Network Design Project 1

Bryan McKinney

Liberty University

Professor Arthur Salmon

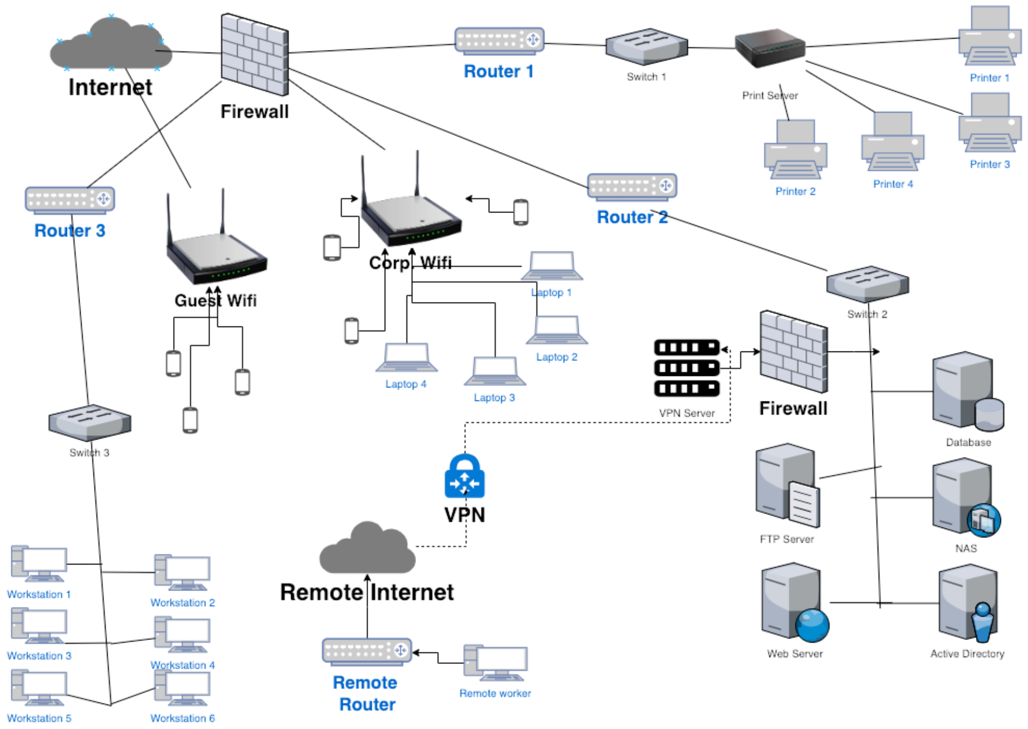
CSCI 601 - Applied Network Security

February 10, 2019

Liberty Beverage Company Overview

The Liberty Beverage Company current network is outdated and is need of a redesign/overhaul. The proposed network diagram (as seen below) will be the new network layout standard for the 2019 fiscal year as well as the foreseeable future with minor upgrades and changes as needed. The current network is no longer meets any modern network standards and there is too much risk involved in keeping the old network. All employees will be trained and about the latest attacks that the Liberty Beverage Company has been facing and how those threats can make the company vulnerable. The following are the current threats to the organization: DOS/DDOS, Worms/Viruses/Trojans/malware, Man in the Middle attacks, Rootkit injections, and security and privacy for mobile devices. For a larger view of the Network layout please see Appendix B.

Liberty Beverages Company Network Layout



Denial of Service (DOS) and Distributed Denial of Service (DDOS) attacks

The Denial of service attack (DOS) is "used to tie up a website's resources so that users who need to access the site cannot do so" (Norton, 2015). There are two ways a DOS attack is carried out. The first way is by "Flooding attacks. Flooding is the more common form DoS attack. It occurs when the attacked system is overwhelmed by large amounts of traffic that the server is unable to handle. The system eventually stops" (Norton, 2015). The second way is by "Crash attacks. Crash attacks occur less often, when cybercriminals transmit bugs that exploit flaws in the targeted system. The result? The system crashes" (Norton, 2015). Each version of the DoS attack can cause great deal of frustration for the end users and the IT professionals in charge of keeping sites and servers up and running. DoS and DDoS attacks are threats because they will knock the server offline that is being targeted keeping end users from being able to access it. This is a vulnerability because depending on what type of server is taken offline there could be important information that is needed. Usually DoS/DDoS attacks are carried out again webservers, but they can be targeted at any server with a known IP address and is accessible to the public internet.

Worms, virus, Trojan horses, and other malware.

There are many different types of vulnerabilities that can make a computer and network open to outside threats. A virus "attaches itself to a program or file so it can spread from one computer to another, leaving infections as it travels. Much like human viruses, computer viruses can range in severity: Some viruses cause only mildly annoying effects while others can damage your hardware, software or files. Almost all viruses are attached to an executable file, which means the virus may exist on your computer, but it cannot infect your computer unless you run or open the malicious program. It is important to note that a virus cannot be spread without a human action" (Symantec, 2019). A worm is "similar to a virus by its design and is considered to be a sub-class of a virus. Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any help from a person. A worm takes advantage of file or information transport features on your system, which allows it to travel unaided. The biggest danger with a worm is its capability to replicate itself on your system" (Symantec, 2019). A Trojan is "not a virus. It is a destructive program that looks as a genuine application. Unlike viruses, Trojan horses do not replicate themselves, but they can be just as destructive. Trojans also open a backdoor entry to your computer which gives malicious users/programs access to your system, allowing confidential and personal information to be theft" (Symantec, 2019).

Man-in-the-middle (MITM) attacks

A Man in the middle attack is "a general term for when a perpetrator positions himself in a conversation between a user and an application—either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway" (Incapsula, 2019). The treat that is profound with Man in the middle attacks is the ability the attacker has to track your online activates and intercept any personal information that you are communicating to the end server. MITM attacks can be avoided by simply not going onto public WIFI connections that have password protection and not using websites that don't include the HTTPS extension as those connections are not secure.

Rootkit injections

A rootkit is "a clandestine computer program designed to provide continued privileged access to a computer while actively hiding its presence" (DuPaul). The threats that can be associated with rootkits and vast and wide. Given backdoor access to any server, computer, or other no specific electronic device is a dangerous place to be. With backdoor access the attacker has not only that component at it mercy they also have the ability to be on the network undetected as detecting rootkits is difficult and no commercial software is available at the moment to track all known rootkits.

Data security/privacy on remote mobile devices

Cell phones have become engrained in our day to day lives. Most people can no long fathom leaving their homes without their cell phone in their pocket waiting for the chance to ignore the world around them and check their phones. While cell phones have a lot of good applications in our lives, they also pose a security threat. One way is by the permissions we give those apps we love to install. "Both Android and iOS allow you to toggle individual permissions, which is great. But since apps can access that information for anything once you permit it, there's no telling what privacy violations apps commit. You might let an app use your microphone to record voice messages, but it's secretly listening to the TV shows you watch to help advertisers build a profile around you. Or apps with access to your contacts could upload them to spam lists" (Stegner, 2018).

Security Threats

If we were to take five different items from the components from above and list how they may be affected from the security attacks that could happen each one of them would react in a slightly different way. For instance, the servers on the network. Depending on the server each one is not limited to just one type of attack. Web servers are vulnerable to Dos/DDos attacks as well as virus, worms, etc. But the desktop computers are not as vulnerable to Dos/DDos attacks like the servers are. But desktop computers are at risk of rootkits being installed, a multitude of viruses and other malware can be installed. All of the devices that are password protected are at risk of their password and security keys being exposed or decrypted. The cell phones are at risk of rootkits and malware that can cause them to share personal information to the attacker and give over vital information. Finally, the VPN system is vulnerable if the person connecting from their home internet is not safe and connects to a public WIFI that isn't encrypted as they can be a victim of a man in the middle attack.

Beyond the network design

I believe that if end users were better educated on the subjects of cyber security and data integrity then many (not all) issues could be mitigated. Education is a great asset to any organization of any size. The more the end users know about security and how their day to day choices can greatly impact the security of the network and their own personal data then I believe many issues that we face as IT professionals will fall to the wayside. If the end users were better equipped to know that opening suspicious emails and then running an EXE from said email was/is/always will be a bad idea that not only effects the company but also can put their own personal information at risk then there should be a slight decrees in exploits like virus's, worms, trojans, etc.

Biblical Principles

While computers weren't around in biblical times the idea of security is not a new concept. In the book of Proverbs, it is written "29 Do not devise harm against your neighbor, while he lives securely beside you. 30 Do not contend with a man without cause, if he has done you no harm." (Proverbs 3:29-30, NASB). We are instructed to live in peace with those around us. Not to bring harm to our neighbors who live "securely" among us. I believe in the given context that we should be looking out for neighbors and not being malicious with the knowledge of cyber security we have. We should not be taking advantage nor setting our neighbors up for fail or harm while they leave in peace with us. We are to not cause any harm to those around us. I find this difficult for people who are on the opposite side of being an ethical hacker. As they are trying to cause harm or disrupt some sort of status quo that everyone has come to know.

References

DuPaul, Neil. RootKit: What is a Rootkit Retrieved from https://www.veracode.com/security/rootkit

Incapsula (2019). Man in the Middle Attack Retrieved from https://www.incapsula.com/web-application-security/man-in-the-middle-mitm.html

Norton (2015). What are Denial of Service (DoS) attacks? DoS attacks explained Retrieved from https://us.norton.com/internetsecurity-emerging-threats-dos-attacks-explained.html

Stegner, Ben (24, July 2018). 7 Shifty Ways your Smartphone is violating your privacy Retrieved from https://www.makeuseof.com/tag/phone-privacy/

Symantec (2019). The Difference Between a Virus, Worm and Trojan Horse Retrieved from https://www.websecurity.symantec.com/security-topics/difference-between-virus-worm-and-trojan-horse

Appendix A

Wireless Communication Standard

Last Update Status: *Updated February 2019*

1. Overview

See Purpose.

2. Purpose

This standard specifies the technical requirements that wireless infrastructure devices must satisfy to connect to a Liberty Beverage Company network. Only those wireless infrastructure devices that meet the requirements specified in this standard or are granted an exception by the InfoSec Team are approved for connectivity to a Liberty Beverage Company network.

Network devices including, but not limited to, hubs, routers, switches, firewalls, remote access devices, modems, or wireless access points, must be installed, supported, and maintained by an Information Security (Infosec) approved support organization.

3. Scope

All employees, contractors, consultants, temporary and other workers at Liberty Beverage Company and its subsidiaries, including all personnel that maintain a wireless infrastructure device on behalf of Liberty Beverage Company, must comply with this standard. This standard applies to wireless devices that make a connection the network and all wireless infrastructure devices that provide wireless connectivity to the network.

Infosec must approve exceptions to this standard in advance.

4. Standard

4.1 General Requirements

All wireless infrastructure devices that connect to a Liberty Beverage Company network or provide access to Liberty Beverage Company Confidential, Liberty Beverage Company Highly Confidential, or Liberty Beverage Company Restricted information must:

- Use Extensible Authentication Protocol-Fast Authentication via Secure Tunneling (EAP-FAST), Protected Extensible Authentication Protocol (PEAP), or Extensible Authentication Protocol-Translation Layer Security (EAP-TLS) as the authentication protocol.
- Use Temporal Key Integrity Protocol (TKIP) or Advanced Encryption System (AES) protocols with a minimum key length of 128 bits.
- All Bluetooth devices must use Secure Simple Pairing with encryption enabled.

4.2 Lab and Isolated Wireless Device Requirements

- Lab device Service Set Identifier (SSID) must be different from Liberty Beverage Company production device SSID.
- Broadcast of lab device SSID must be disabled.

4.3 Home Wireless Device Requirements

All home wireless infrastructure devices that provide direct access to a Liberty Beverage Company network, such as those behind Enterprise Teleworker (ECT) or hardware VPN, must adhere to the following:

- Enable WiFi Protected Access Pre-shared Key (WPA-PSK), EAP-FAST, PEAP, or EAP-TLS
- When enabling WPA-PSK, configure a complex shared secret key (at least 20 characters) on the wireless client and the wireless access point
- Disable broadcast of SSID
- Change the default SSID name
- Change the default login and password

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Related Standards, Policies and Processes

- Lab Security Policy

7 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at: https://www.sans.org/security-resources/glossary-of-terms/

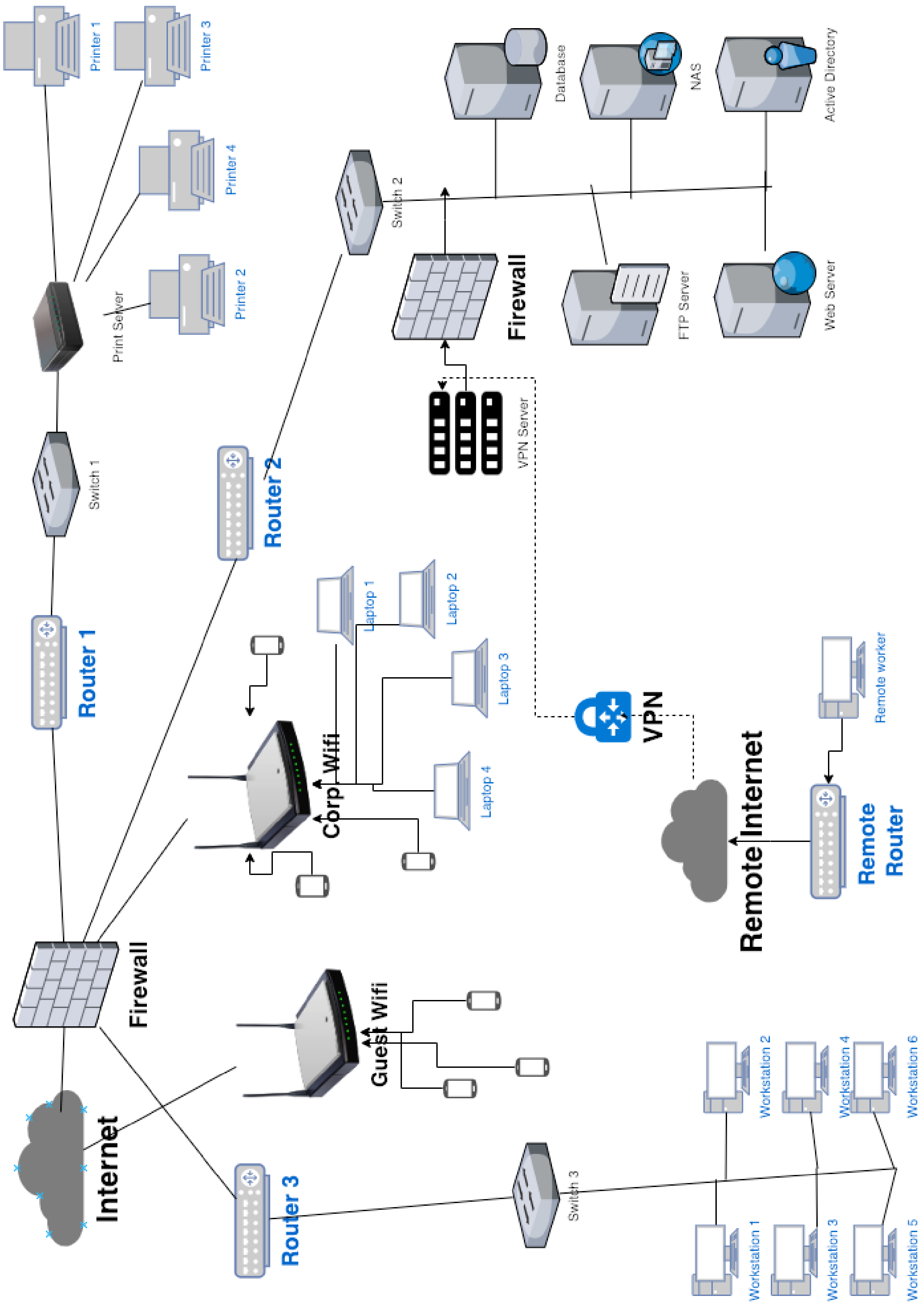
- AES
- EAP-FAST
- EAP-TLS
- PEAP

- SSID
- TKIP
- WPA-PSK

8 Revision History

Date of Change	Responsible	Summary of Change
February 2019	Bryan McKinney	Updated

Appendix B


Printer 1
Printer 3
Printer 4
Printer 2
Print Server
Switch 1
Router 1
Router 2
Switch 2
Firewall
Database
NAS
Active Directory
FTP Server
Web Server
VPN Server
Laptop 1
Laptop 2
Laptop 3
Laptop 4
Corp Wifi
VPN
Remote worker
Remote Internet
Remote Router
Internet
Firewall
Guest Wifi
Router 3
Switch 3
Workstation 1
Workstation 2
Workstation 3
Workstation 4
Workstation 5
Workstation 6