Final Report

ITIS 4246-091

Jake Treese

Observations

My first observation is that there is no information about what type of security policies the Office Switch has. Network switches themselves most commonly have little to no security by default. There are also no designated subnets in the diagram. So, since the Office Switch has little to no security, I can also assume that it is possible for all devices to see or communicate with each other. This poses an obvious backdoor security risk.

For specific items I see as issues:

- The VoIP Phones should not be connected to the Manager PC since calls made outside of the infrastructure can be hacked and used to gain administrative access.
- All the servers should not be directly connected. While it may be easier from a DB configuration standpoint, it opens them up to all being compromised.
- Guest Access should not be connected to the Office Switch at all.
- The printers should not be on the same connections as the DNS and DHCP servers. This opens servers to attacks by using the printers.
- The Accounting, HR, DevOps, Admin Assistant, and Accounting PCs should all be separate connections or subnets. It may be harder to implement, but the chance of someone in HR or Accounting getting compromised is probably higher than DevOps or Admin Assistants.
- There should also be security on the Office Switch side of the Internet connection as well.
- There are no firewalls or any other security measures on the office side.

The main tasks needing to take place are:

1. Remove all backdoor connections
2. Replace the current Office Switch with an AAA server cluster

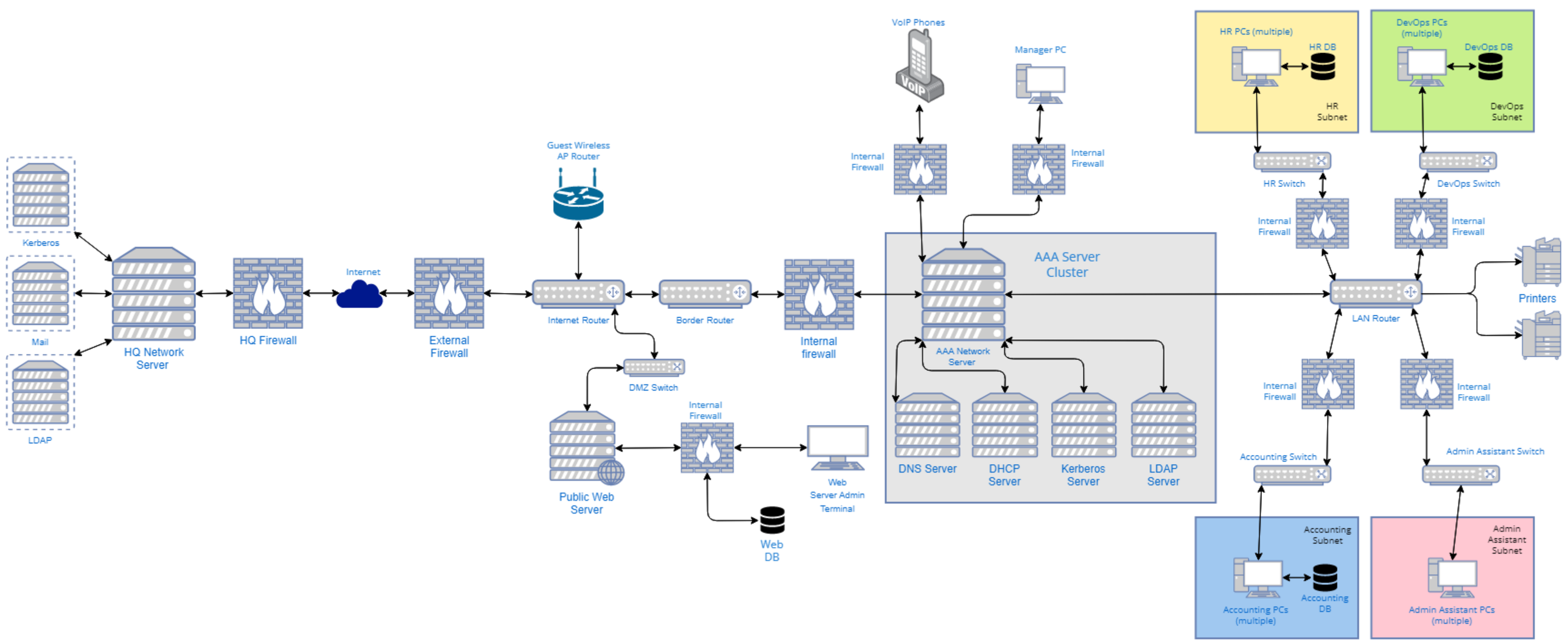
3. Make sure devices with multiple network interfaces are at the same security level
4. Implement subnets with intermediary devices that provide extra security and access control
5. Implement a network perimeter device filter traffic
6. Update all software, verify file integrity, and set up a scan schedule
7. Configure port security on the switches
8. Configure the permissions and authorization for each subnet
9. Set up a completely separate Guest Wi-Fi access point
10. Ensure DBs are properly configured to prevent injection or corruption of data
11. Get a good, secure company to set up VoIP and connect it through a firewall to the AAA cluster
12. Set up firewalls between all internet and intranet switches

For the strengths:

- The system seems like it would be very easy to manage. If everything is connected under one switch, it would be simple to view.
- It is most likely fast and convenient. Since many of the devices are connected on the same lines and they all flow through one switch, then there is most likely little delay from one to another.
- The HQ setup seems to be relatively safe. There should probably be more than just LDAP and Kerberos, but it is a good start.

The biggest problem with the original network was the distinct lack of authentication, filtering, and subnets. I created a prototype network topology diagram and have included it below. Following the diagram, I will explain my thoughts on the design and how I would go about implementing it.

Topology Diagram


Kerberos
Mail
LDAP
HQ Network Server
HQ Firewall
Internet
External Firewall
Guest Wireless AP Router
Internet Router
Border Router
Internal firewall
DMZ Switch
Public Web Server
Internal Firewall
Web DB
Web Server Admin Terminal
VoIP Phones
Internal Firewall
Manager PC
Internal Firewall
AAA Server Cluster
AAA Network Server
DNS Server
DHCP Server
Kerberos Server
LDAP Server
HR PCs (multiple)
HR DB
HR Subnet
DevOps PCs (multiple)
DevOps DB
DevOps Subnet
HR Switch
DevOps Switch
Internal Firewall
Internal Firewall
LAN Router
Printers
Internal Firewall
Internal Firewall
Accounting Switch
Admin Assistant Switch
Accounting Subnet
Accounting PCs (multiple)
Accounting DB
Admin Assistant Subnet
Admin Assistant PCs (multiple)

Explanation

I will split this explanation into parts for each section: AAA Server Cluster, Subnet and Intranet, DMZ, and Routing/Firewalls. I will explain what each part does and what implementations will be used in my network topology.

AAA Server Cluster

An AAA server is a service that handles requests for access and provides authentication, authorization, and accounting services. Most commonly these are run in clusters using servers for each part of the AAA schema. In my topology I am using a RADIUS network server as the main AAA access point along with the logging, LDAP for extra authentication, and Kerberos for authorization to use and access services.

- **AAA Server**: This stores user credentials, group information, passwords, usernames, and sometimes other items like hashes or keys. When trying to access a service going through the AAA server the user is led to a to log in page. They must log in with valid credentials before they get access to the network. For this topology, I have chosen to make a network server the main AAA server. This allows for data to flow in through a secure point which is easily monitored and has robust filtering. The filters would mainly be focused on keeping all subnets and other devices separate since the firewalls will handle internet traffic. This way if there was a security breach, it could be quickly contained before it spread.

- **LDAP Server:** The AAA server sends received log in attempts to the LDAP server. The LDAP server checks to see if the credentials are valid and if this user has permissions to access what they are requesting. If they do, it will send a confirmation back to the AAA server. If not, it will deny access and send an alert to the IT manager. In this case, LDAP is simply running on the network server, but it is technically a virtual server. The employees would all make usernames and passwords during the setup, and then the LDAP server would be populated with them and their permissions/access level.

- **Kerberos Server:** The Kerberos server (or KRB as I will call it) verifies the credentials your user profile has and gives you a ticket. This ticket will allow the user to access whatever services they have permission to. In my network I am taking the principle of least privilege. Every user will have the lowest level privilege to perform their tasks. If they need higher then they will be prompted to put in their higher privilege credentials, which will go through the AAA server process again.

- **DNS and DHCP:** These servers will provide the DNS and DHCP functionality to the network. They will be run through the network server so all subnets and devices can function properly on the network. They will be protected and require admin level privilege to access anything relating to viewing or changing the information.

I chose this type of centralized server structure because of my experience working with the US government. They use this type of verification with many redundancies and the least privilege principle to prevent data breaches and unauthorized access. This is substantially safer than the direct switch/router connection to the internet as well as peer-to-peer connections on the original diagram. This would also allow for greater growth should the office expand. I would suggest using the Pulse Secure access management framework which will allow for the easiest setup with the ability to perform AAA tasks efficiently.

Subnets and Routing

In the original topology, there were no subnets or servers capable of running an intranet. On top of this, all the devices were connected to each other via an office switch. Subnets are an integral part of a secure network. It allows like machines to be grouped with like and for the separation of data to prevent backdooring and eliminate peer-to-peer hacking. I decided to implement 4 subnets based on the databases and PC groups. I included the databases with their respective PCs and ran the access of the subnet through a switch and internal firewall. These firewalls would filter out any traffic attempting to access the PCs or databases. This includes other subnets and devices on the network. This is to prevent a compromised device on one subnet from infecting or breaching other subnets. The switches would be connected to the LAN

Router. The LAN router would have separate ethernet connections and filters to prevent any bleeding of information. The router has a path to the AAA network server to verify the credentials of the users and to allow internet access. The router would also have a one-way connection to the printers, meaning if the printer was compromised, it would have no route to send information or access any other information. This would prevent hijacking or piggybacking. The other devices connecting to the network server are important as well. The VoIP phones should have an internal firewall between them and the network server. This will mitigate VoIP hacking attempts. The Manager PC should be separate from the rest of the subnets, but have the ability to, with Kerberos, access all the subnets if need be. This PC will be behind not only a strict internal firewall with a deny-by-default ruleset, but also four layers of authentication. First the operating system credentials, then the AAA credentials, followed by the Kerberos tickets, and finally the privileged user credentials. These are four different forms of authentication and authorization to prevent any unwanted access. Even on the subnets, three forms of authentication are required to access and move within them. This, while redundant, makes it much harder for a hacker to gain entry.

DMZ

Another problem with the original topology was the public webserver, web database, and the wireless guest AP. These all had no security and were, with the exception of the webserver, on the same network as every other device. I chose to implement a DMZ to prevent attacks and cordon off any sensitive data. The DMZ is a small zone between the ISP router and the border router that handles all internet communications on the webserver and guest access point. The ISP router is connected to a DMZ switch which will filter requests and data to prevent unauthorized access to the web server. This is all behind the external firewall which is already filtering the broad threats. The webserver can retrieve or store data to the web DB which is behind another internal firewall. The webserver and its DB need to be configured to prevent injection and other SQL attacks. I also added another device, that being the web server admin terminal. This is connected, through a firewall, to the public web server and web DB to allow for scanning, DB maintenance, and software updates to be performed. This terminal is not

connected to the main network in the event that a breach occurs. The DMZ also includes the guest access router. This router is connected directly to the ISP router and should be configured to only have access to the internet. The border router is there to ensure no unauthorized access is allowed from the guest AP, webserver, or internet at large. It also tells the network where the intranet ends. This router is connected to the AAA server through an internal firewall as well.

Routing and Firewalls

In the given diagram there were no routers or designated routes for ingress and egress of data. I implemented simple but secure routing in the intranet and from the intranet to the internet itself. I also implemented firewalls between subnets, devices, the intranet, and the internet.

- **Internet Router:** this is the ISP router that allows for access to the internet at large. It has an external firewall configured with basic filters to prevent unauthorized access as well as block access to dangerous or blacklisted ports like Telnet, FTP, and DNS to name a few. It is connected to the public webserver through a DMZ switch. It also is connected with the Wi-Fi guest router to allow internet access.
- **Border Router:** this is the edge of the network. This router tells the rest of the network that past this is the ISP router and therefore it is less safe. I would call my solution a pseudo-border router. It does not cut off all internet connection, but incoming information will be filtered with a deny-by-default policy with exceptions, of course. This is also the place where the internal firewall is implemented. The internal firewall is the same throughout the network, but with different IP addresses based on what lies behind them. In this case, the standard ports are blocked but also IP addresses originating from within the network. This is a clear sign of attempted spoofing since only outgoing data would have IP addresses within the network (the webserver admin terminal is technically not inside the network).
- **Network Server:** all data coming to and from the internet comes through here first. As previously discussed, users without valid credentials will be rejected and IT notified. It also works to allow all the permitted users to access any part of the intranet as a main sort of hub.

- **LAN Router:** this is what handles the subnet switches, printers, and data coming to and from the network server. Each switch is plugged in to its separate port to prevent unwarranted access between subnets. The printers are plugged in to outgoing ports to prevent data coming back. Each of the switches connected to the LAN router are going through a firewall. This firewall only denies any access coming from any device without designated permission to access this subnet. This means any users from DevOps, Accounting, or Admin Assistant cannot connect to any devices in the HR subnet without having the predetermined permissions or by being whitelisted.
- **Printers:** these only have the ability to receive incoming information from the devices on the network. This is so they cannot be compromised and used to attack other devices.
- **HQ Access:** I added a firewall to the HQ, simply because I figured they would already have one and if not, then that's not in my contract. To access the features on the HQ servers I am implementing MTS-STS (again, technically not my job). This allows mail only from connections using TLS 1.2 or 1.3. I also would install the SSL/TLS certificate so that we could receive encrypted mail through ports 993 or 995. We can then send mail using SMTPS on ports 465 or 587 as well. If these certificates are not updated then we may lose access, so regular scanning and updates will be required.

Conclusion

I believe that my network topology is significantly more secure than the given documentation. With the abundant firewalls, least privileged policy, AAA server cluster, and subnets I believe that an attacker would be highly discouraged from attacking this network. The layers of firewalls and filters along with the routing and subnets prevent them from accessing any other part of the network, and if they try then IT will be notified and can respond quickly. The extra devices such as printers cannot be used to attack the network either. Kerberos and the least privilege policy prevent any unauthorized user from gaining increased privilege without credentials and a ticket. If they were to do that the AAA server is logging traffic and would pick up on connections to other ports if they were not already blocked by the three firewalls between them. This whole system is full of redundancies to try and mitigate damage from social engineering. Due to the

firewall on the VoIP and the SSL/TLS on the email server, receiving phishing phone calls or emails is also substantially harder if not impossible. I believe my topology provides a reasonable solution to the problem without being prohibitively expensive or time consuming.