Cybersec Notes

Security Assessment & Audits

Security Assessments:

- Can be a pentest
- Usually non-confrontational & discreet in terms of the results.

Security Audits:

- Often confrontational, not exactly discreet in terms of results (result could be published publicly)

- The goal of both security assessments & security audits is to provide evidence of a system's security being up to par.

Governance, Risk, & Compliance (GRC)

GRC:

- **Governance** - High-level oversight of business processes in relation to security
- **Risk** - Reducing risks & consequences of attacks to a manageable level
- **Compliance** - Ensuring the company is complying/conforming with framework & tools implemented (EX: PCI-DSS)
- If a framework you are attempting to follow is considered stronger than the security requirements your company currently follows, this is considered a **gap** (**EX**: if your security policy states passwords must be 7 characters long while the framework requires 10 character long passwords, this area is considered a gap). To fix this gap, you change the requirements to comply with the framework.
- If a framework comes along, let's say it states passwords have to be at least 7 characters long but your security policy states passwords have to be 10 characters long, no change is required, you are technically complying with the framework.

Hybrid Cloud

Shifting:

- The shift from a perimeter protected enterprise to a more cloud based virtualized enterprise is due to:
    - Running services on the cloud (SaaS) is **cheaper**
    - **Ease of access** in terms of accessing data from mobile devices remotely.
    - **Flexibility** (easy to transition to different services).

Micro-Segmentation:

- The technique of creating a mini perimeter around apps that are hosted on the cloud. The perimeter would be a virtual concept such as a firewall, IDS, or IPS etc.
- Kinda like putting applications in a protective container

Defense in Depth through Micro-Segmentation:

- The idea of layering defense within the micro segment & in the overall cloud. This can be done with or without physical hardware but most likely through virtualization.

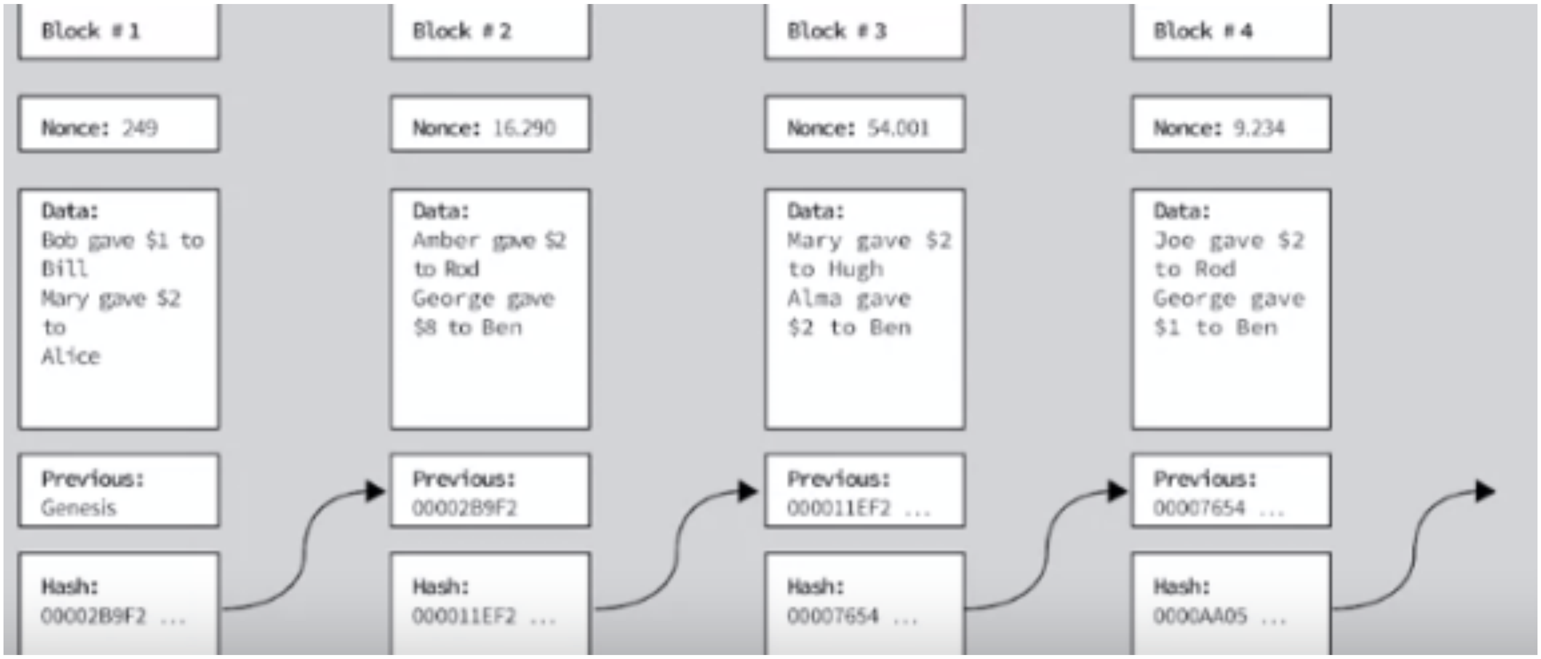
CASB:

- CASB = Cloud Access Security Broker
- CASB is like a man-in-the-middle which offers access control, monitoring, logging/auditing for multiple clouds in a centralized environment, like a SIEM.

Blockchain

Blockchain In Cybersecurity:

- Blocks have to do with hashing data with a nonce that will end up resulting (the hash being the result) in a string of characters that starts with four 0s, if this isn't the result. You try again with a different nonce until you get the four 0s in front.
- In the sense of security, blockchains provide integrity & confidentiality of data.
- Now in terms of chaining, we have one more component called the **Genesis** block or the “previous” block, the previous doesn't exactly exist which is why it's called Genesis (Note Genesis only exists when constructing the first block). The normal concept still remains, where our goal is to gain a hash beginning with four 0s. We then take the previous data we just hashed & move onto our next block of data where we insert the previous hash output that we acquired from the previous block (see photo). Literal chaining of data.



Block #1	Block #2	Block #3	Block #4
Nonce: 249	Nonce: 16,290	Nonce: 54,001	Nonce: 9,234
Data: Bob gave $1 to Bill Mary gave $2 to Alice	Data: Amber gave $2 to Rod George gave $8 to Ben	Data: Mary gave $2 to Hugh Alma gave $2 to Ben	Data: Joe gave $2 to Rod George gave $1 to Ben
Previous: Genesis	Previous: 00002B9F2	Previous: 000011EF2 ...	Previous: 00007654 ...
Hash: 00002B9F2 ...	Hash: 000011EF2 ...	Hash: 00007654 ...	Hash: 0000AA05 ...

- If a hacker were to say go back to the Block #2 & changes the data, it messes up the “chain” & the problem spreads to the chains after the Block #2. In this case since the hash value of Block #3 contains the hash value of Block #2 (recall, since the data is different, the hash isn't going to stay the same).
- The main thing that will be messed up will be the fact the hash will no longer have those four 0s in front, of course a hacker can go back in and modify the nonce until the hash has those four 0s in front but since the data is changed the hash will not be the same until the data is reverted back to the original. While all these changes are occurring, the chain of data may be growing so catching up to modify the next block of data to make sure it goes unnoticed would be nearly impossible.

Cyber Attribution

Cyber Attribution:

• When a successful cyberattack has been launched, there is many concern about catching the criminal who did it which is the definition of **cyber attribution**
• Due to spoofing & other tools (proxies, vpns etc) detecting the source of the attack is difficult. But law enforcement agencies in developed countries do have good techniques/tools/skills to attribute cyber attacks to certain individuals. These techniques include:

- **Cyber forensic** (forensic analysis on the tools used to carry out the attack)
- **Network Monitoring** (tracing logs, etc)
- **Offensive attacks** (nation state actors breaching other countries infrastructure or individual infrastructure & finding stolen data from previous attacks.)
- **Insider observation**
- **Information leaks** (documents that describe attacks or leaked texts, etc)
- **Law enforcement investigation** (basic investigation that would be done with normal crimes)
- **Partner/Ally sharing** (Kinda like insider observation, sharing details of attacks conducted)

Onion Routing

Onion Routing:

- The idea of onion routing sprung from a hypothesis of being able to browse resources without having it being attributed to your identity.
- The way it works is between the client & the server, the client's connection is routed/sent through various nodes (or servers) to travel through to mask the original client's identity & after a few routes, it finally connects to the server anonymously. But recall the FBI has control of some of these nodes that do the routing, making this less trustable than it was a few years ago.
- In terms of cybersecurity, this onion routing protocol has 2 things to do with security:
    - Illegal commerce which will normally take place using the onion routing protocol (Tor) involving data stolen after breaches
    - Anonymity

Chaum Blinding Algorithm

Chaum Blinding Algorithm:

- This algorithm's purpose is to introduce anonymity between clients & servers.
- How it works: A sender creates 1,000 duplicate notes (number can be any amount), only difference is the serial numbers & keys are different but the amount is the same. This is sent to a 2nd person (all 1,000) & this 2nd person at random picks a number between 1 & 1,000 without the original sender knowing the number (lets say the number he picked was 53), the 2nd person then requests all the keys except the key for the number he picked (in this case 53). The keys are provided excluding the one, & the 2nd person now reads the notes to see if they are legitimate, the 2nd person concludes the 1 note they didn't request the key too will most likely be legitimate as well & signs the note & sends it back to the original sender. The concept could be applied to numerous things.

Critical Infrastructure

Critical Infrastructure:

- A **definition** of critical assets would be if it was removed, that asset makes the organization's mission impossible to accomplish. In terms of infrastructure, if these assets were removed, a negative impact on society would occur. Some examples include:
    - Agriculture & food
    - Banking & financial services
    - Chemicals
    - Commercial facilities

Protecting Critical Infrastructure:

- In order to protect critical infrastructure, you need to treat it importantly **EX**: You can't protect critical infrastructure with the same tools you use to protect your PC at home (basic firewalls, AV scans, etc).
- 1 way is **Situational Awareness** which is where you are always aware of new threats & vulnerabilities as well as existing ones.
- The other way is **Introducing Diversity** to the ecosystem, this includes having different operating system applications & different operating systems, having different geographic regions & network technologies because if someone attacks 1 piece of infrastructure or equipment, it won't easily cascade across & flow into the differnet infrastructure components. Most executives in an organization are tough on not having diversity since it introduces a higher cost.

Mobile Security

Architecture:

Includes:

- ▪ Mobile devices
- ▪ Device management
- ▪ Operating System
- ▪ Mobility infrastructure (wifi, 4g, 5g, etc)
- ▪ Applications

Mobile Device Management:

• Previously, we had to keep PCs in check but now we're in an era where most businesses keep mobile devices in check due to people working more off them now (tablets, phones, etc). Keeping these devices “in check” refers to keeping track of these devices, ensuring updates are performed, etc.
• In terms of ISPs for mobile devices, one of the main concerns would be jamming or DoS attacks. But since we are very dependent on these services, long term outages would surely not be tolerated.
• We also have the app store (both Google Play & Apple) where users can upload their own apps freely, its arguable that Apple's app review of updates & new apps is more scrutinizing than Google's as seen with previous cases.

IMSI Catching

IMSI Catching:

- AKA **Individual Mobile Subscriber ID**
- In early generations of mobile, the handset would connect to towers & authentication wasn't considered until the 2nd generation but even in the 2nd generation only the tower authenticated the handset but the reverse wasn't done so the mobile device didn't authenticate the tower which means anyone can build their own mini tower with a stronger signal (since the mobile devices are programmed to connect to the tower providing the strongest signal) & place it somewhere.
- With 3G though, the tower would be authenticated by the mobile device! But sadly enough, since devices connected to the strongest signal, if there were no 3G capable towers & a device was forced to connect to a lower generation, then the mobile device wouldn't be able to authenticate the tower due to it having to downgrade to the lower 2g or lower generation for signal.
- Obviously with 3G and up, mobile devices always authenticate the tower they're connecting to.

IoT Security

IoT Security Categories:

1. Industrial Control Systems/Devices
- These are devices that have consequences, if hacked, to some critical infrastructure component. Can be considered critical infrastructure as well.

2. IoT Consumer items
- Fridges, video recorders, watches, basically anything else that's internet connected & things that if hacked, wouldn't have negative consequences to critical infrastructure.

- In between these 2 categories, we also have things such as medical devices that are connected to the Internet, these devices aren't exactly ICSes but if they are hacked, they can have negative consequences but the consequences wouldn't cascade like they would with an ICS & the negative consequences wouldn't be as large as they would with critical infrastructure.

IoT Issues:

- Legacy Devices (where security is not natively embedded)
- Protocol (Proprietary protocols are used in many of these IoT devices)

Security Through Obscurity

Security Through Obscurity:

- In cryptography, this means making your algorithm more secure by not telling anyone what the algorithm is & hoping people don't find out. This also leaks out to software where certain vendors don't open-source their software (instead, they make their software proprietary where the code is secret) in order to keep it more “secure” because the vendor believes that if the code is kept secret, vulnerabilities will not be found which is generally true but it's better for them to be found by the community so it can be reported & fixed. But of course there are sides of the community that won't report them & be malicious.
- Generally not a great idea.

Definition of a Firewall

Definition of a Firewall:

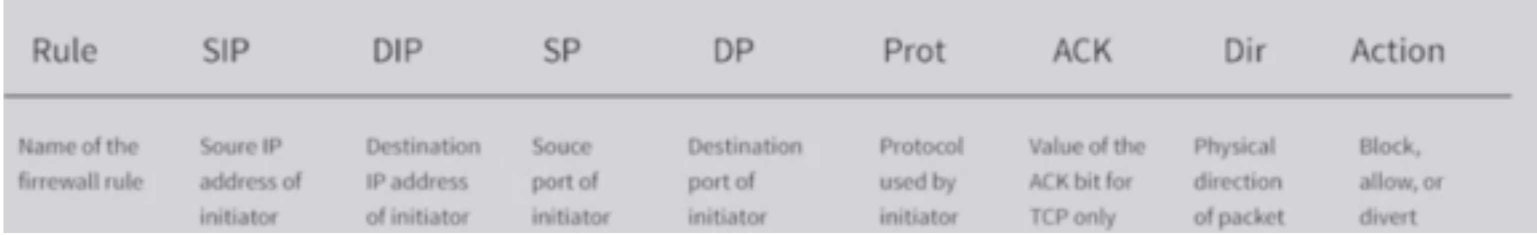
1. Separates 2 or more networks
2. Enforces network security policies (what it lets through & what it doesn't let through; firewall rules)
3. Administered by a network administrator
4. Cannot be tampered with
5. Cannot be bypassed

Stateful vs Stateless Firewalls:

- **Stateful Firewall -** Remembers info between states, context-sensitive, more powerful than stateless. Stateful firewalls can identify unauthorized & forged communications & are also aware of communication paths & can implement various IP security functions (tunneling & encryption)
- **Stateless Firewall** - Doesn't remember info between states, context-free, less powerful than stateful. Stateless firewalls usually have a rule set guiding it in what to do
- A fun way to think of these is a stateless firewall is like an employee who needs to be told step by step what to do while stateful firewalls are the employee who learns quickly what to do and remembers procedures

Firewall/Router Packet Filtering

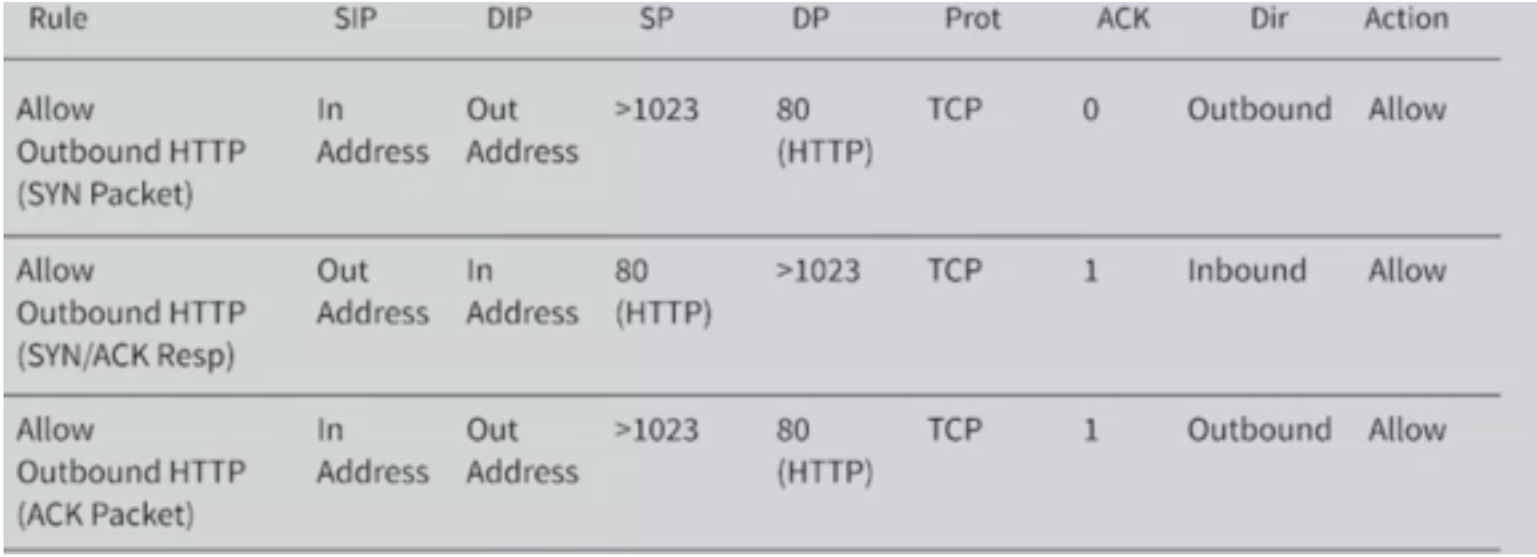
Firewall/Router Packet Filtering:



Rule	SIP	DIP	SP	DP	Prot	ACK	Dir	Action
Name of the firrewall rule	Soure IP address of initiator	Destination IP address of initiator	Souce port of initiator	Destination port of initiator	Protocol used by initiator	Value of the ACK bit for TCP only	Physical direction of packet	Block, allow, or divert

- **Dir** = Physical direction in terms of inbound or outbound traffic (inbound is normally trusted, outbound is normally untrusted)
- Any packet that's leaving the internal network is called **outbound** while any packet that is coming from the external network to the internal is called **inbound**. This is the directions available.

Firewall Rule Allowing Outbound Web Browsing



Rule	SIP	DIP	SP	DP	Prot	ACK	Dir	Action
Allow Outbound HTTP (SYN Packet)	In Address	Out Address	>1023	80 (HTTP)	TCP	0	Outbound	Allow
Allow Outbound HTTP (SYN/ACK Resp)	Out Address	In Address	80 (HTTP)	>1023	TCP	1	Inbound	Allow
Allow Outbound HTTP (ACK Packet)	In Address	Out Address	>1023	80 (HTTP)	TCP	1	Outbound	Allow

- The ACK bit being 0 is due to it being the first SYN packet (to initialize/synchronize the connection)
- This rule allows internal IPs to send traffic out to the external network to port 80 for HTTP web servers in order to connect, you could also enable the DP to be port 443 for secure connections.

Management by Exception

Management by Exception:

• Management by exception is the concept of watching the network's behavior (whether it be on a weekly, daily, or monthly basis) & you keep track of what's normal & build a profile of what's normal
• With management by exception, if there are any changes from what's considered normal, there may be an attack or something going wrong.
• Management by exception is useful when signatures are being used to detect attacks, when signatures cannot be used, & when real time protection of a network is required.
• Management by exception can also be considered heuristic based detection.

Auditing:

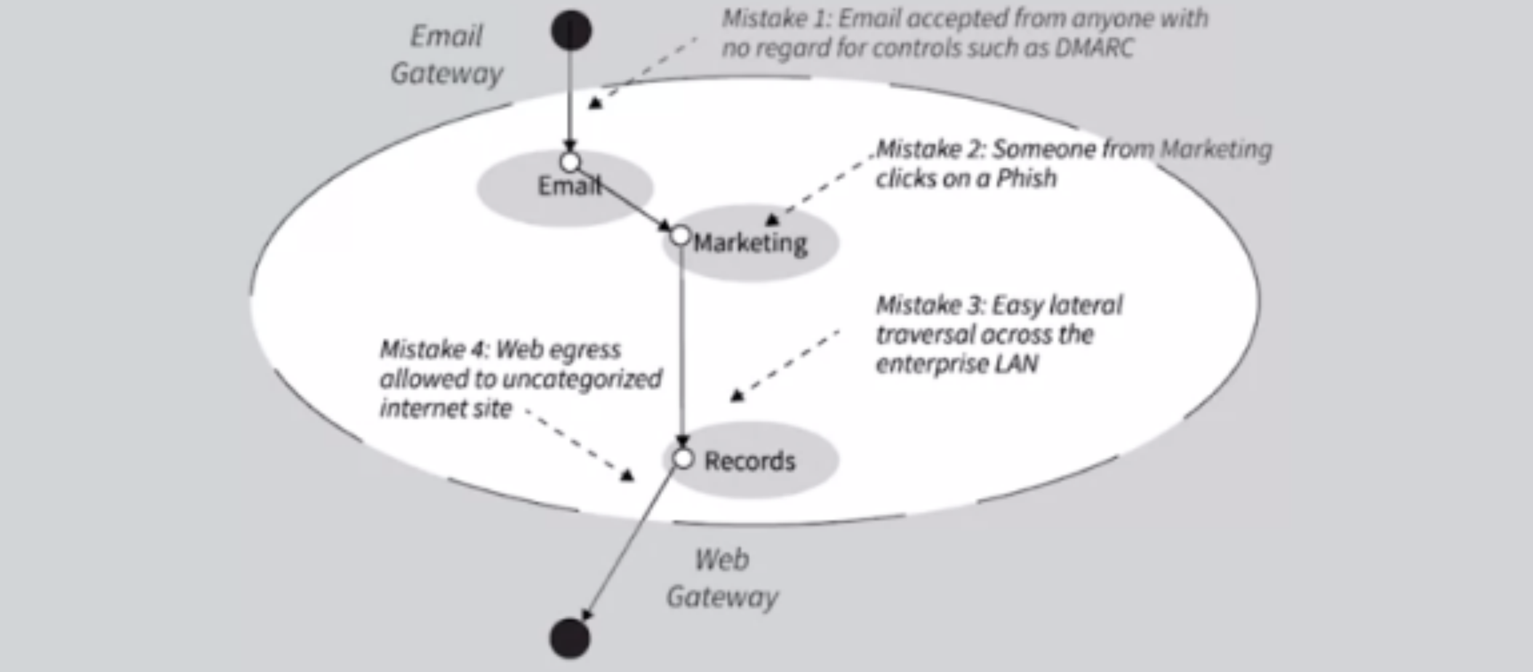
- Auditing can either be **internal** or **external**
- **Internal Auditing** generates/collects data logs natively, from the inside and collects log files this way
- **External Auditing** uses outside systems to collect data
- If you buy something that doesn't have an auditing capability with it, you're forced to do it externally. But most operating systems do indeed generate log files of activity so technically it is done internally.

3 Levels Where Auditing Is Performed:

- **Application level** - This level can relate to things such as your browser, which generates a browsing history, it's an application level internally generated component that gives indication on the behavior of the application.
- **System Level** - Think of operating system, or the kernal. This includes internally generated log files, & if the OS doesn't automatically generate log files then you have to find something that provides logging capabilities (note this would be considered external logging if your OS doesn't automatically have logging capabilities).
- **Network Level** - At the network level, you want to have an understanding of how the network “normally” performs, you do this by building a profile. This is basically management by exception. External auditing of a nework is more common than an internal method of generating audit logs.

APT Through Perimeter Holes

APT Through Perimeter Holes:


Email Gateway
Mistake 1: Email accepted from anyone with no regard for controls such as DMARC
Email
Mistake 2: Someone from Marketing clicks on a Phish
Marketing
Mistake 3: Easy lateral traversal across the enterprise LAN
Mistake 4: Web egress allowed to uncategorized internet site
Records
Web Gateway

- The holes or openings in this server are there due to the different services offered by the company, things such as web gateways, email gateways, etc provide holes in the network that can be attached through attacks such as phishing, watering hole attacks, etc)

Mistakes That Lead To Attacks:

1. The first mistake is the email gateway allowing email from everyone, there can be an argument that if email wasn't allowed to come from everyone then how would customers/clients communicate w/the organization. Fair. But the email gateway can have the DMARC (or Domain-based Message Authentication, Reporting & Conformance) protocol which is a protocol that checks if the email is from who it really claims to be. It grabs the from header and checks the IP address & compares it to the IP address of the mail server of that from header (**EX**: If an email claims to be coming from paypal.com, DMARC would check the IP of paypal's mail server then compare it to the IP of the email to confirm)
2. The second mistake is someone from marketing clicking on the link in the phishing email, this can be for many reasons. The phishing attack could've been a spearphish attack targeting that specific person.
3. The 3rd mistake is that the internal network is easy to laterally move in, meaning, the computers trust each other & you can easily see what other devices are in the network due to lack of firewalls between the nodes/devices.
4. Mistake 4 would be that the organization allows the internal network to access resources on the internet which is an advantage for the attacker, this makes it not only so phishing attacks could be successful but also for attackers to be able to exfiltrate data to their own domains. In a perfect world, the organization would have a forward proxy for internal users to connect to before going out to the internet and this proxy would check the site that's attempting to be visited against a list of sites that are deemed inappropriate or malicious and if the site isn't on that list, it allows the user to go. Obviously, this is still flawed through watering hole attacks but it's better than not having it.

Third Party Security

Third Party Security:

- The first party is you and your business
- The second party is your customers
- The third party is there to support the customers & is hired by the first party
- Third parties typically have special access to the first party's network which can result in major damage to the first party if the third party is hacked.
- If the third party is compromised and it has access to the first party's network, the attacker can then move move into the first party's network and move laterally throughout it if the first party doesn't have any type of internal security that separates parts of the internal networks (**EX**: Having firewalls that separate different servers & LANs that house different types of data). Of course if the third party is able to move laterally throughout the network without any type of authentication or anything of that nature, it does fall on the first party for not implementing adequate security.
- Third parties are the source of all types of attacks, including the major Target breach.

Layer 7 Application Level DDOS Risk

Layer 7 Application Level DDOS:

- This is an attack where a server is sitting in a network or hosting center where an attacker would want to cause problems for the hosting center or network. The server would be hosting things that any individual can download for free & a botnet would then request a bunch of downloads which would overload the bandwidth of the network & the ISP wouldn't see any of it as it seems like normal traffic so the ISP cannot be of any assistance to this DDOS.
- Application level DDOS attacks would be able to surpass DDOS scrubbing due to it looking like normal traffic.