**Group Members**

Adonai Kebede Sixto Rio

Minichel Gera Maddek Richardson

**FineBrew Inc**

Final Project

**Table of Content**

**Company** **Details**1

Company descriptions2

Network Topology4

**Network** **Devices**6

**Windows** **Server** 20197

Installation

Hardening

Active Directory

**Windows** **10** **workstations**8

Installation

Hardening

**Linux** (Ubuntu Workstation) 11

Installation

Adding Ubuntu to the Domain

Hardening

**Window** **Server** **2016** (Vulnerable) 13

Breaking

Vulnerabilities

**References**20

# **Company Description**

At the Des Moines Retail Store (DMRS), we provide grade A quality products to our customers. We make sure this happens at the lowest cost possible. We are always aiming for the best customer service. Our company does not have any vehicles provided for the employees. An employee must arrive on time, ready to work, and complete their tasks for the day.

For departments, our team has one Head Manager, two employees for Purchasing and Accounting, one employee running the front counter, one employee for Marketing, and one employee to take care of Human Resources. This means that we would have six total people working at our location.

A white mug on a table

Description automatically generated with medium confidence

Figure 1FineBrew

Departments:

Head manager - 1

Purchasing/Accounting - 2

Front Counter - 1

Marketing - 1

Human Resources - 1

Total - 6

We will have our switches, which houses all our machines and server, and connect the switches to our router to provide us with a firewall and access to the internet. The only server we have will be the main server. We will not have a backup server because if this were a real scenario, and the main server gets hacked into, then the backup server will be attacked the same way.

Our office holds eight machines. Our employees are planned to have four machines that they can work from. Three of which are Windows Office Computers and one Linux Office Computer. Next, our head mangers will also have four computers. One will be the Windows 10 Computer, next to it will be the Windows 2019 Server. Then, we will have an Ubuntu 20.04 Computer, next to it will be the Ubuntu 20.04 Server. Each computer will not have a backup script as we would need to have a backup server. Having the servers split up from the computers will provide the company with more security.

For security measures, we will be using the programs that we have practiced with in class. This is to make sure penetrators can’t get as much information and will alert us when something wrong is happening.

***We provide!***

***we make!***

***we are the Des Moines Retail Store.***

FineBrew Inc

Network proudly installed by Cisco System

Diagram

Description automatically generated

**Network Topology**

This is a visual representation of the FineBrew, the newly thriving company network topology. FineBrew consist of two servers and six workstations. Our network is currently operating efficiently with little to no issue. We have Server 2019, which is acting as the main server on our system. Our network also consists of Linux server which is many used as webserver, and five windows 10 workstations and one Ubuntu 20.04. Our company is growing, therefore with scalability in mind, we are counting on ourselves in building a secure and trusted network for ourselves and for our trusted customers.

# **Network Devices:**

# **Windows 2019 Sever**

# **Windows 10 workstations**

# **Ubuntu 20.04**

# **Vulnerable Machine**

# **Installation:**

# **Hardening**

# **Active Director Management**

# **Windows 2019 Sever Installation**

Installing Windows 2019 was relatively an easy task. Once the server is installed, we proceeded to add the rules for Active Directory Domain Service (ADDS), The Domain Name System (DNS), and The Domain Host Configuration Protocol (DHCP).

Graphical user interface, application

Description automatically generatedFortunately, we did not run into a big deal of problem while performing these tasks. All our machines that are using these resources are perfectly functional, computers on the network are properly added to the domain controller, and all the machines get their IP addresses number for

the DHCP and are using our DNS server for Name-IP resolution.

This is result of nslookup done in Ubuntu machine showing the above facts. Text

Description automatically generated

# **Window 10 workstation Installation**

**0**ur network consists of five windows 10 workstation. All configured and setup for different purpose and to be operational for everyday tasks on for the company. These machines are under our domain server –iServeGroup4.local. Our manager, [Minichel Gera](https://canvas.highline.edu/groups/673235/users/5038651) is responsible for creating and managing the user and the group policies on Our domain Controller.

Users on the domain:

Graphical user interface

Description automatically generated

These machines are restricted to an outside user who is not on our domain. Therefore, all employees are required to have a login—username and password.

Graphical user interface, text, application

Description automatically generated

Detail information is also provided by the manager on the matter of joining these machines to the domain—iServerGroup4.local. If one desires to add machine to an existing domain controller, for windows 10, one should navigate to System and Security, and then click system. Then Computer Name, Domain, and workgroup setting. Click change settings on the name tab, then click change, then Under member of, click domain and type the name of the domain you wish the computer to join. Graphical user interface, application

Description automatically generated

# **Hardening**

The teamwork on Hardening the windows 10 workstations have been excellent. The first type was to make sure the windows are configured to have unique and strong usernames and password, and we have made sure that the are required at login. In addition, the windows will require login if the machine is left idle for more than 10 minutes. We have also made window firewall is up and running correctly. Furthermore, we have disable unnecessary outside connections, such as Windows Remote Desktop features. This feature allows users with the proper credential to manage the machines from a remote location over the internet, which also opens opportunity for hackers to find ways to exploit this feature. Therefore, since we are not planning to manage our domain machines from a remote location, we have decided to disable it.

The team have also suggested that keeping the machines UpToDate from the perspective of hardware, drivers and software is another aspect of hardening the windows.

**Ubuntu 20.04**

Installing Ubuntu had taken us through similar process as the rest, however, we found adding ubuntu to our domain a bit complicated. Despite the fact we were able to add and verify functionality. The step to add ubuntu to the domain require us to download multiple packages, such serv

The screenshot bellow was captured during the installation Text

Description automatically generated

**Vulnerable Machine (Windows Server 2016)**

We choose windows 2016, because it thought it is more vulnerable. As we continue to the scanning, we will see that multiple unknow service are running on ephemeral ports, which if not filter can lead to catastrophic consequences. For our vulnerable machine, we have fixed windows server 2016 to be exploited in many ways. For instance, Disabling the fire wall was the first step we took. On Windows 2016, the built-in firewall (also known as the “Microsoft Defender Firewall”) is a powerful feature that has been designed to protect your device and data from different threats from outside trying to get in as well as threats from inside trying to get out. A firewall is gatekeeper that blocks all unwanted network ports, and apps and services that tries to communicate outside the machine, the firewall will check specific rules in the database to allow or deny network access. If the rules cannot be found the system will prompt an input to grant or deny permission.

# Steps taken to make the windows 2016 vulnerable

* Open **Windows Security**.
* Click on **Firewall & network protection**. Click the**Advanced settings**option.
* Select **Inbound Rules** from the left navigation pane.
* Under the “Actions” section, in the right pane, click the **New Rule** option.
* Select the Port option.
* Click the **Next** button.
* Select the appropriate protocol (TCP or UDP) depending on the application. (Usually, the option is TCP.)
* In the **Specific local ports** field, type the port number.
* Click the **Next** button.
* Select the **Allow the connection** option. (Using the same step, note that you can also block connection.)

# These are some of the tools we use to find vulnerability on our network.

* Zenmap
* OpenVAS
* Armitage

For this task, we found that Zenmap and OpenVAS vulnerability scanners to be of a great benefit. Zenmap like many others is an open-source security scanner that is also used for network discovery, inventory, managing service upgrade schedule, and monitoring host or service uptime

Vulnerability scanners are valuable tools that search for and report on what known vulnerabilities are present in an organization’s IT infrastructure. Using a vulnerability scanner is a simple, but critical security practice that every organization can benefit from. These scans can give an organization an idea of what security threats they may be facing by giving insights into potential security weaknesses present in their environment.

**2** We have run multiple Open port scans and various scans to discover versions and services that are running on the port and the resalt came out as showing in the following screenshots.

These screenshot results are form our windows Server2019, with assigned static Ip-address of 192.168.4.10.

The following screenshot of scan result for Windows server 2016, shows the open ports and the service that are currently running on the ports. There are about thirty-one ports open and fourteen of them are ephemeral and are running unknown services.

**Graphical user interface, text

Description automatically generated**

We also have scanned the rest of our windows with the above mentions tools and have discovered known open ports with known services. We have also run some scripts to get some more information about the service and their vulnerabilities. For example, the following screenshot show the result from our trust and main servers. A screenshot of a computer

Description automatically generated with medium confidence

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Ports** | C-**Type** | **State** | **Services** | **Version** |
| * 53 | TCP | * Open | * domain | * DNS Plus |
| * 88 | TCP | * Open | * Kerberos-Sec | * Mic-Win-Kerberos |
| * 135 | TCP | * Open | * msrpc | * Mic-win RPC |
| * 389 | TCP | * Open | * LDAP | * Microsoft Active Directory LDAD |
| * 139 | TCP | * Open | * Netbios-ssn | * -------------------------- |
| * 445 | TCP | * Open | * Microsoft-ds | * -------------------------- |

As shown in the screenshots, some of the service running on this server include

One security risk discovered during the scanning phase is that one of the services running on port is the smb2-security-mode: 3.1.1 which can be vulnerable to relay attack again our Active Directory, however we noticed that Signing is anabled and required to gain access. A SMB relay attack is where an attacker captures a user’s NTLM hash and relays it’s to another machine on the network. Masquerading as the user and authenticating against SMB to gain shell or file access.

Text

Description automatically generated

Some of measurements taken to mitigate our machines vulnerability include filtering unused ports, such as ftp ports, SSH port and remote management services. In addition, we have managed to make our network inaccessible by machines outside of our domain

# **Reference**

# [Computing for Geeks](https://computingforgeeks.com/join-ubuntu-debian-to-active-directory-ad-domain/)

[Mile2.com](Mile2.com/)

[https://microsoft.com](https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview)