LAB CYBER

www.labcyber.com

PART 2

THE ABSOLUTE BEGINNERS HAND BOOK GUIDE TO CYBER SECURITY

IP Address

- IP = Internet Protocol
  - They are assigned when a device joins a network to make them traceable.
  - 2 Types - IPv4 & IPv6
  - Your Router will have the internet visible IP address but will assign a private IP address to your computer and every other device on its network.
  - If directly connected, your computer will have the internet visible IP address.

MAC Address

- MAC = Media Access Control
  - It's the unique serial number assigned to every network adapter when manufactured.
  - MAC addresses are typically used only to direct packets from one device to the next as data travels on a network.
  - Can't be hidden but doesn't travel beyond the local network.

Switches vs Routers

- A Switch transmits data among devices on a local network while a Router routes data among networks.
- Switches use MAC addresses while Routers use IP addresses.
- Routers are far more powerful and provide additional features such as firewall protection.

Ethernet

- A protocol that determines how data is transmitted in a Local Area Network (LAN).
- Technically referred to as IEEE 802.3 protocol.
- Used widely in offices, banks and in homes.
- Most laptops & PCs come with integrated ethernet cards.

Ethernet Process

- Device A wants to send data to Device B.
- Device A checks to see if the carrier (main wire connecting the devices) is free.
- If YES, device A sends the data packet on the network.
- Device B receives the packet.
- If NO, device A waits for some thousandths of a second and tries again.

HTTP

- Hypertext Transfer Protocol
- It defines how messages are formatted and transmitted over the web.
- It also determines what actions web servers and browsers should take in response to various commands.

HTTPS

- Hypertext Transfer Protocol Secure
- Communication between the web browser and web server is encrypted.
- A must for websites where sensitive info like passwords, credit card details are exchanged.
- Encryption is implemented by making use of TLS or SSL.

SSL

- Secure Sockets Layer
- Establishes an encrypted link between web server and browser.
- Your web server requires an SSL certificate to be installed on it.
- This certificate serves as proof that the website is secured with SSL but also has an expiry date.
- A browser connecting to your site will check to see if the certificate has expired before completing the connection.

TLS

- Transport Layer Security
- Successor to SSL
- More advanced and offers a higher degree of encryption and security.
- SSL & TSL are used interchangeably.

The Internet Protocol Suite

TCP/IP

- The conceptual model and set of communication protocols used on the internet.
- Provides end-to-end data communication specifying how data should be packetized , addressed, transmitted, routed and received.
- Responsible for data sent from a host to a destination (another host, network or internet) and vice versa.
- Commonly referred to as TCP/IP (the two foundational protocols):
  1. Transmission Control Protocol
  2. Internet Protocol

Divided into 4 main layers:

- Link Layer
- Internet Layer
- Transport Layer
- Application Layer

Link Layer

- The lowest layer in the TCP/IP architecture.
- Communication protocols that only operate on the link that a host is physically connected to.
- Sample protocols include:
  1. MAC
  2. Ethernet
  3. IEEE 802.11 (wifi)

Internet Layer

- Handles internetworking between networks.
- Is not responsible for a reliable transmission.
- Captures data packets and sends them to the appropriate transport layer protocol.
- Provides error detection and diagnostics.
- Sample protocols include:
  1. IP - IPv4 & IPv6
  2. ICMP - Internet Control Message Protocol used for error detection

Transport Layer

- Handles host to host communication.
- Is responsible for a reliable transmission.
- Handles flow control and prevents congestion.
- Core protocols include:
  1. TCP
  2. UDP

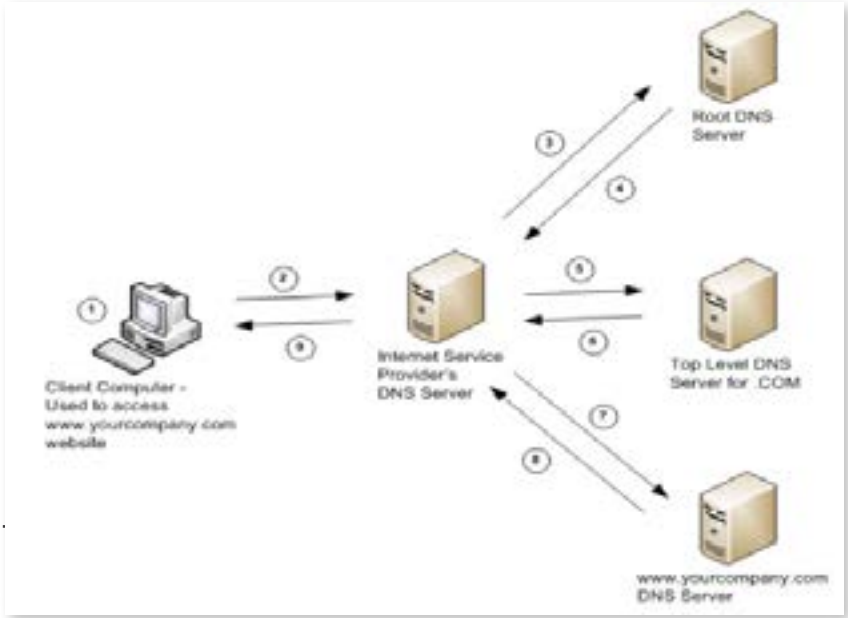
Application Layer

- Handles data exchange between applications.
- Make use of specific protocols in the layers beneath them.
- Sample protocols include:
  1. HTTP
  2. SSL
  3. FTP
  4. SMTP

The DNS System

DNS

- Domain Name System
- Translates domain names into IP addresses e.g www.alex.com = 101.43.192.45
- The phone book of the internet



What is Privacy?

- The ability to protect valuable
- and sensitive information.

  Privacy ensures that personal information is collected, processed, used and destroyed in a legal and fair manner. E.g medical records.

What is Anonymity?

- Keeping a user's identity hidden.
- Actions carried out cannot be traced back to the user.
- Hackers dream
- Can never be guaranteed.

What is Pseudonymity?

- The near anonymous state where a user has a consistent identifier that is not their real name - pseudonym.
- In pseudonymous systems, the real identities are available to the administrators. E.g Hookup sites.

Pseudo-anonymity ***

- The appearance but not the reality of anonymity online.
- Enables anonymous posting without the need for an identifier e.g pseudonym.
- Users can still be traced through IP addresses and are generally required to provide some ID when signing up.

Identity Strategies

- Open
- Avoidance
- Persona
- Compartmentalization
- Selective/Custom

Open Strategy

- Authentic
- Can leave you vulnerable

Avoidance Strategy

- Deprives you of online benefits

Persona Strategy

- Vulnerable, Fake personality
- Very common with journalists, politicians

How We are Tracked Online

- Every device behaves in a unique manner when interacting with a web page.
- The action is invisible to the user and can be used to create a fingerprint for the device.
- The user can then be tracked using the fingerprint when the same device goes back online.
- This tracking technique is called canvas fingerprinting.
- The tracking script on the website visited will instruct your browser to draw an invisible image behind the scenes.
- Every device will draw such an image in a unique manner thus creating a special ID and fingerprint for each device.
- Cookie Syncing - Tracking companies share the information they have about you without your knowledge or approval.

5 Tips to Make You Harder to Track

- Use a VPN
- Email Caution
- Clear Browser Cache
- Adjust Social Media Privacy Settings
- Turn off Location Tracking

Anonymizers, Proxies, Virtual Private Networks & Tor

Anonymizers

Anonymizer is the collective term for tools and software that are used to make activity on the Internet untraceable.

- Offers protection against hackers & identity theft.
- Provides privacy.
- Bypasses censorship allowing access to information.

Types of Anonymizers

Single Point - Passes your surfing through a single point to protect your identity e.g proxy server.

Networked - Transfers your communication through a network of computers e.g Tor

Proxy Servers

A proxy is a server that acts as an intermediary for requests made by clients seeking resources from web servers.

- Can provide you with a proxy IP address for defeating restrictions and censorship.
- Bypasses your ISP.
- Useful for torrents.

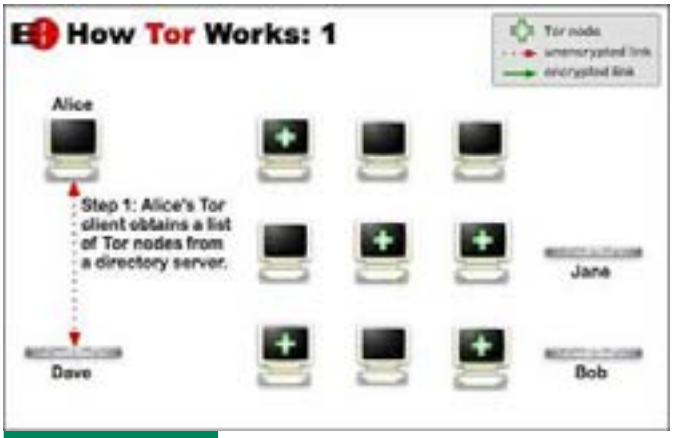
Things to Note

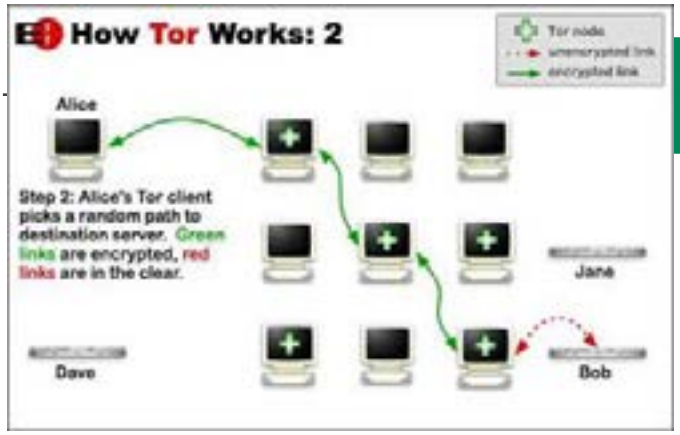
- Speed can be an issue.
- Reliability not a guarantee.
- Provides no encryption.

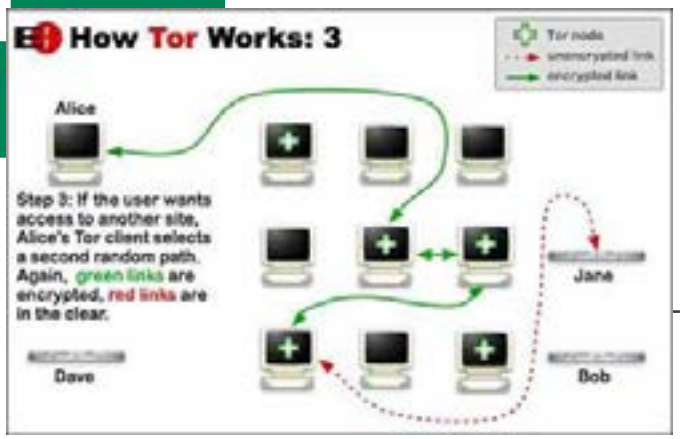
Virtual Private Network

A VPN is a solution that allows users to send and receive data while maintaining the secrecy of a private network.

- More powerful than a proxy server.
- Creates an encrypted tunnel that secures the traffic between the client and VPN server.
- In theory, VPN can provide optimal but not total privacy.
- Useful for accessing a form's intranet while away.







Tor through VPN Connection - **Pros**

- Use of Tor is hidden from ISP.
- Tor entry node will not see your IP address but that of the VPN.
- Allows access to hidden Tor services / websites.

VPN through Tor Connection - **Pros**

- Bypasses blocked exit nodes.
- VPN provider cannot see your real IP address.
- Protection from malicious exit nodes due to encrypted data entering and exiting Tor network.

Tor Through VPN Connection - **Cons**

- VPN provider knows your real IP address.
- Tor exit nodes are unencrypted and can be monitored.

  Tor edit nodes can be blocked.

VPN through Tor Connection - **Cons**

- VPN providers can see your traffic.
- More susceptible to end-to-end timing attacks.
- VPN through Tor connection provides true anonymity and is more secure ***

Malware, Viruses, Rootkits, Ransomware & Attacks

Malware

- Malware is the collective term for all malicious software & programs.
- No all-in-one solution.

Malware Family

- Viruses - Replicate themselves by contaminating legit programs with their own code.
- Worms - Self replicate and spread themselves through a network.
- Trojans - Pretend to be real programs e.g games. Do not inject themselves into other programs.
- Rootkits - Provide access to unauthorized areas. Extremely hard to detect and eradicate.
- Ransomware - Blocks access to data until a random is paid.

Exploits - Take advantage of bugs and vulnerabilities.

Viruses

- Viruses typically attach themselves to executable files and Word documents.
- They spread via email attachments, infected websites and flash drives.
- A virus will remain dormant until the infected file or system is activated.

Once activated, the virus causes destruction.

Worms

- Worms enter systems via network connection or a downloaded file.
- They then make copies of themselves and can spread via a network / internet connection.

Fight Against Viruses & Worms

- Antivirus and Antimalware products.
- Restrict use of flash drives.
- Scan Email Attachments.

What is an Antivirus?

- Anti-virus software is used to protect a computer from malware.
- Viruses detect malware by signatures i.e pattern of data that is known to be related to already identified malware.
- Antiviruses can also use Heuristic methods i.e predicting a file is malicious by studying its behavior.
- Sandbox Testing - the file is allowed to run in a controlled virtual system to see what it does.
- Can result in a false positive - a legit program classified as malware.

Antivirus Operations

- On Access Scanning - The antivirus checks every file or program that is opened.
- Full System Scan
- Polymorphic virus - A virus that morphs or changes its code making it very difficult to be detected.

Types of Rootkits

1. Kernel Level - They have the highest privilege and can inject code in the core of the OS.

2. Application Level - Can modify the behavior of existing applications.

3. Library Level - Can hook, patch or replace system calls with malicious code to hide its presence.

4. Hypervisor Level - They target the boot sequence and load themselves as an hypervisor.

5. Firmware Level - Overwrite the BIOS of the PC. Allows the rootkit to install and hide malware.

Symptoms

- Antimalware doesn't work anymore.
- Windows settings change e.g pinned items changing, background images.
- Frozen input devices like mouse and keyboard.
- High network usage on idle computers.

Ransomware

Infection Methods

- Email Attachments - Infectious links or attachments are sent via an email from the attacker to the victim.
- Exploits - Attacker takes advantage of bugs and unpatched vulnerabilities on a PC.

Doxing

- The public release of private information about an individual or company.
- The attacker threatens to release sensitive info unless the victim pays up.
- Potentially more effective than traditional ransomware attacks.

Prevention Methods

- Email Attachments - Never Open suspicious attachments or links sent via email.
- Exploits - Always update and patch whenever possible.
- Malware - Install antimalware software.
- Backups - This won't prevent attacks but will reduce the severity of a successful attack.
- Websites - Say no to porn websites

Backups, Storage, The Cloud & Encryption

MAC Address

Storing & accessing files & data on the internet rather than a local hard drive.

- The word "cloud" is a metaphor for the internet.
- Data should be accessible anywhere & anytime with an internet connection.
- Web based apps - **office online**.

Types

- Google Drive
- iCloud
- Amazon Web Services
- Dropbox (**hybrid**)

Cloud Arguments

- Control, privacy and trust issues
- Outages and lack of access
- Ownership - who owns the data?

Best Practices

- Never store sensitive data e.g medical records in the cloud
- Store music, videos and regular files.
- Use more than one.

Encryption/ Decryption

What does Encryption protect you against?

- Physical theft
- If your device is seized
- Repairs
- Data alteration

What doesn't Encryption protect you against?

- Malware & Rootkits
- Cold Boot Attack
- After decryption, the key can be gotten from memory.
- Files back to an unencrypted location are vulnerable.

Encryption Attacks Rootkits & Bootkits

- Rootkits have equal or more privileges than the operating system.
- Application level rootkits can bypass encryption.
- **Secure boot** process can be used to prevent this attack.

Brute Force Attacks

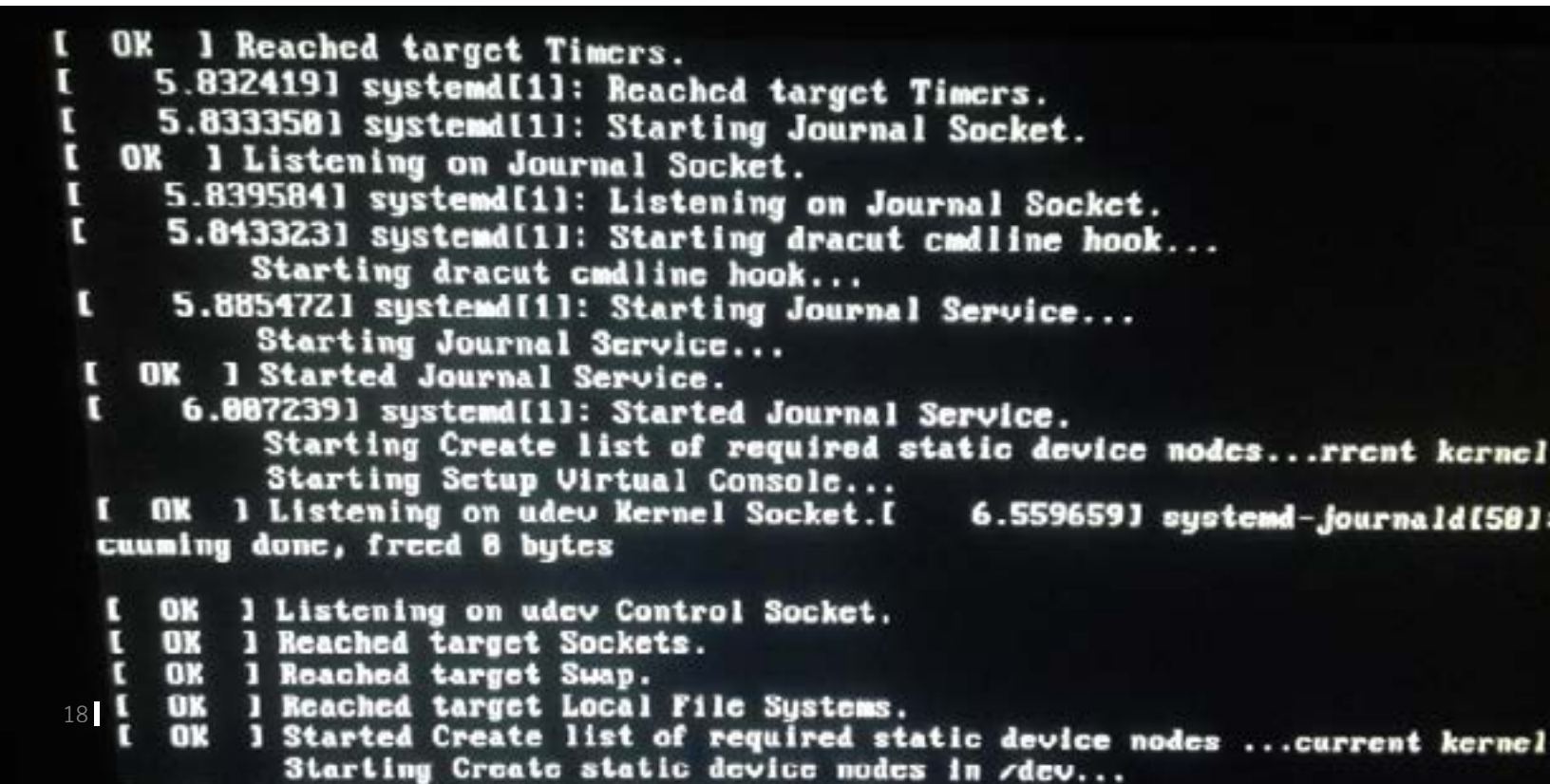
- The process of trying millions of passwords until the right one is found.
- Fairly easy to combat with complex passwords and account lockouts.

Direct Memory Access Attack

- A second PC running a memory scanning tool is connected to the target PC through the DMA port e.g thunderbolt.
- Once connected, the software scans the memory and uncovers the encryption key.
- The encryption key can then be used to decrypt the hard drive.
- Vulnerable ports can be disabled.

Hyberfil.sys Attack

- hyberfil.sys is the Windows hibernation file which contains a snapshot of the system memory when the system hibernates.
- Tools exist that can be used to scan the file for the encryption keys.
- By default, Windows is designed to be secure against this attack because the hyberfil.sys file is stored within the encrypted container.



Memory Remanence Attack

- Cold boot attack
- Memory chips don't immediately lose their power when a PC is turned off.
- An attacker with physical access to the memory chips can read the encryption key.
- Freeze the PC's memory. For example, an attacker can freeze the memory to -50°C by spraying it with aerosol air duster spray.
- Restart the PC.
- Instead of restarting Windows, boot to another operating system. Typically, this is done by connecting a bootable flash drive or loading a bootable DVD.
- The bootable media loads the memory remanence attack tools, which the attacker uses to scan the system memory and locate the encryption keys.
- The attacker uses the encryption keys to access the driver's data.

Social Engineering - Scams, Cons, Tricks & Fraud

Social Engineering

- The art of gaining unauthorized access to buildings & systems through the exploitation of human psychology.
- Targets the weakest link in a security model/system - the human element.
- The term was popularized by **Kevin Mitnick**.

Types of SE Attacks

- Phishing *
- Vishing
- Smishing
- Sextortion
- Insider
- Phony recruiters

Vishing

- Attacker calls the target and pretends to be from Microsoft or from the target's company.
- Attacker claims the victim's computer has been infected with malware and has the solution.
- Attacker directs the victim to perform certain operations on the computer in order to grant the attacker access.

Smishing

- Attackers use text messages.
- The text will contain either a link or a phone number that can be used to lure the victim.

Sextortion

- Attacker poses as a potential sex partner and lures the victim to share compromising videos or pictures.
- The videos/photos are then used to blackmail the victim.
- Senior officials or top executives are often targets.

Insider

- Attacker infiltrates a company through a job offer or connects with a disgruntled employee of the target company.

Phony Recruiters

- Attacker pretends to be a headhunter and lures the victim to provide confidential data.
- Attackers can get enough data to figure out who to attack in the company.

Prevention

- Vigilance
- Training

Receiving Email **Ports & Protocols**

- IMAP port 143 (unencrypted)
- POP port 110 (unencrypted)
- IMAP port 993 (SSL/TLS encrypted)

  POP port 995 (SSL/TLS encrypted)

- **IMAP** (Internet Message Access Protocol) - emails are synced between the mail client and the mail server. Less secure but more convenient.
- **POP** (Post Office Protocol) - emails are stored only on the client. More secure but less convenient.

Sending Email **Ports & Protocols**

- SMTP port 25 (unencrypted)
- SMTP port 465 (SSL/TLS encrypted)
- STARTTLS port 587 (SSL/TLS encrypted)
- **SMTP** (Simple Message Transfer Protocol)
- **STARTTLS** - can turn an insecure connection to a secure one.

Phishing

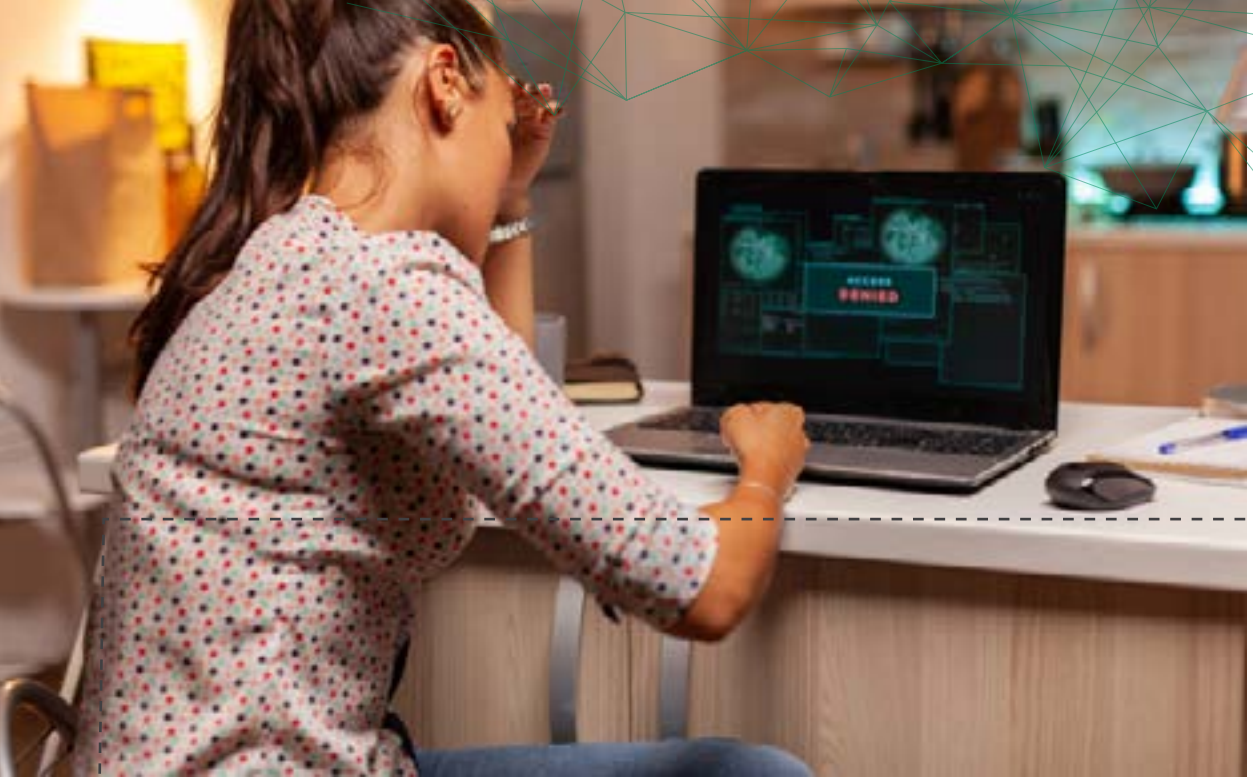
- Attacker masquerades as a reputable person or company in an email (spoofing).
- Emails contain malicious links or attachments that can be used to extract data e.g passwords, CC details, etc.
- Target emails are gotten through reconnaissance methods.
- Phishing campaigns are often built around popular events or breaking news.

The CEO Wire Fraud Attack

- Attacker sends an email “spoofed” to look like it was sent by top ranking executives and asks to have funds transferred to a financial institution.

Prevention

- Never download attachments or click on links from unknown sources.
- It’s okay to open phishing emails.
- Double check before transferring funds.



USEFUL LINKS

- https://www.labcyber.com/
- https://www.linkedin.com/in/alexanderoni/
- https://www.linkedin.com/company/lab-cyber/
- https://www.youtube.com/channel/UCfYIZcXn7mrIucP8vPbbbXg
- https://www.howtogeek.com/115483/htg-explains-learn-how-websites-are-tracking-you-online/
- https://www.techradar.com/news/us-uk-investigating-facebooks-role-in-cambridge-analytica-data-breach
- https://pastebin.com/TB4ifihx
- https://docs.microsoft.com/en-us/windows/security/information-protection/secure-the-windows-10-boot-process
- https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview
- https://www.computerweekly.com/feature/Self-encrypting-drives-SED-the-best-kept-secret-in-hard-drive-encryption-security
- https://www.youtube.com/watch?v=F78UdORll-Q
- https://www.csoonline.com/article/2123704/social-engineering--anatomy-of-a-hack.html