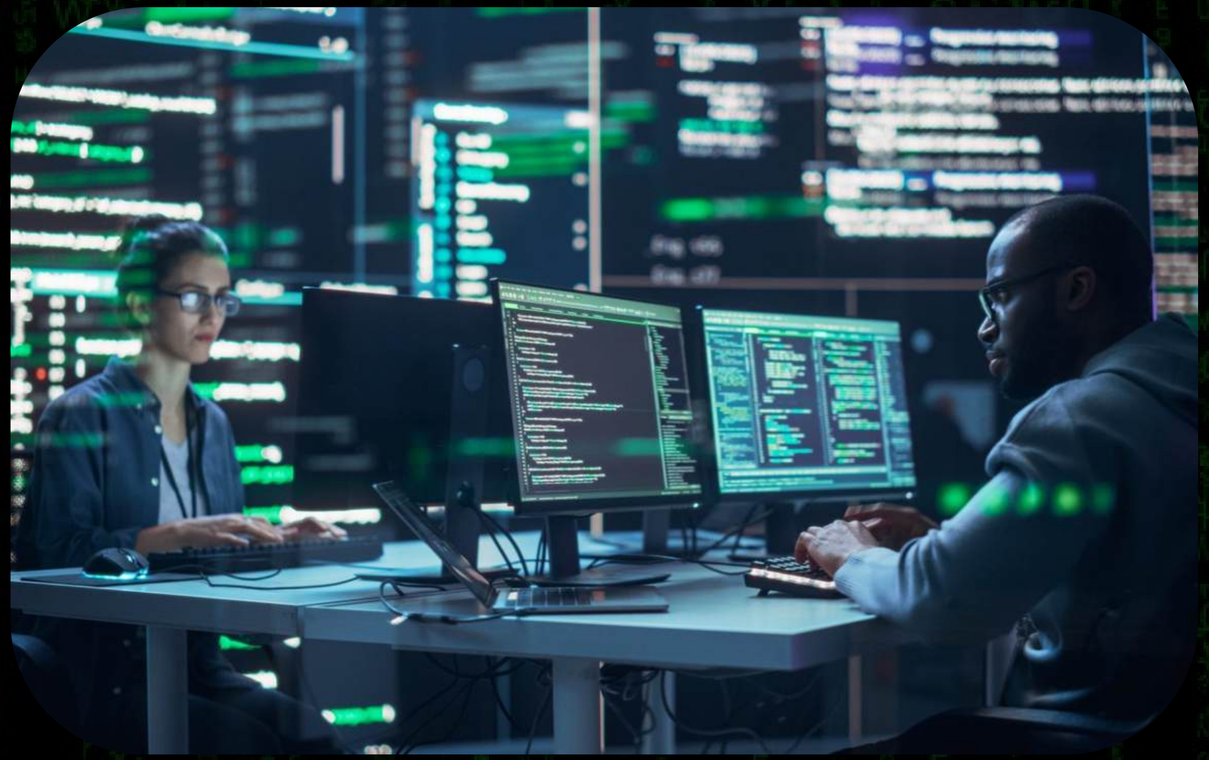
Introduction to Cybersecurity



BUNA BYTE

@bunabyte

Course Overview:

In this course,

- I will introduce you to the foundational concepts of cybersecurity.
- It will also serve as a solid foundation for more advanced cybersecurity courses under the Buna Byte.

INTRODUCTORY CONCEPTS

BUNA BYTE

@bunabyte

Security Terminology:

Black Hat

- Malicious hackers who hack for bad

White Hat

- Cybersecurity professionals who hack for good

Script Kiddie

- A hacker who uses scripts found online to conduct their hacks. They typically have little skill.

Vulnerability

- A weakness or flaw in a system, application, or network.

Exploit

- A piece of software, code, or sequence of commands that takes advantage of a vulnerability to compromise a system or perform malicious actions.

External Threats

- originates from outside the organization and is usually carried out by individuals or groups who do not have authorized access to the system.

Internal Threats

- comes from within an organization or system.

- These threats may be intentional or accidental.

What Is Data?

Data is nothing but digital information. Data can be personal [belonging to one individual] or organizational [belonging to an organization or company]

Personal	Organizational
Medical	Financial
Employment	Intellectual
Education	Confidential

How is Data Stored?

Data is typically stored either locally or remotely. Large sums of data are stored in databases.

Locally means that the user has direct and physical access to their data.

- Hard Drive
- USB Drive

Remotely means the data is stored on a server. A server is just a computer we can remotely connect to

- The Cloud
- Google Drive

Security Breaches:

A security breach is a type of cyber attack where a Black Hat hacker gains unauthorized access to a system and leaks data.

This leaked data can be detrimental to organizations and peoples lives. Which is why we have cybersecurity.

2022 security breach

What Is Cybersecurity?

Cybersecurity is the act of keeping data secure on networked systems. White Hat hackers need to fight against cyber attacks to keep individuals and organizations secure.

Why Is Cybersecurity Important?

Companies are trusted with the private data of its users, If this trust is broken by hackers, it will cause big issues for the company at hand.

If a hacker leaked the passwords of the users to this company, it would ruin the company's reputation and harm the digital lives of their clients.

SECURITY CAREERS

BUNA BYTE

@bunabyte

The Four Domains Of Security:

Generally speaking, there are four domains to the world of cybersecurity.

Red Teaming

Blue Teaming

Cybercrime and Analysis

Development and Engineering

Red Teaming:

White Hat hackers who act like Black Hat hackers.

Careers:

- ***Penetration Tester***, legally assess the security of a company.
- ***Ethical Hacker***, find vulnerabilities within a clients' system by emulating a hacker.
- ***Web Specialist***, discovers vulnerabilities in web infrastructure.

Blue Teaming:

Defending a system against all sorts of cyber attacks.

Careers:

- ***Network Administrator***, they are responsible for overseeing a network of computer and devices.
- ***System Administrator***, they are responsible for the maintenance and upkeep of computer systems.
- ***Incident Responder***, they are the first responder's in the event of a security breach.

Cybercrime And Analytics:

Cyber security law enforcement, understanding hackers.

Careers:

- ***Cybercrime Investigator***, an investigator/detective that will assist law enforcement or work as a private investigator.
- ***Intrusion Analyst***, they are responsible for preventing unauthorized entry to a network.
- ***Network Analyst***, they are networking specialists who are responsible for the implementation and upkeep of networks.

Development And Engineering:

Hackers who develop tools for better security.

Careers:

- ***Malware Developer***, develops malware to test the security of a network
- ***Security Engineer***, designs and creates a secure network
- ***Software Developer***, develops secure software for clients

UNDERSTANDING HACKERS

BUNA BYTE

@bunabyte

The Five Stages Of A Hack:

Reconnaissance:

Gathering Target Info like a Stalker

Scanning and Enumeration

Finding Vulnerabilities

Gaining Access

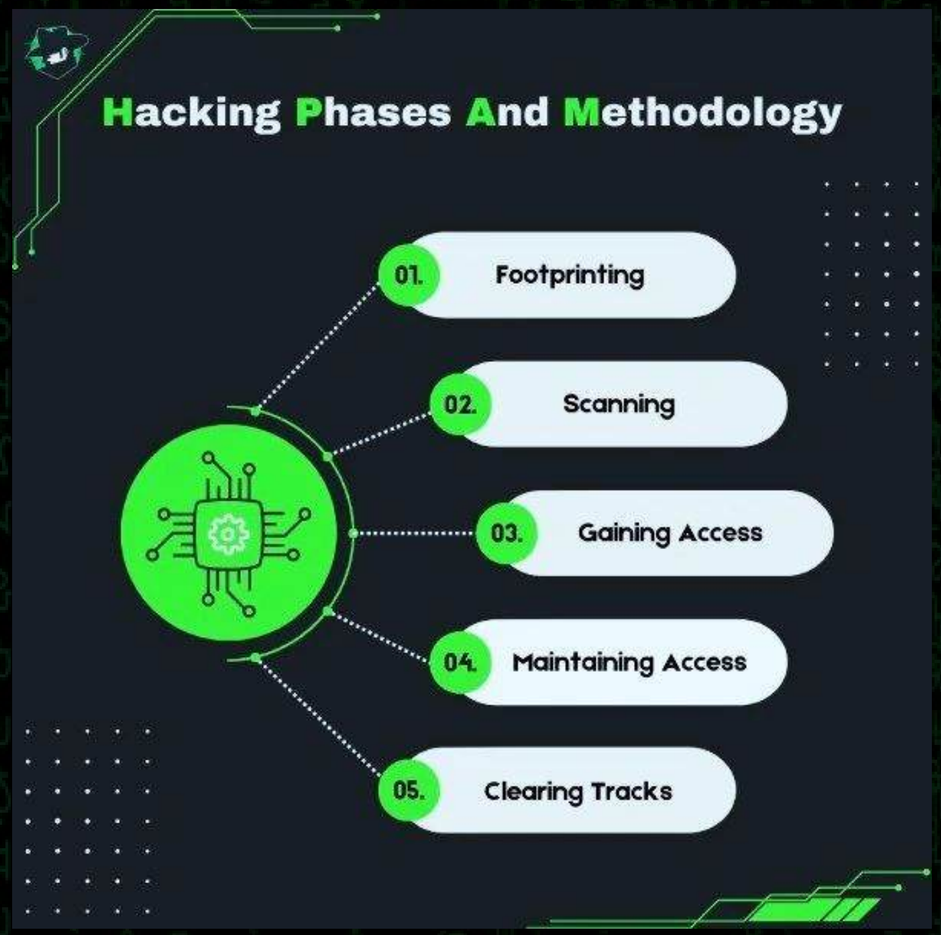
Getting into Systems like a Sneaky Ninja

Maintaining Access

Being able to keep your access to a target

Covering Tracks

Removing all traces of your presence

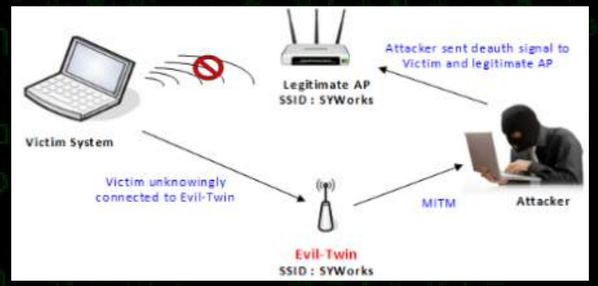


Types Of Attacks:

Black Hat hackers can use a wide range of cyber attacks. However, it all depends on the efficiency of each attack, and knowing what attack should be used in a given situation.

Online Attacks

Wireless Attacks



Physical Attacks

Social Engineering

Online Attacks:

Online attacks are attacks done digitally without any local access.

Examples:

- Phishing
- Malware
- Cracking
- Exploitation

Phishing:

Phishing is when an attacker sends a fraudulent e-mail, sms, message to someone to try to get their data and information.

For example:

A hacker sets-up a fake login portal, in which he has full control about anything going in and out.

Malware:

Malware is a piece of software designed to cause disruption and gain knowledge and/or control over any IoT device.

For example:

A piece of code that steals login credentials from your web browser by grabbing your saved passwords and usernames

Cracking:

Cracking is the process of using a series of patterns to gain access into a system.

For example:

An attacker will try as much passwords that he stored inside a file (commonly used is a database leak and its passwords) to try and get the right password.

Exploitation:

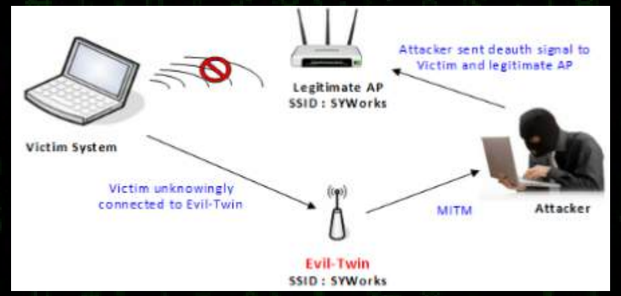
Exploitation is when an attacker finds vulnerabilities for a specific target and uses its vulnerabilities to get information and/or gain control over that target.

For example:

An attacker finds out you have an outdated service on your system and thus he can hack into your device by using an certain exploit for that outdated service.

Wireless Attacks:

Wireless attacks are essential for hackers because they allow them to exploit a certain target without needing any physical access.



Wi-Fi Attacks:

Evil Twin Attack, is a fake Wi-Fi access point used to mislead people into using it and thus the attacker can spy on the people on there.

Bluetooth Attacks:

BlueSnarfing, an attack that will let the attacker have full access to a person's phone by using a vulnerability in the bluetooth of that device.

Physical Attacks:

Physical attacks are attacks done by a hacker with the help of a HID (Human Interface Device) like a USB, on that there are exploits that the attacker can use to exploit a certain target.

Examples:

Rubber Ducky, a USB device that acts like a keyboard. It can inject keystrokes at a super fast speed and its known as a HID device.

Lan Turtle, this piece of tech is a device used to plug into a network and get a shell the second you do, it's a covert system administration and penetration testing tool.

Social Engineering Attacks:

Social Engineering attacks exploit the internal vulnerabilities of organizations. This is done by “hacking” the employees.

Includes:

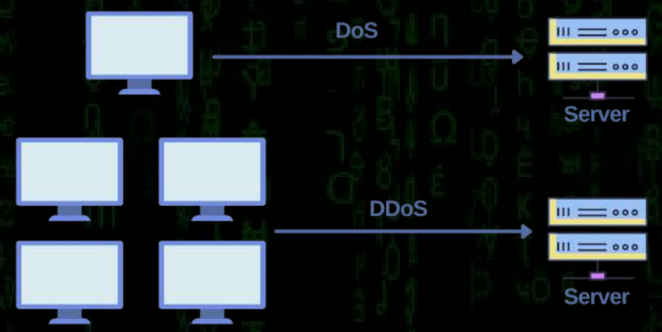
- Lying
- Pretending to be someone they aren’t
- Exploiting human emotion

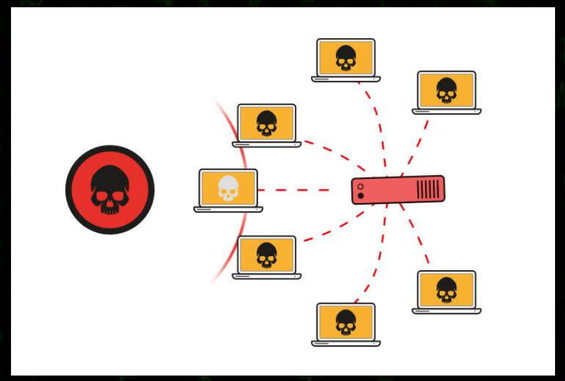
Denial Of Service Attacks:

A Denial of Service or DoS cyber attack where a hacker overwhelms the traffic to a specific host to the point where any other clients can no longer reach the host.

A DDos or Distributed DoS is where multiple clients will overwhelm a hosts traffic. This make the target harder to identify, because more often than not, these clients are infected by the hacker to perform the DoS attack.

This collection of infected clients are referred to as a BotNet.





These are merely the introductory concepts. However, this course should prepare you for other Buna Byte Cybersecurity courses to build up your cybersecurity skills.

Thank You!

SUBSCRIBE

BUNA BYTE

@bunabyte