ZROC102

zumaroc

Module 1: Introduction

BEING A HACKER

What is Hacking?

Hacking is the activity of identifying weaknesses in a computer system or a network to exploit the security and to gain access to personal data or business data. An example of computer hacking I.e. Using a password cracking algorithm to gain access to a computer system.

Who is a Hacker?

A **hacker** is a person who uses computer programming or technical skills to overcome a challenge or problem.

There are good hackers, bad hackers and hackers who fall in-between.

BEING A HACKER (CONTD.)

We have White Hat, **Black** Hat & Gray Hat hackers

- **White Hat Hacker (Ethical Hacker):**

A security hacker who gains access to systems with a view to fix the identified weaknesses. No malicious intent.

- **Black Hat Hacker (Cracker):**

A hacker who gains unauthorized access to computer systems for personal gain. The intent is usually to steal corporate data, violate privacy rights, transfer funds from bank accounts etc.

- **Grey Hat Hacker:**

A hacker who both a white and black hat hacker. He/she breaks into computer systems without authority with a view to identify weaknesses and reveal them to the system owner.

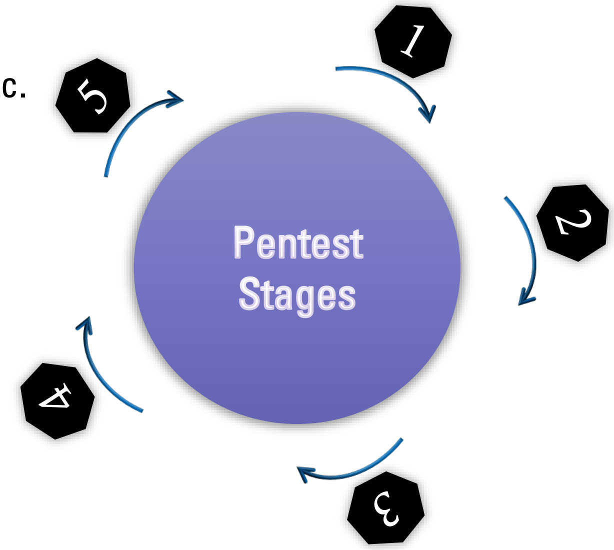
ABOUT PENETRATION TESTING

A penetration test is an ongoing cycle of research and attack against a target or boundary.

The attack should be structured, calculated, and when possible, verified in a lab before being implemented on a live target.

❖ **Penetration Steps:**

- ✓ [1] Information Gathering e.g., DNSrecon, DNSenum, Whois, nslookup etc.
- ✓ [2] Service Enumeration e.g., Nmap, Google dorking etc.
- ✓ [3] Exploitation
- ✓ [4] Maintaining Access
- ✓ [5] Reporting & Recommendations



NOTE TAKING

Information is key, so taking and keeping organized notes is vital. We recommend that you document everything to start with. This includes all the console output, as well as screenshots of key events.

“It’s better to have too much than to repeat material in order to fill in gaps”.

Developing good documentation skills will also allow you to quickly find that long command that you used to exploit a given machine several days before, should you ever need to re-exploit it, or cross-reference users during post-exploitation after having successfully compromised each target machine.

A good documentation process will save you considerable time and a few headaches as well.

EFFECTIVE NOTE TAKING/REPORTING

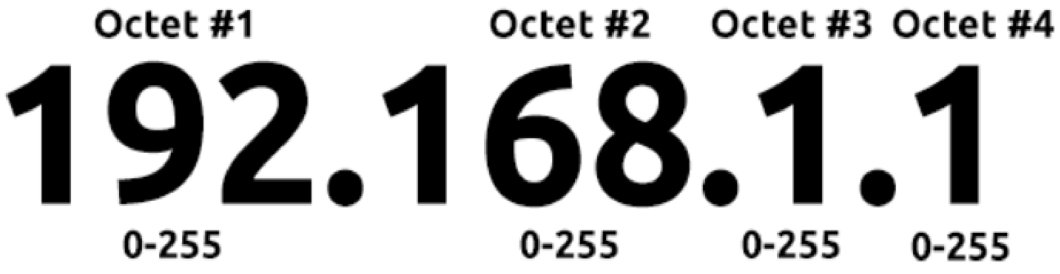
Reporting is often viewed as a necessary evil of penetration testing.

Guidelines:

- ❖ **Consider the Objectives:**
  - ✓ What did you set out to accomplish
  - ✓ Is there a single, specific statement you hope to make in the report?
- ❖ **Consider the Audience:**
  - ✓ Executive summary for high level less technical executives.
  - ✓ More technical part of report for other IT professionals on the team.
- ❖ **Consider What to Include:**
  - ✓ Only include relevant and meaningful content.
  - ✓ Reports do not have to be extremely long.
- ❖ **Consider the Presentation:**
  - ✓ Write coherent sentences that flow smoothly, logically and spellcheck x5

IP ADDRESS

An IP address is a unique address that identifies a device on the internet or a local network.



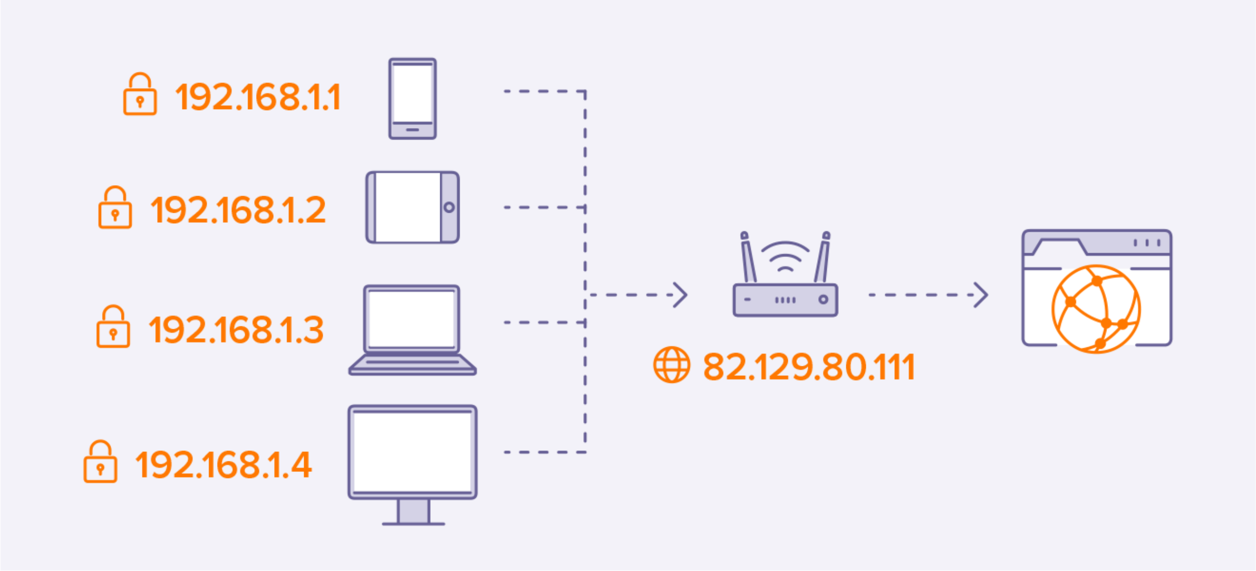
An **IP** address is a set of numbers that are divided into four octets. The value of each octet will summarize to be the IP address of the device on the network.

PUBLIC & PRIVATE IP ADDRESS

The main difference between public and private IP addresses is how far they reach, and what they're connected to.

A **public IP address** identifies you to the wider internet so that all the information you're searching for can find you.

A **private IP address** is used within a private network to connect securely to other devices within that same network.



PUBLIC & PRIVATE IP ADDRESS CONTD.

Your private IP address exists in **the specific** private IP address range reserved by the Internet Assigned Numbers Authority (IANA) and should **not** appear on the **Internet.**

There are millions of private networks across the globe, all of which include devices assigned private IP addresses within these ranges:

❑ **Class A:** 10.0.0.0 — 10.255.255.255

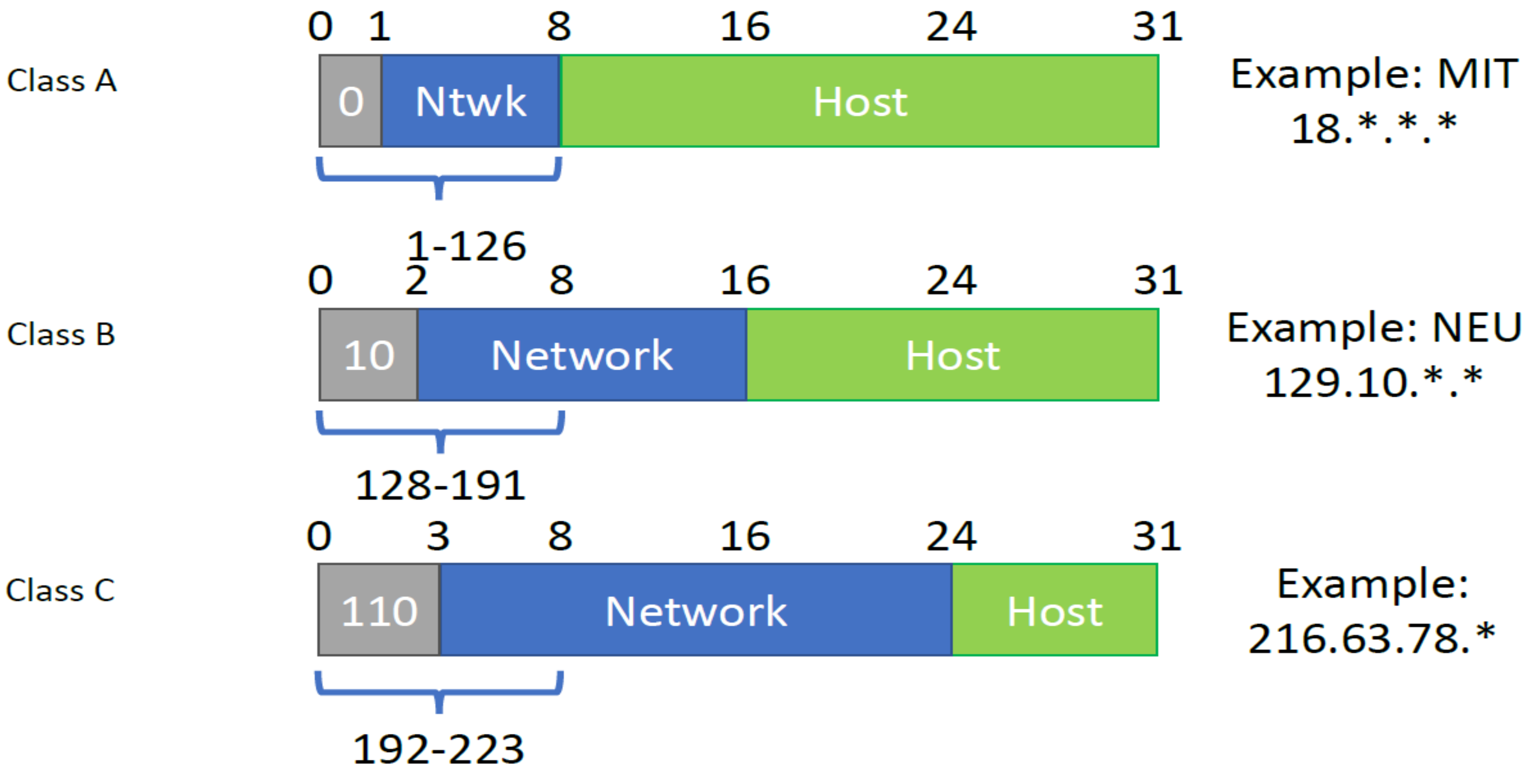
❑ **Class B:** 172.16.0.0 — 172.31.255.255

❑ **Class C:** 192.168.0.0 — 192.168.255.255

The **public** IP address range encompasses every number not reserved for the private IP range. Since a public IP address is a unique identifier for each device connected to the internet, it needs to be unique.

As more and more devices become connected, it is becoming increasingly harder to get a public address that isn't already in use. For example, Cisco, an industry giant in the world of networking, estimated that there would be approximately 50 billion devices connected on the Internet by the end of 2021. (Cisco., 2021). Enter IP address versions. So far, we have only discussed one version of the Internet Protocol addressing scheme known as IPv4, which uses a numbering system of 2^32 IP addresses (4.29 billion) -- so you can see why there is such a shortage!

CLASSES OF IP ADDRESS



Class D is for multicast networking and the **Class E** address range **is reserved for future or experimental purposes**.

IPV6

IPv6 is a new iteration of the Internet Protocol addressing scheme to help tackle this issue. Although it is seemingly more daunting, it boasts a few benefits:

- ❖ It supports up to **2^128** of IP addresses (340 trillion-plus), resolving the issues faced with IPv4.
- ❖ More efficient due to new methodologies

❖ **Address Format:**

- ✓ 8 groups of 16-bit values, separated by ‘**:**’
- ✓ Leading zeroes in each group may be omitted
- ✓ Groups of zeroes can be omitted using ‘**::**’
  - 2001:0db8:0000:0000:0000:ff00:0042:8329
  - 2001:0db8:0:0:0:ff00:42:8329
  - 2001:0db8::ff00:42:8329

LOCALHOST ADDRESS

Localhost is a **top-level domain** reserved for **documentation and testing purposes**. If you access "http://localhost" in the browser, the request will not be forwarded to the internet through the router but will instead remain in your own system. **Localhost** has the IP address 127.0.0.1, which refers to your own server.

What is localhost in IPv4?

127.0.0.1

What is localhost in IPv6?

::1

MAC ADDRESS

A MAC address, or Media Access Control address, is a 48-or 64-bit address associated with a network adapter. While IP addresses are associated with software, MAC addresses are linked to the hardware of network adapters. It is sometimes called the hardware address, the burned-in address (BIA), or the physical address.

They are expressed in hexadecimal notation in the following format:

- ❑ 01-23-45-67-89-AB, in the case of a 48-bit address.
- ❑ 01-23-45-67-89-AB-CD-EF, in the case of a 64-bit address.
- ❑ Colons (:) are sometimes used instead of dashes (-)

MAC addresses are often considered permanent, but in some circumstances, they can be changed.

Example:

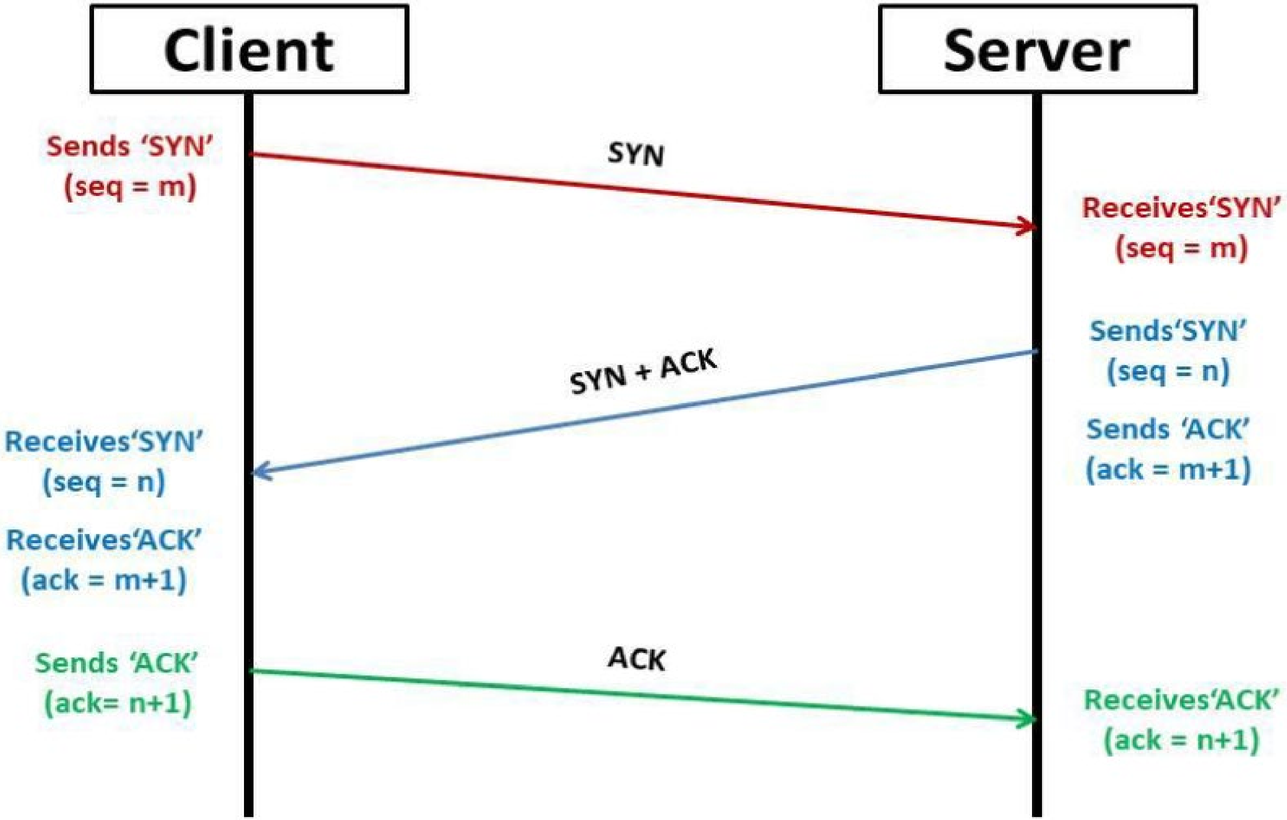
a4:c3:f0:85:ac:2d

- The blue bits indicates OUI (Organizationally Unique Identifier)/Vendor who built the network interface.
- The Violet bits indicates NICS (Network Interface Controller Specific)/UAA/unique address of the network interface.

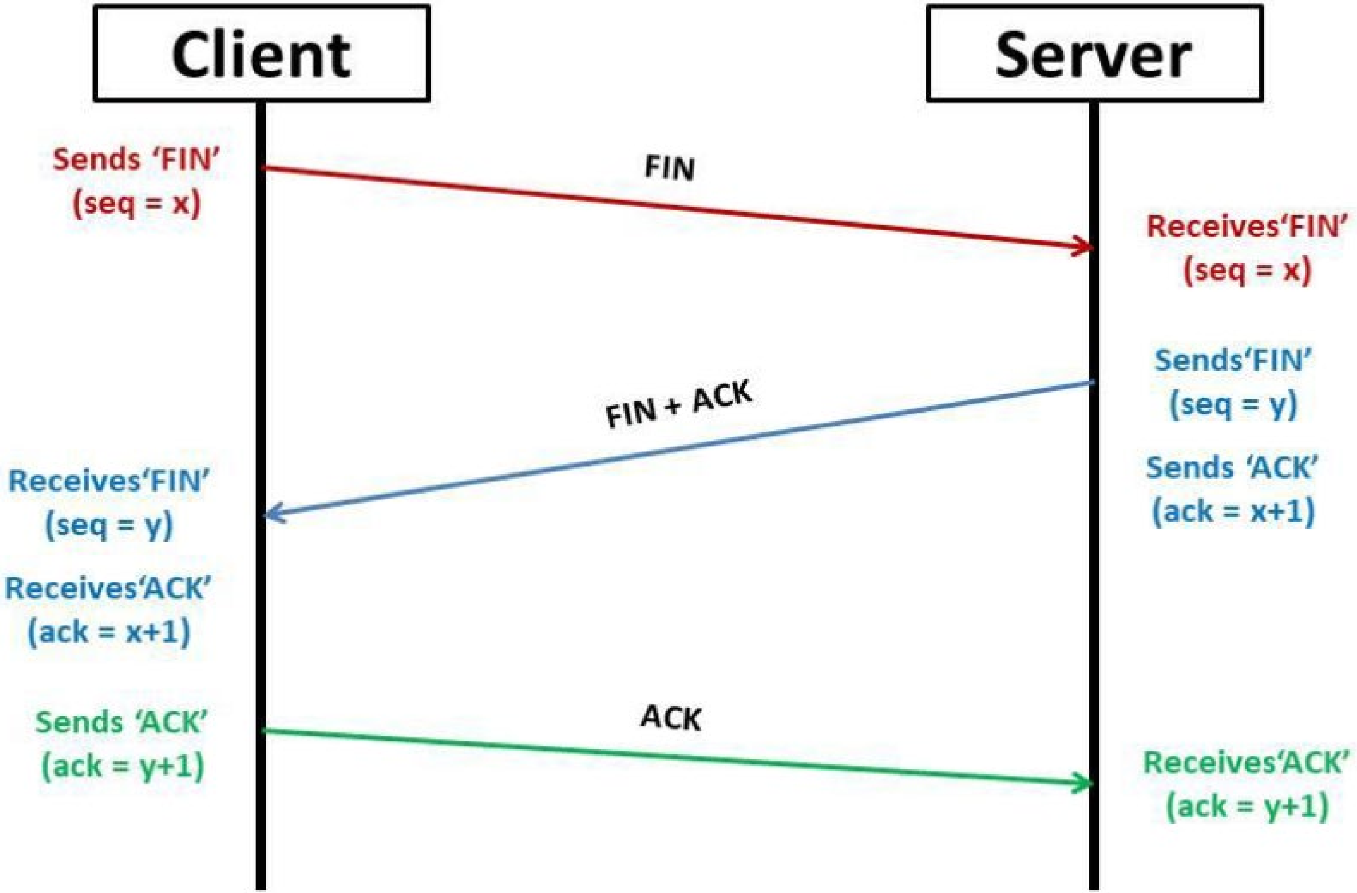
TCP & UDP

	Reliable	**Best-Effort**
Protocol	TCP	UDP
Connection Type	Connection-oriented: ✓ Provides reliability, and error correction and detection ✓ Guarantees of delivery ✓ Adds a sequence number to each packet so that the other end can verify that sequencing and look for missing pieces or packets	Connectionless: ✓ It provides limited error checking. ✓ No data recovery features to recover from packet loss. ✓ it does not offer retransmissions of packets in and off itself
Sequencing	Yes	No
Uses	Email, File Sharing, Downloading	Voice streaming, Video streaming, Realtime services
Examples	Web, SSH, FTP, POP etc.	Youtube, Tunnelling/VPN etc.

3-WAY HANDSHAKE (ESTABLISH CONNECTION)



3-WAY HANDSHAKE (TERMINATE CONNECTION)



COMMON PORTS AND PROTOCOLS

Protocol	TCP/UDP	Port Number
FTP (File Transfer Protocol	TCP	20/21
SSH (Secure Shell)	TCP	22
Telnet	TCP	23
SMTP (Simple Mail Transfer Protocol	TCP	25
DNS (Domain Name System)	TCP/UDP	53
DHCP (Dynamic Host Configuration Protocol)	UDP	67/68
HTTP (Hypertext Transfer Protocol)	TCP	80
POP(Post Office Protocol) v3	TCP	110
NetBIOS	TCP/UDP	137/138/139
IMAP (Internet Message Access Protocol)	TCP	143
HTTPS (Hypertext Transfer Protocol Secure) over SSL/TLS	TCP	443

LAB SETUP

- Install Virtualbox:
https://www.virtualbox.org/wiki/Downloads

- Download kali VM:
https://www.kali.org/get-kali/#kali-virtual-machines

- Register for ZrocCyberSec:
https://zumaroc.com/zroc/index.html

- Exploring HTB:
https://www.hackthebox.eu/

- Tryhackme
https://tryhackme.com

- Portswigger Academy:
https://portswigger.net/users/register

SOURCES

IP Address:
https://en.wikipedia.org/wiki/Classful_network
https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

Private & Public Address:
https://www.avast.com/c-ip-address-public-vs-private

Mac Address Lookup:
https://macaddress.io/
https://aruljohn.com/mac.pl