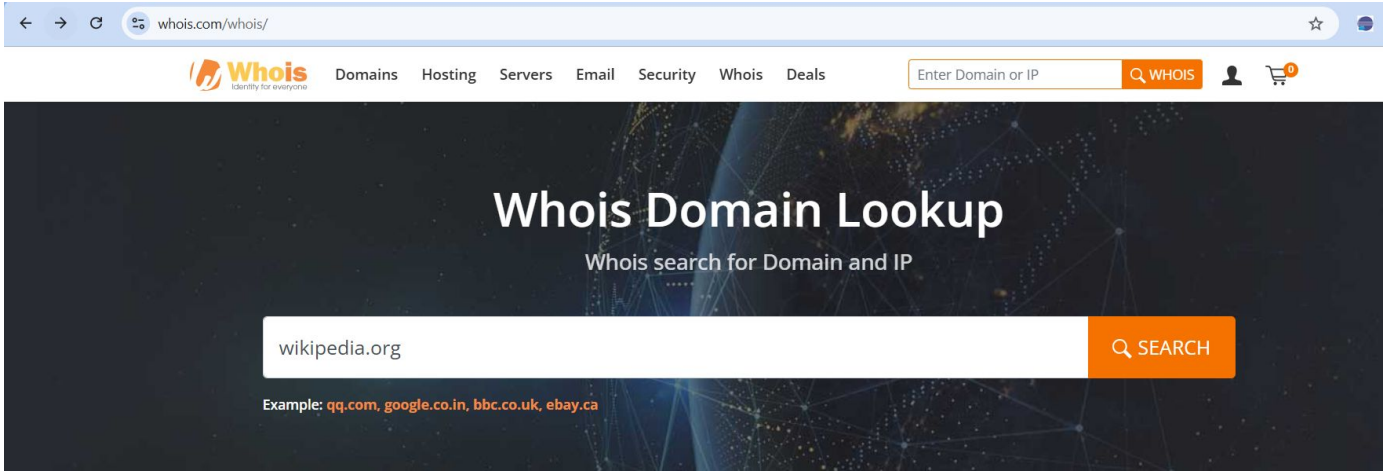
What are the Sources of Information?



- Websites
- WHOIS Databases
- Job Advertisements
- Public Manuals and Brochures

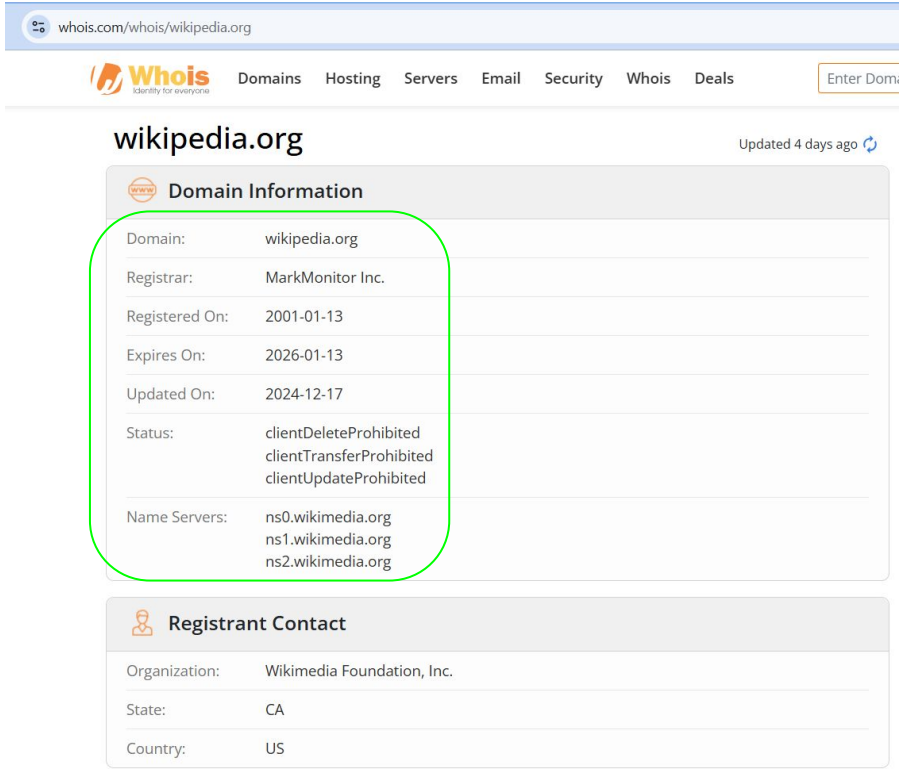
How to work with Whois database

Easily enter the IP address or the Domain name



WHOIS works only for public domains. If a domain has privacy protection, you won't see personal information.

Formatted Output of WHOIS data



Step 2.

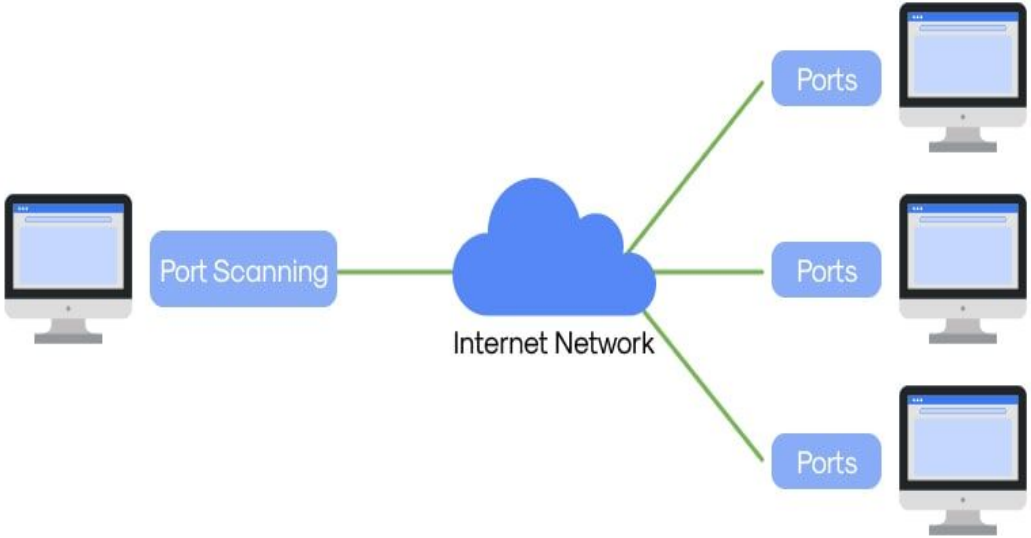
Scanning:
Identifying Weak Points

Step 2: Scanning - Identifying Weak Points

Scanning

1. Port Scanning
2. Operating System Scanning
3. Vulnerabilities Scanning

What does port scanning does?



The goal of port scanning?

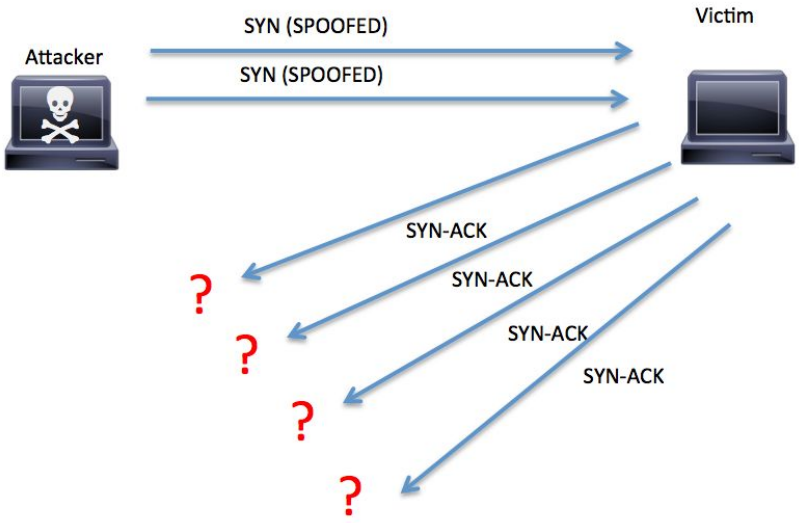
1. What ports are open and what services are running on them

How to achieve this goal?

2. By sending network packets to the target

3. The target response get observed to determine the state of the port

Nmap approach: Popular tool for doing port scan



If it gets SYN-ACK, the port is **open.**

If it gets RST, the port is **closed.**

If there's no response or an error, the port is **filtered.**

Nmap: Overview of the Output of port scanning.

```
root@Kali2:~# nmap 192.168.68.12

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-12-15
mass_dns: warning: Unable to determine any DNS servers. Rev
 Try using --system-dns or specify valid servers with --dns
Nmap scan report for 192.168.68.12
Host is up (0.0043s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
143/tcp  open  imap
443/tcp  open  https
445/tcp  open  microsoft-ds
5001/tcp open  commplex-link
8080/tcp open  http-proxy
8081/tcp open  blackice-icecap

Nmap done: 1 IP address (1 host up) scanned in 1.20 seconds
```

Figure Source [Ethical Hacking: Research and Course Compilation]

Explanation of some of the response from Nmap output

1. **22/tcp open ssh**

   How an Attacker Could Exploit It:

   Dictionary Attack

   Poor credentials : Guessing the username & Password

2. **80/tcp open http**

   How an Attacker Could Exploit It:

   SQL Injection

   Unsecured File Uploads: send malicious database queries to steal or manipulate data via web application forms.

Step 2: Scanning - Identifying Weak Points

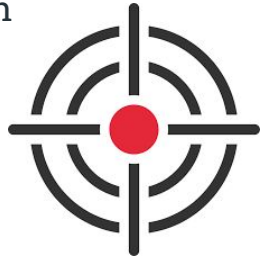
Scanning

1. Port Scanning
2. Operating System Scanning
3. Vulnerabilities Scanning

Scanning operating system: Nmap

1. Nmap sends a crafted network packet with TTL value (Time-to-live)

2. The target system responds



3. Nmap analyzes:
   1. TTL in the response
   2. Windows Size

Nmap compare windows size with its OS Fingerprint DB.

Output of nmap OS scanning

```
# nmap -A -T4 scanme.nmap.org

Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.029s latency).
rDNS record for 74.207.244.221: li86-221.members.linode.com
```

This helps narrow down potential vulnerabilities specific to that OS.

```
646/tcp  filtered ldp
1720/tcp filtered H.323/Q.931
9929/tcp open     nping-echo  Nping echo
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.39
OS details: Linux 2.6.39
Network Distance: 11 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel
```

specific OS type and version.

Figure source: [Chapter 15. Nmap Reference Guide | Nmap Network Scanning]

Step 2: Scanning - Identifying Weak Points

Scanning

- Port Scanning
- System Scanning (Operating System Scanning)
- Vulnerabilities Scanning

Nmap Vulnerability Scan:
nmap --script vuln target_ip

Step 3.

Gaining Access

Approaches to gain access

Breaking Authentication Barriers

Guessing the passwords

How to gain access via cracking the Password?

How do you think your password really gets stored?

123456 Or 6w3fH3...$abcdef123456

Hash value: Digital value of the Password

But why passwords are stored as hash value?

One way encryption that cannot be reversed to be guessed

What is the hackers strategy to guess the password?

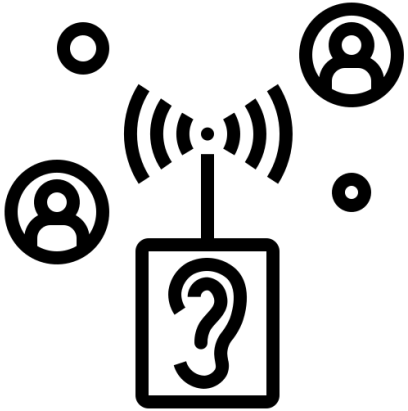
Obtain the hashed passwords	Use password guessing techniques
Hacker accesses a file named hash.txt	By guessing the correct password and calculating the hash value of it using the same hash algorithm

Bingo! Password is cracked

TO SPEED UP THE PROCESS SOFTWARES SUCH AS JOHN THE RIPPER CAN BE USED. JOHN THE RIPPER HAS ACCESS TO wordlist.txt

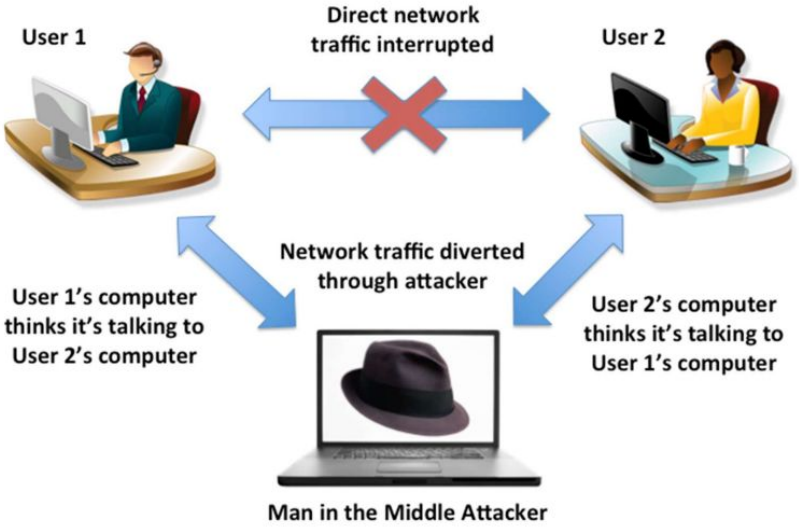
Approaches to gain access

Intercepting Communications



Intercepting Communications: The MITM Technique

1. Set up a malicious Wifi network
2. Victim connects to this Wifi
3. Attacker can monitor traffic and manipulate data



Step 4.

Maintaining Access

Backdoor

- **What is it?**
  - Allows bypassing authentication to maintain access to a system.
- **Purpose**
  - Simulates how attackers might persist in a system post-exploitation.
- **Types**
  - Standalone programs or integrated into existing software

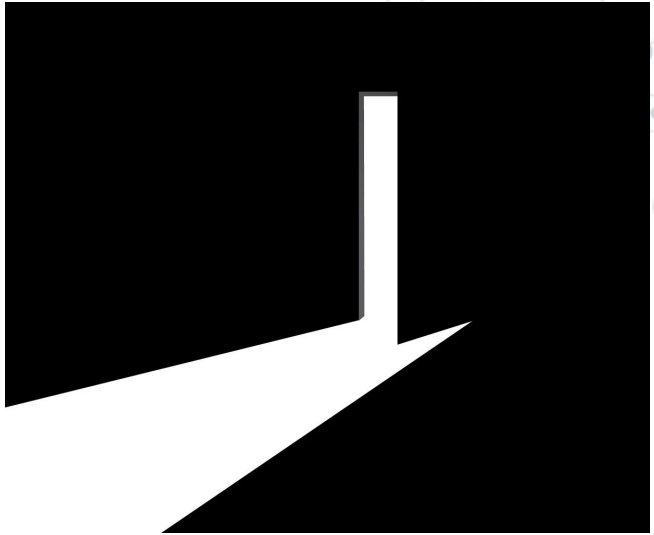
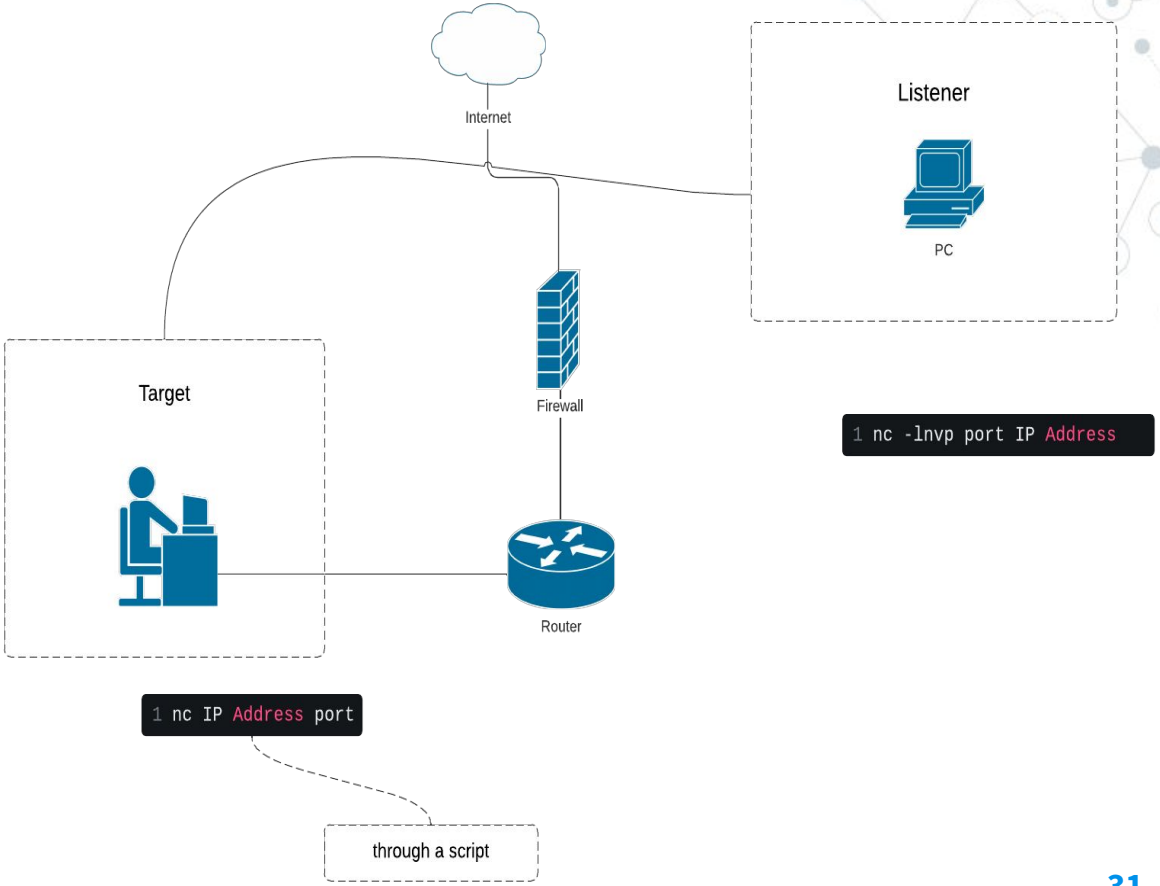


Figure: Back door

Reverse Shell using NetCat

- **NetCat: The Swiss Army Knife**
  - Flexible tool for communication and network traffic.
  - Connects any local port to any target port.



```
root@localhost:~# root@localhost:~#
root@localhost:~#
root@localhost:~#
root@localhost:~#
root@localhost:~#
root@localhost:~#
root@localhost:~#
root@localhost:~# nc -lvnp 87 -s 69.164.204.158
Listening on [69.164.204.158] (family 0, port 87)
Connection from [redacted] received!
```

Figure: Terminal image

Step 5.

Cover tracks

Simulated Techniques

Techniques

Log File Manipulation

Test whether critical logs can be tampered with or deleted **without triggering alerts**

Timestomping

Test if attackers can **modify timestamps** on files to hide evidence of their activity

Clearing Command History

Simulating an attacker's attempt to **remove traces** of commands used during exploitation

Why?

- Evaluate the effectiveness of logging and monitoring systems.
- Test the organisation's incident response capabilities
- Provide insights on improving detection mechanisms

Step 6.

Reporting

The Report

- The principal reflection of an Ethical Hacker competence
- What should it include:
  - **Summary**: The highlights of the testing
  - **Report**
  - **Raw output** (when requested)

6. Resources

- Patrick Engebretson, The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy , 2nd ed. Elsevier, 2013.
- https://nmap.org/book/man.html
- https://www.theseus.fi/bitstream/handle/10024/119594/Matero_Ida.pdf
- OS Detection | Nmap Network Scanning
- https://www.diva-portal.org/smash/get/diva2:1517798/FULLTEXT01.pdf
- https://www.pentestpeople.com/blog-posts/the-top-5-most-dangerous-cyber-attacks-of-all-time
- https://www.cobalt.io/blog/biggest-cybersecurity-attacks-in-history

Thanks!

Any questions?