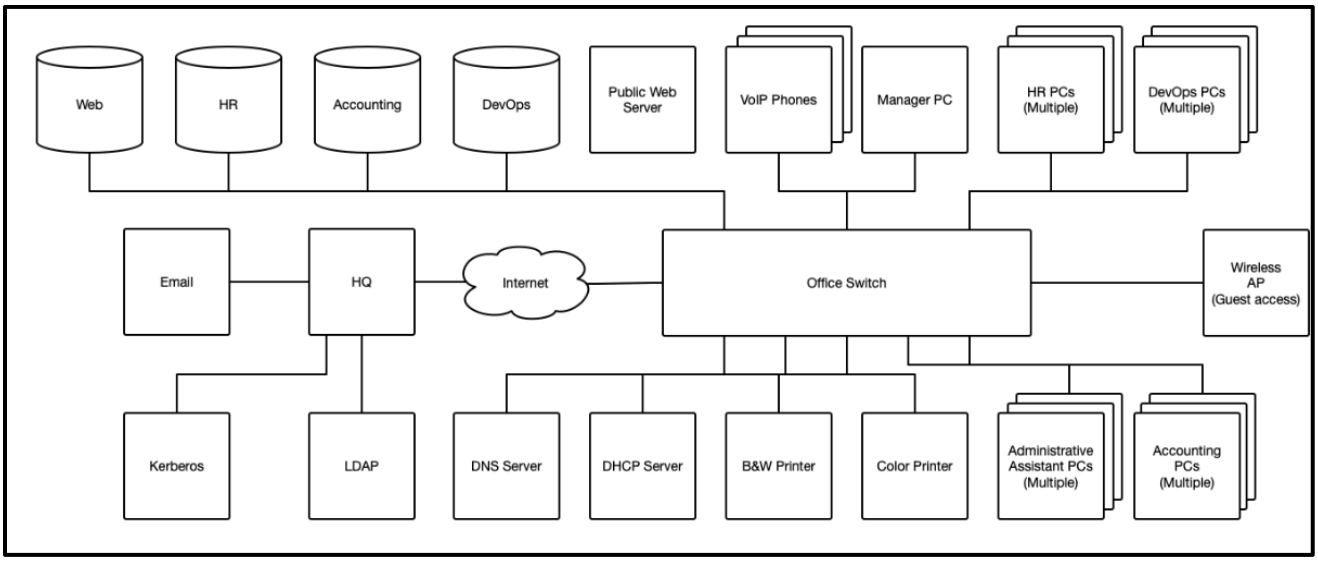
ITIS 6010-Cyber Defense

FINAL GRADUATE REPORT

Group Members: Shail Sandip Patel, Ruchira Pokhriyal, Sneha Rangari

Current network architecture:



- **Evaluate the current architecture from an IT security perspective. What are the strengths and weaknesses of the current setup?**

Security Flaws/ Weaknesses of The Current Architecture:

There aren't any internal and external firewalls present in this architecture, this major security flaw would permit all the data packets to enter and exit the network unrestricted. This includes not just expected traffic, but also malicious data, thereby putting the network at risk. This gives rise to several internal and external threats.

Internal threats:

- **Malware:** This includes viruses, trojan horses, worms, spyware/adware, phishing and pharming.
- **Spyware/adware:** These malicious entities gather information about you. It can record keystrokes and, as such, can potentially be very dangerous, revealing everything you do on your computer.
- **Unauthorized Access:** None or weak authentication schemes can lead to unauthorized access to systems containing sensitive data. This is a major security flaw. and the way to deal with this is to have proper authentication procedures in place, for both local and remote access.
- **Weak Password Protection Schemes:** In many cases, employees do not follow strong password policies which leads to their systems being compromised. Also, just password protection to a system is not enough to prevent it against several other security breaches.

- **Data Theft or Leakage:** Further potential problems are from data theft or leakage, for example when a laptop is stolen. The answer here is to encrypt all sensitive data. Low cost solutions are available from companies such as Utimaco.
- **VoIP attacks** are possible in the current network architecture.
- **Shared Access:** We can see that shared access is granted to multiple to administrative PCs which is a violation of Non-Repudiation.
- **Absence of VPN for remote access:** Because VPN is not present in the current architecture, the organization's data can easily get to the hands of third parties, an entity's identity and location gets exposed, Imposters can steal the data in a matter of seconds.
- **No segregation of Duties:** There is just one core switch present in the current architecture. This is bad security practice as the entire network will collapse if something happens to the core switch.

External Threats:

If an unauthorized entity manages to get into the system, the security is obviously compromised. Several of the below mentioned external attacks can compromise the current network architecture:

- **Man-In-The-Middle Attack:**
  All the administrative PCs and other devices like switches and databases are connected to each other without any preventive "filter" of some sort between them. In this case, it's very easy for a MITM attack to take place. Man-in-the-middle attacks are cybersecurity attacks that allow the attacker to eavesdrop on communication between two targets. It can listen and possibly alter to a communication which should, in normal settings, be private.

Some of the types of possible MITM attacks in the current network architecture:

→DNS spoofing
→HTTPS spoofing
→IP spoofing
→ARP spoofing
→SSL hijacking
→Wi-Fi hacking

- **Phishing:**

Since no visible email authentication mechanism can be identified in the current architecture, it could be safely said that the current architecture is susceptible to Phishing attacks. Phishing is about fake emails trying to extract sensitive information, such as bank passwords or credit card details and a variation of this is pharming, where the criminal sets up a fake web site which looks like one you normally use. Once a member of the said organization fails to notice a phishing email and enters his/her or the organization's personal details, the adversary would be is able to plunder the organizations sensitive information.

- **DDoS Attack:** Another danger to the current network is from a DDoS (distributed denial of service) attack. This is a malicious attempt to prevent an organization being able to use its Internet based systems by flooding them with emails until the servers are overwhelmed.

- In the current architecture, since there is no protection to the VLANs, there is a possibility of attacks such as MAC Attack, ARP attack etc., on the VLAN as well.

Strengths of the current architecture:

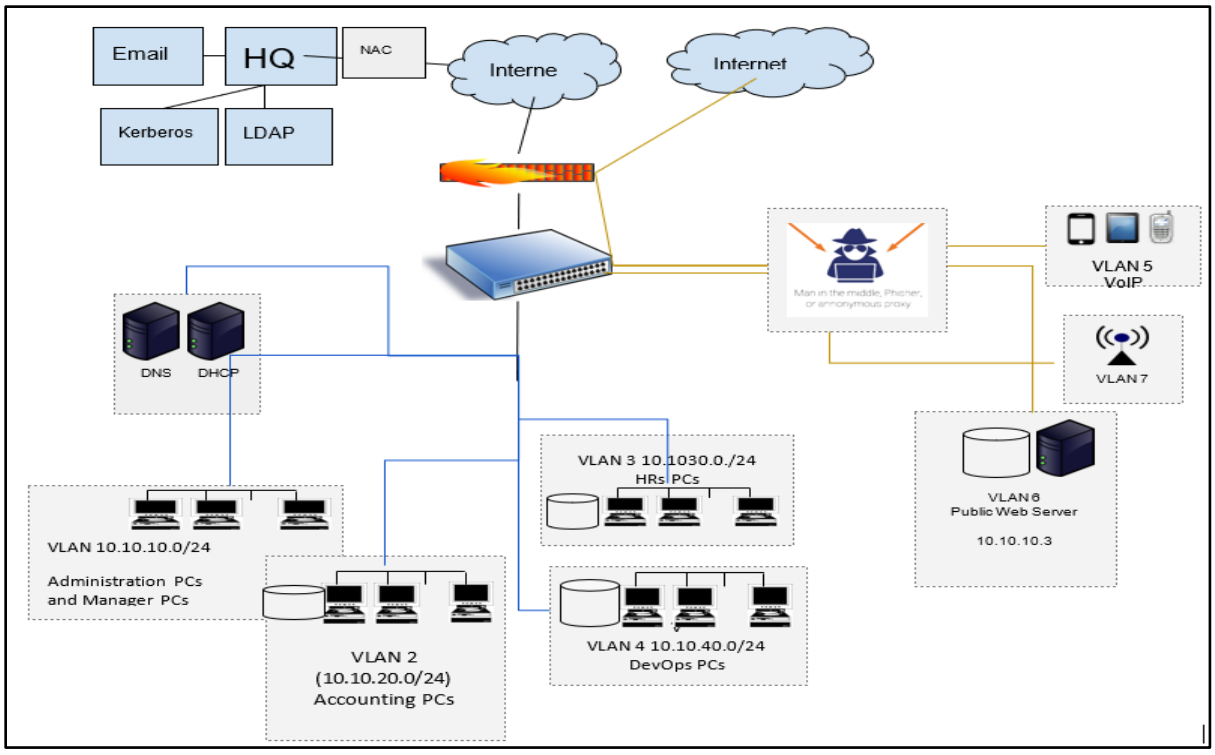
- Implementation of Sigle Sign-on can be seen with the presence of Kerberos and LDAP.
- Proper segmentation of servers such as: Web Server, HR, Accounting and DevOps.

Possible Security Improvements:

- Setting up internal and external firewalls.
- Implementation of host-based firewall rules to restrict communications
- Making sure that there's updated antivirus/antimalware software present on every machine.
- Implementation of IDS/ IPS for external threats
- Any known vulnerabilities should be patched soonest.
- Setting up email authentication schemes such as SPF, DKIM, and DMARC.
- Enforcing safe password practices, meaning that ensuring passwords are salted and hashed as well as that they are changed on a timely basis.
- Ensuring that data is backed up regularly to prevent potential loss in case of system failure or ransomware attacks.
- Limiting unnecessary lateral communications.
- Hardening of all the network devices.
- Securing access to infrastructure devices.
- Performing Out-of-Band network management.
- Validating integrity of hardware and software.
- Implementing multi-factor authentication to protect against security breaches. Use of strong authentication with tokens provides much better security.
- Applying encryption to all the management channels—database encryption, encryption of all the communications.
- Implementing VLAN Access Control List (VACL) to control access to and from VLANs.
- Application of DLP (Data Leakage Prevention) for detecting and preventing data breaches, exfiltration, or unwanted destruction of sensitive data in the current network through Emails, USB cords or online drives.

- Design a new security architecture for the network that addresses the possibility of a remote attacker and also an attacker that might social engineer their way into the office and connect their laptop to the network. Be detailed in how you describe the architecture. What subnets/VLANs/services/configurations/etc. are required? Diagrams will be helpful in doing this.

Network Architecture Prone to Remote and Social Engineering Attacks:



Possible Remote and Social Engineering Attacks:

As mentioned earlier, there isn't any visible email authentication or encryption policies in place which makes the given network architecture prone to several remote attacks as well as social engineering attacks. Here we describe few of the possible remote and social engineering attacks and how we could prevent these from taking place.

Phishing:

A phishing attack is the most common social engineering attacks that is the cause of fall-down of several large organization. Below are the following ways in which phishing attacks can affect the given network architecture:

- Embedding a link in an email that redirects an employee to an unsecure website that requests sensitive information.
- Installing a Trojan via a malicious email attachment or ad which will allow the intruder to exploit loopholes and obtain sensitive information of employees and organization.

- Spoofing the sender address in an email to appear as a reputable source and request sensitive information.
- Attempting to obtain company information over the phone by impersonating a known company vendor or IT department.

Preventive Measures against Phishing:

- Educating employees and conduct training sessions with mock phishing scenarios.
- Deploying a SPAM filter that detects viruses, blank senders, etc.
- Keep all systems current with the latest security patches and updates.
- Install an antivirus solution, schedule signature updates, and monitor the antivirus status on all equipment.
- Develop a security policy that includes but isn't limited to password expiration and complexity.
- Deploy a web filter to block malicious websites.
- Encrypt all sensitive company information.
- Convert HTML email into text only email messages or disable HTML email messages.
- Require encryption for employees that are telecommuting.

VLAN Hopping attack:

As you can see in the above diagram we have implemented VLANs for security segregation-to filter communication between systems on the network, to limit and effectively broadcast traffic, thereby improving bandwidth, and for limiting MAC address counts since most of the switches can handle a limited number of MAC addresses. However still, a VLAN hopping attack is possible in the current architecture.

VLAN hopping is a method of attacking a network by sending packets to a port that is not normally accessible from a given end system. There are two primary methods of VLAN hopping: **switch spoofing** and **double tagging**.

Preventive Measures:

To make switch **spoofing impossible**, one can can disable “trunking” on all ports that do not need to form trunks. Furthermore, one needs to disable DTP on ports that do need to be trunks.

Disabling Trunking:

Switch1(config)# interface gigabitethernet 0/3

Switch1(config-if)# switchport mode access

Switch1(config-if)# exit

Preventing the Use of DTP:

Switch1(config)# interface gigabitethernet 0/4

Switch1(config-if)# switchport trunk encapsulation dot1q

Switch1(config-if)# switchport mode trunk

Switch1(config-if)# switch port nonegotiate

MITM Attack

As seen, we have a wireless access point in our network design, and most MITM attacks thrive on Wi-Fi connections. In our current network architecture, an adversary can set up a Wi-Fi connection with a legitimate-sounding name which can be easily trusted by the employees of the organization. Now the attacker just has wait for someone to connect to this access point and once that is done, the attacker will instantly gain access to the connected device. The attacker can also create a fake Wi-Fi node disguised as a legitimate Wi-Fi access point (Evil Twin Attack) to stealthily capture all the personal information of people who connect to this access point.

Preventive Measures:

We could implement Certificate-Based authentication for all employee machines and devices to prevent against MITM attacks. With this implemented, only the endpoints with properly configured certificates can access the networks and systems. This approach would save additional hardware requirements and user training too.
Additionally, implementation of VPNs will help in creating a secure environment for sensitive information within a LAN. VPNs make use of key-based encryption to create a subnet for secure communication. So, even if an adversary happens to get on a shared network, he will not be able to decipher the traffic in VPN.

One thing to consider is that because this is a branch office, some services must be accessed from the headquarters. Identify potential solutions for ensuring that these services are protected, and the data being exchanged between the HQ and the branch office are not compromised.

1. **Managing branch networks**: These may include firewall, VPN, IPS, web and email protection. IT management, implementation or upgrade can be costly when dealing with multiple offices, yet safety for data housed remotely is just as important as that of information residing at headquarters.

2. **Thin client security**:
   In lieu of firewall, VPN, IPS, web and email security running together on a costly branch office device, all functions can be routed via a command center. This hub is able to reside in the corporate office or in the cloud. The “thin client" approach to security allows for a remote device to be placed within the branch office. Traffic is directed to the central device where it’s scanned, filtered and then released to the internet.

3. **IT policies**:
   Internet usage policies should be a major focus, as bandwidth at local offices may be spotty. Branch locations are usually smaller; therefore, the internet connection will be smaller as well. There may even be just one solitary on-site network connection. Rules regarding site access and non-work related "surfing" will have to be more stringent to ensure that bandwidth is being utilized for business purposes only. Freeing up bandwidth guarantees the central IT team is able to support users properly. Additionally, how employees operate on the network will determine if a company is increasing their risk of a data breach. Workers should be well educated on the use of social media, storage solutions and how their online presence effects the company overall.

New and Secured Network Architecture: