LAB CYBER

THE ABSOLUTE BEGINNERS HAND BOOK GUIDE TO CYBER SECURITY

Part 1

CIA TRIAD

Confidentiality: Ensuring that data is private and accessed only by those with permission to do so. Can be achieved with the use of passwords,biometrics and encryption

Integrity: Ensuring that data has not been altered in any way. Can be achieved through the use of checksums and access control.

Availability: Ensuring that data is always available for access and use. Can be achieved through the use of backups, maintenance & disaster recovery plans

CYBER TERMINOLOGIES

Blacklist: Used to refer to a list of banned IP addresses, applications or users.

Whitelist: The exact opposite of a blacklist

Cat fishing: The process of creating a fake online profile in order to trick people into believing they are someone else for financial gain.

Authentication: The process of proving an individual is who they claim to be.

Data Mining: The activity of analyzing and/or searching through data in order to find items of relevance, significance or value

Threat: This generally refers to anything that has the potential to cause our data, systems and networks harm.

Exploit: A clearly defined way to breach the security of a system.

Vulnerabilities: These are weaknesses within a system or network that can be exploited to cause us harm.

Risk: This refers to the likelihood of something bad happening. A risk requires both a threat and a vulnerability to exist.

Zero Day: This is used to describe a threat that is unknown to security specialists and has not been addressed.

Hack Value: This describes a target that may attract an above average level of attention from an attacker.

Non-Repudiation: This is the concept that once an action is carried out by a party it cannot be denied by that same party.

Logic Bomb: A malicious code that is only triggered when a set of conditions are met.

Obfuscation: A term used to describe the tactic of making code unclear so that humans or programs like an antivirus cannot understand it.

Honey Pot: A decoy or trap for hackers

Spoof: The act of falsifying the identity of the source of a communication or interaction

PORTS & PROTOCOLS

A protocol is a set of rules that determines how computers or networks communicate with each other.

Ports are virtual windows used by protocols and services to run

HTTP (HyperText Transfer Protocol): determines how web browsers and servers communicate. Uses port 80

HTTPS (HyperText Transfer Protocol Secure): The secure version of HTTP that uses encryption. Commonly used on websites where there is an exchange of sensitive data like passwords and credit card details. Uses port 443

FTP (File Transfer Protocol): governs how files and data are transferred between servers and computers. Uses port 21

IMAP (Internet Message Access Protocol): Used by email clients to retrieve messages. Uses port 143

SMTP (Simple Mail Transfer Protocol): Determines how emails are sent. Uses port 25 for plain text and port 587 for encrypted communications.

COOKIES

A cookie is a text file which is placed on your computer whenever you visit a website. Cookies allow the website to keep track of your visit details and store your preferences. The main objective here is to increase the speed with which you visit that same website again. At the same time, they are very useful for advertisers who can match the ads to your interests after they see your browsing history.

Usually, cookies and temporary files may affect your privacy since they disclose your online habits, but it is possible to modify your web browser preferences and set a limit.

TCP/IP

TCP (Transmission Control Protocol): Divides a message or file into smaller packets that are transmitted over the internet and then reassembled at the destination point.

IP (Internet Protocol): Responsible for the address of each packet so they are sent to the right destination

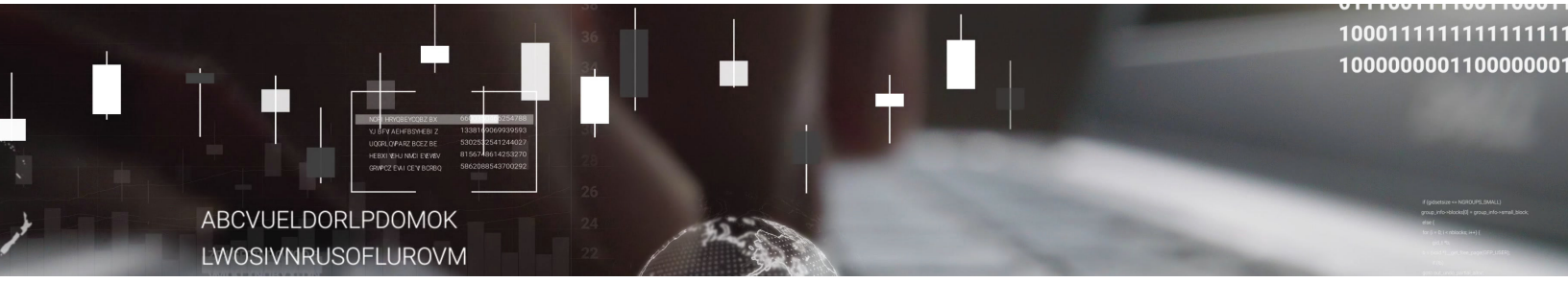
TCP/IP is divided into 4 main layers

Data Link Layer
Consists of protocols that operate on a link that connects hosts on a network e.g Ethernet

Internet Layer
Connects independent networks together e.g IP

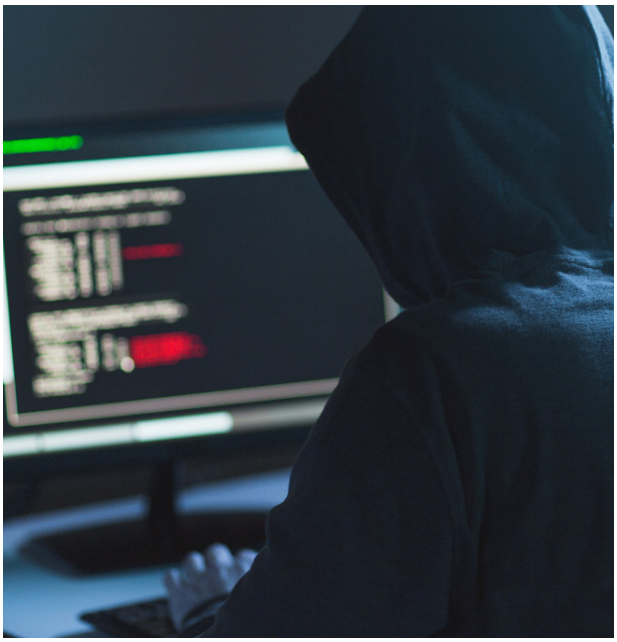
Transport Layer
Handles communication between hosts e.g TCP

Application Layer
Standardizes data exchange for applications e.g HTTP, FTP



HACKERS

WHO ARE THEY?



TYPES OF HACKERS

Script Kiddie
Derogatory term used to describe unskilled hackers

Grey Hats
Use black hat techniques

Black Hats
The bad guys who are highly skilled and hack for personal and financial gain

White Hats
The good guys who defend data and networks from black hats and malware

Hacktivists
Activists who hack for a social or political cause

THE HACKING METHODOLOGY

Reconnaissance/footprinting is the gathering of as much information as possible about the intended target.

Passive Recon: Silent reconnaissance where the target isn't aware of it. Information gathered here include email addresses, phone numbers, social media accounts etc.

Active Recon: More aggressive reconnaissance where the target is actively engaged to discover vulnerabilities. Information gathered here include passwords, IP addresses, open ports, conversation with employees.

Exploitation means taking advantage of a vulnerability to gain access.

Methods of exploitation include:

PHISHING EMAIL	SOCIAL ENGINEERING	UNPATCHED SOFTWARE	WEAK PASSWORDS

Privilege Escalation refers to increasing the control over the exploited target.

Establishing persistence means ensuring continuous access even after the breach/attack has been discovered by the victim.

Attack Phase: When the actual attack takes place

Cover up: Avoiding detection

ATTACKS

BRUTE FORCE ATTACKS

A very violent attack where the hacker attempts to crack a password by using extremely large possible combinations of letters and numbers to guess the right combination. Can be prevented with the use of very strong passwords and timeouts after consecutive failed login attempts.

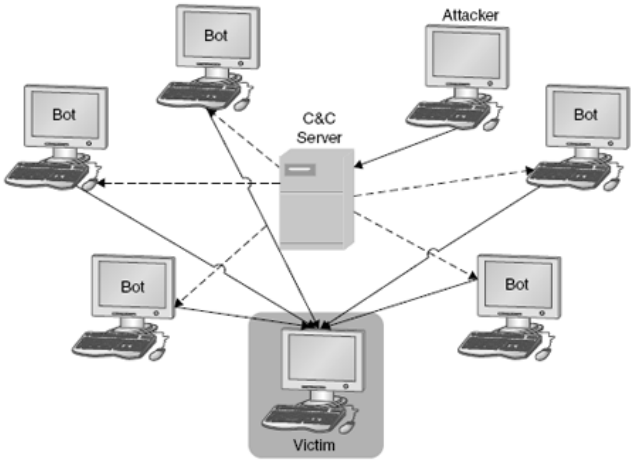
PHISHING

The most popular cyber attack where the victim is tricked into clicking a malicious link in an email. Spear phishing attacks are directed at very specific targets while a whaling attack is directed against senior executives of companies.

EMAIL SPOOFING

This is the forgery of an email header to make it look like the message originated from someone else other than the actual source.

BOTNETS



This refers to a collection of bots (infected computers). A botmaster controls the bots and can use them to perform a DOS attack.

DOS (Denial of Service)

This is an attack where the targeted server is flooded with useless requests in an attempt to overwhelm and shut it down. Can be combated by blocking the IP address of the source of the attack.

DDOS (Distributed Denial of Service)

A more sophisticated form of a DOS attack. Can be prevented with bandwidth overprovision.

MAN IN THE MIDDLE ATTACK

A crafty attack where the hacker is able to intercept and alter or steal data sent between two or more workstations. Examples of this attack include email hijacking, session hijacking and wifi eavesdropping.

SQL INJECTION ATTACK

The attacker executes malicious SQL commands to try and corrupt a database. This type of attack can provide the attacker with unauthorized access to sensitive information like passwords and usernames.

CROSS-SITE SCRIPTING (XSS) Attack

The attacker executes malicious scripts of code into a website or web application

MALWARE FAMILY

VIRUSES

Destroy/corrupt data, can self replicate but cannot spread themselves across a network.

WORMS

Can spread and self replicate themselves

TROJANS

Disguised to look like a legitimate app, cannot self replicate

ROOTKITS

Very hard to detect and remove. Designed to provide remote access

SPYWARE/ ADWARE

Spies on the online activities of the victim

Displays ads on your computer

KEYLOGGERS

Can record keyboard key strokes

Ransomware: An attack where the victim's files are encrypted and need to pay a ransom (usually in the form of Bitcoin) before they can regain access.

DEFENCES

ANTI-VIRUS

This is software used to protect a computer from malware. They are able to detect malware through their signatures.

They can also use heuristic methods i.e predicting a file is malicious by studying its behavior.

Antivirus can report a false positive i.e a legit program or file that was wrongly classified as malware.

Antivirus software differ in their detection rates as well as their system resource usage.

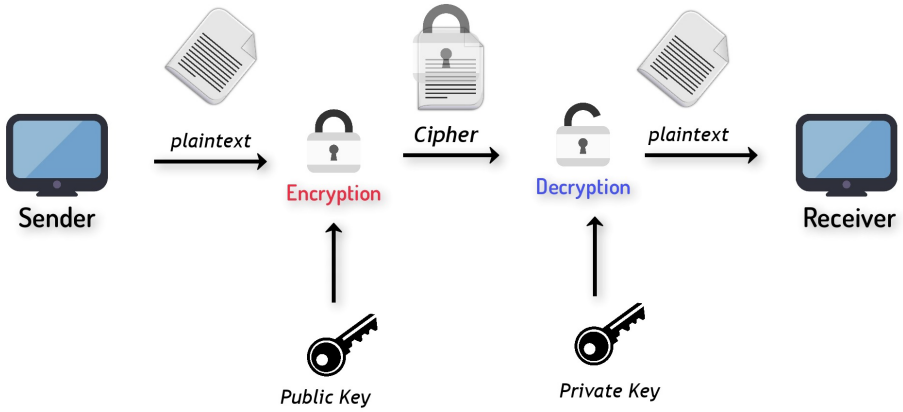
ENCRYPTION

A process of making information hidden or secretive.

Encryption uses a key known as a cipher to make the data secretive. Another key is then needed to decrypt the key and make it accessible again.

Cryptography is the study or science concerned with secret communication.

There are two main types of encryption:



Symmetric
Uses a single key e,g DES & AES

Asymmetric
Uses two different keys for encrypting and decrypting e.g RSA

FIREWALLS

A firewall is a security device that monitors incoming and outgoing network traffic. They can prevent users from sending certain data outside of their network and can also prevent access to certain websites.

Firewalls work by

Packet Filtering	**Proxy Service**	**Stateful Inspection**
Checks all the data passing through using a filter	The firewall acts as an intermediary between systems	Tracks the state of a connection between systems

Firewalls can either be hardware or software.

BIOMETRICS

A security mechanism used to authenticate and provide access based on the verification of physical characteristics.

Biometric identifiers are:

Physiological Characteristics
The shape or composition of the body e.g fingerprints, DNA, face, retina etc

Behavioral Characteristics
The behavior of a person e.g voice, gestures, gait

2 FACTOR AUTHENTICATION

A user provides 2 authentication factors to verify who they are.

Authentication factors include

Knowledge Factor	Possession Factor	Inherence Factor
Something the user knows like a password	Something the user has like a token or mobile device	Something the user is e.g biometrics

Authentication products include tokens, smart cards and smartphones
Multi Factor Authentication can include two or more factors like time and location

HONEY POTS & DMZS

A honey pot is a computer system that is a decoy to lure cyber criminals. They are used to study attempts to gain unauthorized access which would allow security admins to learn how to protect systems against them.

Production Honeypot: Are usually placed inside of a production network with other real servers to act as a decoy. The main objective is to keep the hackers distracted while the real production servers are patched up.

A Demilitarized Zone (DMZ) is a physical or logical subnetwork that separates a local area network from other untrusted networks

WIRELESS SECURITY

This is the prevention of unauthorized access to computers using wireless networks

Wired Equivalent Privacy (WEP)
Very weak with 64-bit and 128-bit encryption keys

Wifi Protected Access (WPA)
Developed by Wi-Fi alliance and uses 256-bit encryption keys. Was superseded by WPA 2 in 2006

PASSWORD MANAGEMENT

A strong password has 4 main requirements

- **AT LEAST 8 CHARACTERS**
- **CONTAIN BOTH NUMBERS & LETTERS**
- **AT LEAST ONE CAPITAL LETTER**
- **AT LEAST ONE SYMBOL**

CYBER SECURITY AT THE **WORKPLACE**

Security Policy: This is a written document that describes how an organization protects its virtual and physical data assets from threats.

BYOD Policy: A policy that describes how employees are able to use their own personal device to access company data in a safe and secure manner.

Incident Response Plan: A set of policies and procedures that are used to identify, contain and eliminate cyber attacks.

Disaster Recovery Plan: A plan that focuses on the restoration of critical systems after a disaster.

The Security vs Ease of Access paradox states that the easier it is to access data the less secure it is and the more difficult it is to access it, the more secure it is.

ACTIONABLE TIPS FOR
PERSONAL CYBER SECURITY

USE A STRONG PASSWORD

One of the easiest things you can do right now. Make sure your password is at least 8 characters in length and has a combination of letters, numbers and a special character.

PASSWORD VARIETY

Even if you have got the strongest password in the world, it's not a good idea to just one password for all your accounts. Try to come up with 2 or even 3 variations of your main password and use those as well for some accounts. An alternative here would be to use password managers like Dashlane or LastPass.

DEPLOY MULTI FACTOR AUTHENTICATION METHODS

Several websites and applications like Gmail recommend a second means of verifying who you are such as receiving a text message with a code on your phone when attempting to log in from a different computer. This extra layer of security can make a huge difference so please do it.

USE AN ANTIVIRUS

You already know why you should. If you want a recommendation, I highly recommend using Kaspersky.

WATCH OUT FOR HTTPS

As we discussed in the Protocols class, HTTPS is the secure version of HTTP and should be used on sites where important information like credit card details are provided. Whenever you are on such a site, make sure that you can see the secure padlock sign in the address bar that shows HTTPS

CHANGE YOUR ROUTER'S DEFAULT PASSWORD

If you have an internet router at home, take 10 minutes now to change the default password now if you haven't.

USE A STANDARD ACCOUNT

On a daily basis I highly recommend you use a non administrative account on your computer. This means that even if you get infected with malware, it wouldn't be able to do much damage. In other words, no admin rights = no admin privileges to infect your PC.

BE CAUTIOUS AT ALL TIMES

Always double check anything you download to your computer. Think twice before clicking on that link you receive in your email. Be extremely wary of free applications.

DON'T STORE SENSITIVE DATA ON YOUR PC

If you have got important files like scanned copies of very important documents, you are better off storing them on a detachable flash drive that you can always plug into your computer and use when you have to.