

**E-MAGINE BIOMEDICAL**

# **CYBERSECURITY AUDIT**



[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)

**John An, Security Analyst**  
**Email:** [johan5257@students.ecpi.edu](mailto:johan5257@students.ecpi.edu)



## CONTENTS

1

Executive Summary .....	.2
Recommendations .....	.3
Conclusion .....	.5
Appendix .....	.6

# Cybersecurity Audit

## Executive Summary

The objective of the E-MAGINE Biomedical cybersecurity audit was to assess the overall state of security for the organization's internal systems managed by the company's IT security team.

Several findings were rated as critical and involved a Windows 2019 server, Linux hosts for development, and a firewall that was installed but not fully configured.



[This Photo](#) by Unknown Author is licensed under [CC BY](#)

The cybersecurity audit of E-MAGINE Biomedical revealed several critical vulnerabilities across Windows Server 2019, Linux development hosts, and pfSense firewall systems. Key issues included disabled automatic updates, weak password policies, poor access controls, misconfigured network shares, unrestricted administrative access, and lack of firewall segmentation between internal segments.

Among the most severe findings:

- All users were members of the Domain Admins group, granting them excessive privileges.
- Password policies were missing or weak, allowing potential brute-force or credential-stuffing attacks.

- **Critical firewall configurations were not in place**, leaving internal systems open to unauthorized access.
- **Linux systems lacked password complexity and SSH controls**, making them vulnerable to privilege escalation and remote attacks.
- **Unrestricted access to the pfSense firewall GUI** posed a major risk for configuration tampering.

If these vulnerabilities had gone unaddressed, E-MAGINE Biomedical would have remained highly susceptible to ransomware infections, insider threats, and external intrusions—particularly given the lack of layered access control and inadequate auditing of system activities. These issues could have led to unauthorized access to sensitive biomedical data, compliance violations, and potential operational downtime.

To mitigate these risks, our remediation plans focused on enforcing secure password policies, segmenting user and group permissions, tightening firewall controls, enabling system auditing and automatic updates, and applying role-based access control on all systems.

# Recommendations

The Cybersecurity team members have reviewed the audit findings. The potential risks considered if controls are not in place include:

## Governance

- Enforce strict group policy management practices.
- Limit privileged group membership to essential IT admin roles.
- Implement a change management policy for all system-level configurations.
- Schedule recurring internal audits to ensure ongoing compliance with organizational security policies.

## Access Control

- Apply least privilege access for both Windows and Linux systems.
- Restrict shared folder access by department using group-based permissions.
- Block root SSH login on Linux systems.
- Limit pfSense GUI access to trusted internal IPs (e.g., Windows Server only).

## Identity Access and Account Management

- Create dedicated administrative accounts separate from user accounts.
- Remove non-IT users from Domain Admin groups.
- Enforce account lockout policies to prevent brute-force login attempts.
- Establish user role groups (IT\_AdminAccess, HR\_ReadOnly, etc.) with clearly defined access scopes.

## Risk Mitigation

- Enable automatic updates across all operating systems to reduce known vulnerability exposure.
- Apply firewall rules to isolate network segments and restrict unauthorized cross-traffic.
- Regularly monitor security event logs and configure alerting for suspicious behavior.
- Back out plans were created and tested for every system change to ensure minimal operational disruption.

## Cryptography and PKI

- Enforce secure transmission protocols (e.g., HTTPS for pfSense, SSH for remote access).
- Begin preparations to implement certificate-based authentication in the future.
- Disable outdated or insecure cryptographic algorithms on all systems.

## Conclusion

**“Cybersecurity is much more than a matter of IT”**

Stephane Nappo

Opportunities exist to further develop and mature E-MAGINE Biomedical’s cybersecurity program. This audit brought to light critical concerns.



This Photo by Unknown Author is licensed under CC BY-ND

The cybersecurity audit of E-MAGINE Biomedical revealed significant gaps in system hardening, access control, and policy enforcement. Through a structured remediation process, these gaps were systematically addressed. Key improvements included implementing password and account lockout policies, enforcing the principle of least privilege, restricting root and administrative access, enabling audit logs, and configuring firewall rules to isolate network segments securely.

These changes have greatly strengthened E-MAGINE Biomedical’s overall security posture. Windows and Linux systems are now better protected against internal and external threats, while pfSense firewall configurations have introduced proper segmentation and control over network traffic.

Following these recommendations is critical to protecting sensitive biomedical research and operational data. As cyber threats continue to evolve, it’s essential that the organization maintains this momentum by adopting a proactive approach to cybersecurity—regularly reviewing policies, monitoring for vulnerabilities, and ensuring compliance with industry best practices.

This remediation project has laid a strong foundation for a more secure and resilient IT infrastructure at E-MAGINE Biomedical.

# Appendix

The following reports document the vulnerabilities to remediate. Each report includes the following primary sections:

## **Pre-execution**

In this section we evaluate the current configurations and values.

## **Execution**

This section documents the steps required to remediate the audit findings and issues.

## **Post-Execution and Deliverables**

This section documents that the changes were made to address the audit findings.

## **Follow-Up**

This section shares any follow-up required after post-execution is performed.

## Project Scope

### *WEEK 1 Vulnerabilities to Remediate*

Windows/Linux - Lack of auditing, Automatic Updates not configured

## Project Lead

John An, Johan5257

## Technical Stakeholders

Dr. William Harding

## Primary Business Users

Thomas Evans - IT Department

Janet Adams - Human Resources

Mary Wilder - Customer Service

## Project Summary

To achieve compliance with the items discovered in the voluntary security audit, several changes are proposed to address the issues listed in the project scope. The requirements for the necessary changes have been defined and low-level details of the specific changes are listed including validation. Risk has been assessed for contingency, and a backout plan is defined to respond in the event of an impact.

## Task List

1. Create project implementation plan per system
  - a. Identify pre and post execution procedures (specific changes to be made and method for validation, i.e., commands or screenshots)
2. \*Notify Stakeholders (Peer review of changes) (Not required for this, for informational purposes.)
3. \*Schedule project in scheduled maintenance calendar (Not required, for informational purposes.)
4. Capture screenshot of current configuration and environment (i.e, make sure you're logged into the right system)
5. Apply changes (commands or screenshots)
6. Document applied settings (commands or screenshots)
7. Notify Validation Group environment is ready for testing. (For this, your instructor is your validation group, so this entails you submitting your results for grading – see Step 10 below.)
8. Summarize scope of remediated vulnerabilities with reference to the specific audit findings for Final Report.
9. Consider additional steps for backout plan.

10. Submit completed document in Canvas.

#### VCASTLE Systems – Usernames and passwords

1. Windows 10	UN: cis230\administrator	PW: Password1	172.16.10.10
2. Ubuntu	UN: ecpi	PW: Password1	172.16.20.20
3. Server 2019	UN: cis230\administrator	PW: Password1	172.16.30.30
4. pfSense	UN: admin	PW: pfSense	172.16.100.1

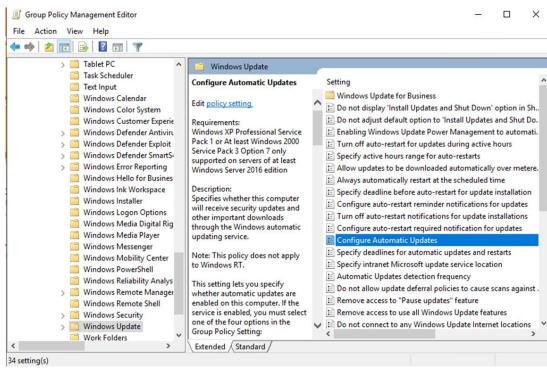
#### Execution Procedures

Note: All activities this week, except the Progress Summary will be done together with the instructor in VCASTLE.

#### Windows OS Execution Plan

##### Enable Automatic Updates

1. Edit current **Windows Updates** settings on system Windows Server 2019
  - Go to **Server Manager** -> **Tools** -> **Group Policy Management**
  - Expand tree -> Right-click on **Default Domain Policy** -> **Edit**
  - Expand **Computer Configuration** section
  - Expand **Policies** section
  - Select **Administrative Templates** -> **Windows Components** -> select **Windows Update**



2. Find **Configure Automatic Updates** in Setting, double click
  - Set to auto download and schedule install
  - Set schedule to every day at 7:00PM every week
  - Click OK to save
  - Close Group Policy Management console.
3. Open command prompt or PowerShell -> Command: **gpupdate /force**

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> gpupdate /force
Updating policy...
Computer Policy update has completed successfully.
User Policy update has completed successfully.

PS C:\Users\Administrator>
```

4. Run command prompt or PowerShell as Administrator
  - a. Type **gpresult**
  - b. Expand **Computer Configuration** section
  - c. Take screenshot showing settings have applied successfully

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> gporesult /r
Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
© 2018 Microsoft Corporation. All rights reserved.

Created on [ 3/ 3/ 2025 at 11:45:44 AM

RSOP data for CIS230\Administrator on CIS230-WIN2019 : Logging Mode
-----
OS Configuration: Primary Domain Controller
OS Version: 10.0.17763
Site Name: Default-First-Site-Name
Roaming Profile: N/A
Local Profile: C:\Users\Administrator
Connected over a slow link?: No

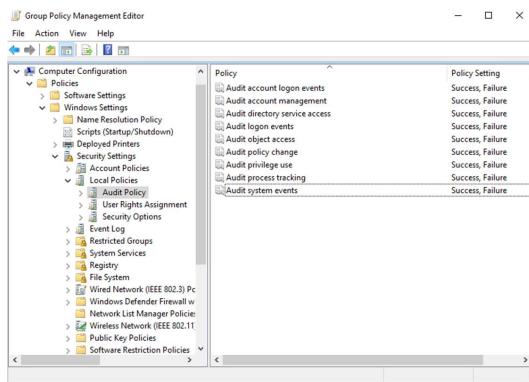
COMPUTER SETTINGS
-----
CN=CIS230-WIN2019,OU=Domain Controllers,DC=cis230,DC=local
Last time Group Policy was applied: 3/3/2025 at 11:41:51 AM
Group Policy was applied from: cis230-win2019.cis230.local
Group Policy slow link threshold: 500 kbps
Domain Name: CIS230
Domain Type: Windows 2008 or later

Applied Group Policy Objects
-----
Default Domain Controllers Policy
Default Domain Policy

The following GPOs were not applied because they were filtered out
-----
Local Group Policy
Filtering: Not Applied (Empty)
```

## Audit Policy Remediation

1. Edit current **Audit** settings on system Windows Server 2019
  - a. Go to **Server Manager** -> **Tools** -> **Group Policy Management**
  - b. Expand tree two levels -> Right-click on **Default Domain Policy** -> **Edit**
  - c. Expand **Computer Configuration - Policies** section
  - d. Expand **Windows Settings -> Security Settings -> Local Policies -> Audit Policy**
2. Enable auditing for all listed event types – Right click, select Properties – check all boxes, click OK.



3. Close Group Policy Management Editor and Console
4. Open command prompt or PowerShell -> Command: **gpupdate /force**

### **Linux OS Execution Plan**

#### **Enable Automatic Updates in Ubuntu**

1. Update Ubuntu package lists and install pending updates:
  - a. Open terminal window
  - b. `sudo apt-get update`
  - c. `sudo apt-get upgrade`
2. Install the `unattended-upgrades` package with `apt`:
  - a. `sudo apt-get install unattended-upgrades`

Add a screenshot here.

```
update-initramfs: deferring update (trigger activated)
Processing triggers for ntp (1:4.2.8p12+dfsg-3ubuntu4.20.04.1) ...
Processing triggers for shared-mime-info (1.15-1) ...
Processing triggers for install-info (6.7.0.dfsg.2-5) ...
Processing triggers for fontconfig (2.13.1-2ubuntu3) ...
Processing triggers for desktop-file-utils (0.24-1ubuntu3) ...
Processing triggers for ca-certificates (20240203-20.04.1) ...
Updating certificates in /etc/ssl/certs...
0 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
Processing triggers for systemd (245.4-4ubuntu3.24) ...
Processing triggers for libgdk-pixbuf2.0-0:amd64 (2.40.0+dfsg-3ubuntu0.5) ...
Processing triggers for dbus (1.12.16-2ubuntu2.3) ...
Processing triggers for initramfs-tools (0.136ubuntu6.7) ...
update-initramfs: Generating /boot/initrd.img-5.4.0-105-generic
ecpi@cis230-ubuntu:~$ sudo apt-get install unattended-upgrades
Reading package lists... Done
Building dependency tree
Reading state information... Done
unattended-upgrades is already the newest version (2.3ubuntu0.3).
0 upgraded, 0 newly installed, 0 to remove and 17 not upgraded.
ecpi@cis230-ubuntu:~$
```

### 3. Enable the unattended-upgrades function

- sudo dpkg-reconfigure --priority=low unattended-upgrades
- Add a screenshot here.

```
Processing triggers for ntp (1:4.2.8p12+dfsg-3ubuntu4.20.04.1) ...
Processing triggers for shared-mime-info (1.15-1) ...
Processing triggers for install-info (6.7.0.dfsg.2-5) ...
Processing triggers for fontconfig (2.13.1-2ubuntu3) ...
Processing triggers for desktop-file-utils (0.24-1ubuntu3) ...
Processing triggers for ca-certificates (20240203-20.04.1) ...
Updating certificates in /etc/ssl/certs...
0 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
Processing triggers for systemd (245.4-4ubuntu3.24) ...
Processing triggers for libgdk-pixbuf2.0-0:amd64 (2.40.0+dfsg-3ubuntu0.5) ...
Processing triggers for dbus (1.12.16-2ubuntu2.3) ...
Processing triggers for initramfs-tools (0.136ubuntu6.7) ...
update-initramfs: Generating /boot/initrd.img-5.4.0-105-generic
ecpi@cis230-ubuntu:~$ sudo apt-get install unattended-upgrades
Reading package lists... Done
Building dependency tree
Reading state information... Done
unattended-upgrades is already the newest version (2.3ubuntu0.3).
0 upgraded, 0 newly installed, 0 to remove and 17 not upgraded.
ecpi@cis230-ubuntu:~$ sudo dpkg-reconfigure -priority=low unattended-upgrades
Replacing config file /etc/apt/apt.conf.d/20auto-upgrades with new version
ecpi@cis230-ubuntu:~$
```

- When prompted to automatically install stable updates, select YES

### 4. Verify unattended upgrade service is working:

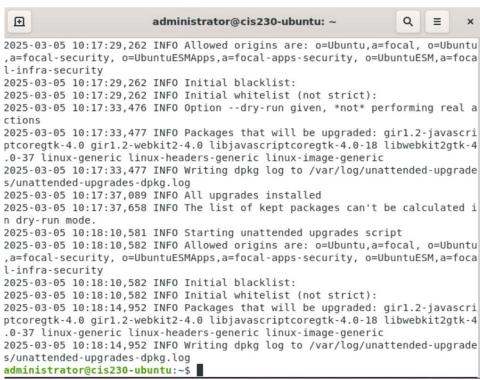
- sudo unattended-upgrades --dry-run (2 dashes)
- Add a screenshot here.



```
ecpi@cis230-ubuntu:~ cat /var/log/unattended-upgrades/unattended-upgrades.log
[sudo] password for ecpi:
/usr/bin/dpkg --status-fd 10 --no-triggers --unpack --auto-deconfigure /var/cache/apt/archives/libatomic1_10.5.0~ubuntu1~20.04_amd64.deb /var/cache/apt/archives/libwebkit2gtk-4.0-37_2.38.6~ubuntu0.20.04.1_amd64.deb
/usr/bin/dpkg --status-fd 10 --configure --pending
/usr/bin/dpkg --status-fd 10 --no-triggers --unpack --auto-deconfigure --recursive /var/cache/apt/archives/libatomic1_10.5.0~ubuntu1~20.04_amd64.deb
/usr/bin/dpkg --status-fd 10 --configure --pending
/usr/bin/dpkg --status-fd 10 --no-triggers --unpack --auto-deconfigure /var/cache/apt/archives/libwebkit2gtk-4.0-37_2.38.6~ubuntu0.20.04.1_amd64.deb /var/cache/apt/archives/libjavascriptcoregtk-4.0-18_2.38.6~ubuntu0.20.04.1_amd64.deb /var/cache/apt/archives/gir1.2-webkit2-4.0_2.38.6~ubuntu0.20.04.1_amd64.deb /var/cache/apt/archives/gir1.2-javascriptcoregtk-4.0_2.38.6~ubuntu0.20.04.1_amd64.deb
/usr/bin/dpkg --status-fd 10 --configure --pending
ecpi@cis230-ubuntu:~
```

tail

- 5. Check Unattended Upgrades Log:**
- tail -n 100 /var/log/unattended-upgrades/unattended-upgrades.log
- Add a screenshot here.



```
administrator@cis230-ubuntu:~ tail -n 100 /var/log/unattended-upgrades/unattended-upgrades.log
2025-03-05 10:17:29.262 INFO Allowed origins are: o=Ubuntu,a=focal, o=Ubuntu,a=focal-security, o=UbuntuESMApps,a=focal-apps-security, o=UbuntuESM,a=focal-infra-security
2025-03-05 10:17:29.262 INFO Initial blacklist:
2025-03-05 10:17:29.262 INFO Initial whitelist (not strict):
2025-03-05 10:17:33.472 INFO Option --dry-run given, *not* performing real actions
2025-03-05 10:17:33.477 INFO Packages that will be upgraded: gir1.2-javascriptcoregtk-4.0 gir1.2-webkit2-4.0 libjavascriptcoregtk-4.0-18 libwebkit2gtk-4.0-37 linux-generic linux-headers-generic linux-image-generic
2025-03-05 10:17:33.477 INFO Writing dpkg log to /var/log/unattended-upgrades/unattended-upgrades-dpkg.log
2025-03-05 10:17:37.089 INFO All upgrades installed
2025-03-05 10:17:37.089 INFO The list of kept packages can't be calculated in dry-run mode.
2025-03-05 10:18:10.581 INFO Starting unattended upgrades script
2025-03-05 10:18:10.582 INFO Allowed origins are: o=Ubuntu,a=focal, o=Ubuntu,a=focal-security, o=UbuntuESMApps,a=focal-apps-security, o=UbuntuESM,a=focal-infra-security
2025-03-05 10:18:10.582 INFO Initial blacklist:
2025-03-05 10:18:10.582 INFO Initial whitelist (not strict):
2025-03-05 10:18:14.952 INFO Packages that will be upgraded: gir1.2-javascriptcoregtk-4.0 gir1.2-webkit2-4.0 libjavascriptcoregtk-4.0-18 libwebkit2gtk-4.0-37 linux-generic linux-headers-generic linux-image-generic
2025-03-05 10:18:14.952 INFO Writing dpkg log to /var/log/unattended-upgrades/unattended-upgrades-dpkg.log
administrator@cis230-ubuntu:~
```

## Enable and configure Auditd for security events

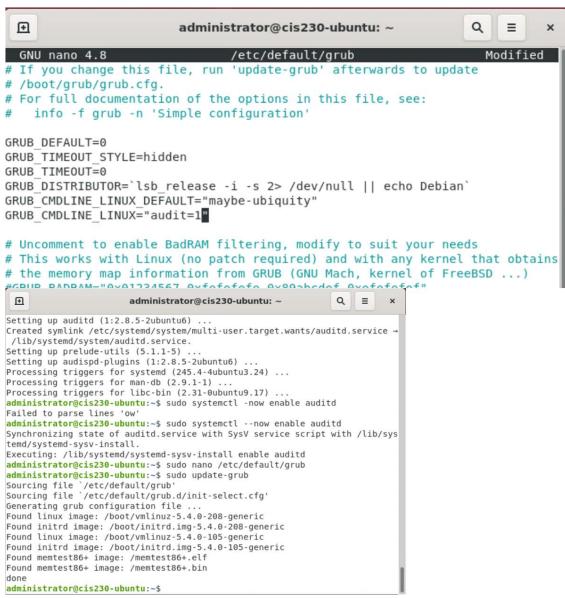
- Install and configure auditd:

  - sudo apt install auditd audispd-plugins
  - sudo systemctl -now enable --auditd (2 dashes)

## 2. Set the parameter on your bootloader to enable during bootup

- a. sudo nano /etc/default/grub
  - i. Find the **GRUB\_CMDLINE\_LINUX=** command line
  - ii. Change value to: **GRUB\_CMDLINE\_LINUX="audit=1"**
  - iii. Save and close Nano - **Ctrl o, Ctrl x**
- b. sudo update-grub

Add a screenshot here.



```

administrator@cis230-ubuntu: ~
GNU nano 4.8          /etc/default/grub           Modified
# If you change this file, run 'update-grub' afterwards to update
# /boot/grub/grub.cfg.
# For full documentation of the options in this file, see:
#   info -f grub -n 'Simple configuration'

GRUB_DEFAULT=0
GRUB_TIMEOUT_STYLE=hidden
GRUB_TIMEOUT=0
GRUB_DISTRIBUTOR=`lsb_release -i -s > /dev/null || echo Debian`
GRUB_CMDLINE_LINUX_DEFAULT="maybe-ubiquity"
GRUB_CMDLINE_LINUX="audit=1"

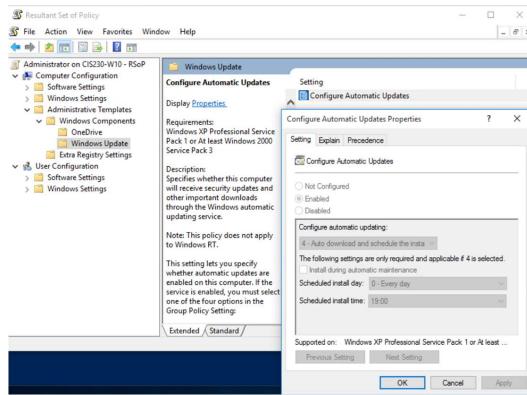
# Uncomment to enable BadRAM filtering, modify to suit your needs
# This works with Linux (no patch required) and with any kernel that obtains
# the memory map information from GRUB (GNU Mach, kernel of FreeBSD ...)

GRUB_BDAPI="https://github.com/audited/badramd.git" GRUB_BDAPI_COMMIT="v0.1.1" GRUB_BDAPI_BRANCH="main" GRUB_BDAPI_GIT="git@github.com:audited/badramd.git"
administrator@cis230-ubuntu: ~
GNU nano 4.8          /etc/default/grub           Modified
Setting up auditd (1:2.8.5-2ubuntu6) ...
Creating symlink /etc/systemd/system/multi-user.target.wants/auditd.service -
/lib/systemd/system/auditd.service → /lib/systemd/system/auditd.service
Setting up prelude-utils (5.1.1-5) ...
Setting up audispd-plugins (1:2.8.5-2ubuntu6) ...
Processing triggers for systemd (246.4-0ubuntu3.24) ...
Processing triggers for libaudit-dev (1:2.8.5-2ubuntu6) ...
Processing triggers for libc-bin (2.31-0ubuntu9.17) ...
administrator@cis230-ubuntu:~$ sudo systemctl --now enable auditd
Failed to parse 'auditd': No such file or directory
administrator@cis230-ubuntu:~$ sudo systemctl --now enable auditd
Synchronizing state of auditd.service with SysV service script with /lib/sys
temd/systemd-sysv-install.
Executing '/lib/systemd/systemd-sysv-install enable auditd'
administrator@cis230-ubuntu:~$ sudo nano /etc/default/grub
administrator@cis230-ubuntu:~$ sudo update-grub
Sourcing file '/etc/default/grub'
Generating grub configuration file ...
Found linux image: /boot/vmlinuz-5.4.0-208-generic
Found initrd image: /boot/initrd.img-5.4.0-208-generic
Found linux image: /boot/vmlinuz-5.4.0-208-generic
Found initrd image: /boot/initrd.img-5.4.0-208-generic
Found memtest86+ image: /memtest86+.elf
Found memtest86+ image: /memtest86+.bin
done
administrator@cis230-ubuntu:~$
```

## Windows Post-Execution and deliverables

2. Log on to Server 2019 as administrator
3. Execute steps from Execution Plan
4. Paste screenshots for steps in the Plan section, as appropriate
5. Log onto Window 10 client as a domain admin

6. Run command prompt or PowerShell as Administrator
  - a. Type **rsop.msc**
  - b. Expand **Computer Configuration** section
  - c. Take screenshot showing settings have applied successfully



## Linux Post-Execution and deliverables

1. Log on to Ubuntu
2. Execute steps from the Execution Plan
3. Paste Screenshots of all configuration changes made through the CLI

```
administrator@cis230-ubuntu: ~
2025-03-05 10:17:29,262 INFO Allowed origins are: o=ubuntu,a=focal, o=ubuntu ,a=focal-security, o=UbuntuESMAApps,a=focal-apps-security, o=UbuntuESM,a=foca l-infra-security
2025-03-05 10:17:29,262 INFO Initial blacklist:
2025-03-05 10:17:29,262 INFO Initial whitelist (not strict):
2025-03-05 10:17:33,477 INFO Option --dry-run given, *not* performing real a ctions.
2025-03-05 10:17:33,477 INFO Packages that will be upgraded: gir1.2-javascri ptcoregtk-4.0 gir1.2-webkit2-4.0 libjavascriptcoregtk-4.0-18 libwebkit2gtk-4 .0-37 linux-generic linux-headers-generic linux-image-generic
2025-03-05 10:17:33,477 INFO Writing dpkg log to /var/log/unattended-upgrade s/unattended-upgrades-dpkg.log
2025-03-05 10:17:37,088 INFO All upgrades installed
2025-03-05 10:17:37,658 INFO The list of kept packages can't be calculated i n dry-run mode.
2025-03-05 10:18:10,581 INFO Starting unattended upgrades script
2025-03-05 10:18:10,592 INFO Allowed origins are: o=ubuntu,a=focal, o=ubuntu ,a=focal-security, o=UbuntuESMAApps,a=focal-apps-security, o=UbuntuESM,a=foca l-infra-security
2025-03-05 10:18:10,582 INFO Initial blacklist:
2025-03-05 10:18:10,582 INFO Initial whitelist (not strict):
2025-03-05 10:18:14,952 INFO Packages that will be upgraded: gir1.2-javascri ptcoregtk-4.0 gir1.2-webkit2-4.0 libjavascriptcoregtk-4.0-18 libwebkit2gtk-4 .0-37 linux-generic linux-headers-generic linux-image-generic
2025-03-05 10:18:14,952 INFO Writing dpkg log to /var/log/unattended-upgrade s/unattended-upgrades-dpkg.log
administrator@cis230-ubuntu:~$
```



- Notify Validation Group environment is ready for testing. (Here, this means submitting this document)

### **Back-out plan – update weekly**

#### **Windows System:**

1. Revert settings to original values
2. Run a **gpupdate /force**

#### **Linux System:**

1. Remove automatic update
  - a. `sudo apt remove unattended-upgrades`
2. Remove auditd
  - a. `sudo apt remove auditd audispd-plugins`

### **Project Notes**

Make sure you specify the systems that you are working on configuring as part of the change management process.

Server Info:

**(Virtual) Server Name:** CIS230-UBUNTU

**OS:** Ubuntu 9.4.0-1ubuntu1~20.04.2

**IP Address:** 172.16.30.30

**Server Specs:**

VM

CPU: Intel® Xeon® CPU E5-2640 v4 @ 240GHz

RAM: 1.9 GiB

STORAGE: 42.9 GB

NETWORK:

2 vCPU, 2GB RAM

**(Virtual) Server Name:** CIS230-WIN2019

**OS:** Windows Server 2019 Standard, 10.0.17763 Build 177763

**IP Address:** 172.16.10.10

**Server Specs:**

VM

CPU: Intel® Xeon® CPU E5-2640 v4 @ 2.40GHz, 2397 Mhz, 2 Core(s), 2 Logical Processor(s)

RAM: 4.00 GB

STORAGE: 60 GB

NETWORK: Intel® 82574L Gigabit Network Connection

2 vCPU, 2GB RAM

**(Virtual) Server Name:** CIS230-WIN10

**OS:** Windows 10 Education, 10.0.10240 Build 10240

**IP Address:** 172.16.20.20

**Server Specs:**

VM

**CPU:** Intel® Xeon® CPU E5-2640 v4 @ 2.40GHz, 2397 Mhz, 1 Core(s), 1 Logical Processor(s)

**RAM:** 2.00 GB

**STORAGE:** 40.00 GB

**NETWORK:** Intel® 82574L Gigabit Network Connection

2 vCPU, 2GB RAM

## Project Scope

### *WEEK 2 Vulnerabilities to Remediate*

**Windows Server** - To ensure proper security measures, it is necessary to configure the network shares in a way that grants access only to the appropriate departments. The recommended configurations are as follows:

1. No access should be given to HR department.
2. Access to IT department should be granted only to their respective group.
3. Users in all departments should be granted read-only access to COMMON, except for HR which should have the ability to create, edit, and delete files.

*Demo: Disable logon name showing on lock and login prompt.*

**Linux** - To improve the security of the network shares, it is necessary to configure the appropriate groups and Samba configuration files. Specifically, the following steps should be taken:

1. Only the appropriate department groups should be granted full access, with no access given to the HR department.
2. The IT department should only be accessible from its respective group.
3. The COMMON network share should be set to read-only access for all users
  - a. HR department should have permission to create, edit, and delete files.
4. The root account should be disabled for SSH access to improve security.

*Demo: Add users to appropriate groups for shares.*

**Pfsense** - Configure firewall rule to limit firewall admin web gui access only from Windows server,

1.  Create new administrative account {studentid-ADMIN}
2.  Login and change password for admin and
3.  Set account properties to disable login.

*Demo: change default web gui port to TCP port above 1024.*

## Project Lead

Your FirstName LastName and ECPI User ID

## Technical Stakeholders

Your Supervisor (Instructor)

## Primary Business Users

Thomas Evans - IT Department

Janet Adams - Human Resources

Mary Wilder - Customer Service

## Project Summary

To achieve compliance with the items discovered in the voluntary security audit, several changes are proposed to address the issues listed in the project scope. The requirements for the necessary changes have been defined and low-level details of the specific changes are listed including validation. Risk has been assessed for contingency and backout plan is defined to respond in the event of an impact.

## Preparation

11. Create project remediation plan per system
  - a. Identify pre and post execution procedures (specific changes to be made and method for validation, i.e., commands or screenshots)
12. \*Notify Stakeholders (Peer review of changes) (Not required, for informational purposes.)
13. \*Schedule project in scheduled maintenance calendar (Not required, for informational purposes.)
14. Capture screenshot of current configuration and environment (i.e, make sure you're logged into the right system)
15. Apply changes (commands or screenshots)
16. Document applied settings (commands or screenshots)
17. Notify Validation Group environment is ready for testing. (Not required for informational purposes.)
18. Summarize remediated vulnerabilities with reference to the specific audit findings for Final Report.
19. Submit completed document in Canvas.

## VCastle Systems – Usernames and passwords

1. Windows 10	UN: cis230\administrator	PW: Password1	172.16.10.10
2. Ubuntu	UN: ecpi	PW: Password1	172.16.20.20
3. Server 2019	UN: cis230\administrator	PW: Password1	172.16.30.30
4. pfSense	UN: admin	PW: pfsense	172.16.100.1

## Windows OS Execution Plan



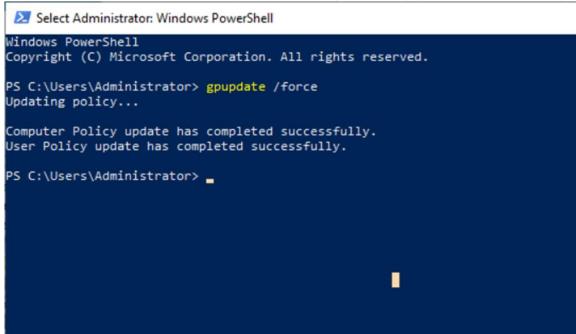
5. Edit current **Windows Updates** settings on system Windows Server 2019
  - Go to **Server Manager** --> **Tools** --> **Group Policy Management**
  - Expand tree two levels --> Right-click on **Default Domain Policy** --> **Edit**
  - Expand **Computer Configuration** section -> Windows Settings
  - Security Settings --> Local Policies --> Security Options
  - Locate and enable **Interactive Logon: Don't display last signed-in** – Double click to open - Select

Enabled – click ok

- Locate and enable **Interactive Logon: Display user information when the session is locked** --> check Define this policy setting --> select **Do not display user information** from dropdown – click **OK**
- Close all dialog boxes**

6. Open command prompt or PowerShell --> Command: **gpupdate /force**

7. Take a screenshot showing this setting have applied successfully.

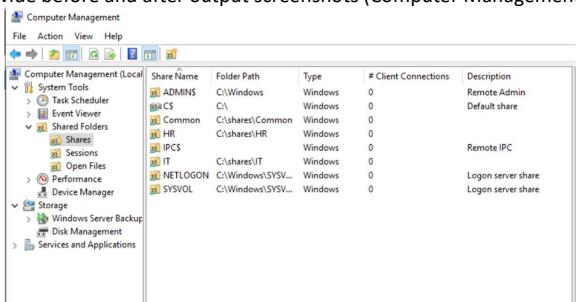


```
PS C:\Users\Administrator> gpupdate /force
Updating policy...
Computer Policy update has completed successfully.
User Policy update has completed successfully.

PS C:\Users\Administrator>
```

#### Correct Network Shares Configuration ( PowerShell)

- List steps to verify C:\Shares and associated subfolders are correctly shared
  - Go to Computer Management > System Tools > Shared Folders > Shares
- Provide before and after output screenshots (Computer Management Shares)



Share Name	Folder Path	Type	# Client Connections	Description
ADMIN\$	C:\Windows	Windows	0	Remote Admin
CS	C:\	Windows	0	Default share
Common	C:\shares\Common	Windows	0	
HR	C:\shares\HR	Windows	0	
IPC\$	C:\Windows\IPC\$	Windows	0	Remote IPC
IT	C:\shares\IT	Windows	0	
NETLOGON	C:\Windows\SYSVOL	Windows	0	Logon server share
SYSVOL	C:\Windows\SYSVOL	Windows	0	Logon server share

#### Linux OS Execution Plan

Correct network shares group access

- Add users to groups:

- a. sudo usermod -a -G common,it tevans
- b. sudo usermod -a -G common,hr jadams
- c. sudo usermod -a -G common mwilder

#### 7. Verify group membership

- a. cat /etc/group

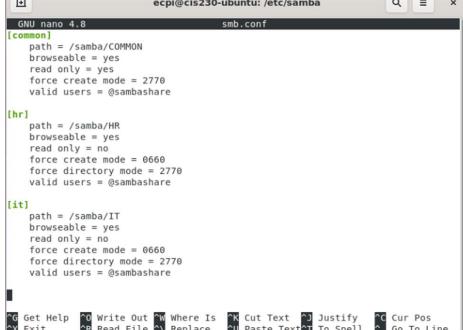
- b.  Provide a screenshot

```
common:x:1002:tevans,jadams,mwilder
hr:x:1003:jadams
it:x:1004:tevans
jadams:x:1005:
mwilder:x:1006:
tevans:x:1007:
ntp:x:135:
ecpi@cis230-ubuntu:/samba$
```

#### Update Samba shares configuration file with updated groups

1. Location of the Samba configuration file is /etc/samba/smb.conf
2. Use Nano to Edit sections: - refer to the Linux Vulnerabilities in Project Scope above.
  - a. Set updated value for COMMON
  - b. Set updated value for IT
  - c. Set updated value for HR

3. Provide screenshots (before and after)



```
GNU nano 4.8          smb.conf
[common]
path = /samba/COMMON
browseable = yes
read only = no
force create mode = 2770
valid users = @sambashare

[hr]
path = /samba/HR
browseable = yes
read only = no
force create mode = 0660
force directory mode = 2770
valid users = @sambashare

[it]
path = /samba/IT
browseable = yes
read only = no
force create mode = 0660
force directory mode = 2770
valid users = @sambashare
```

4. Restart samba services

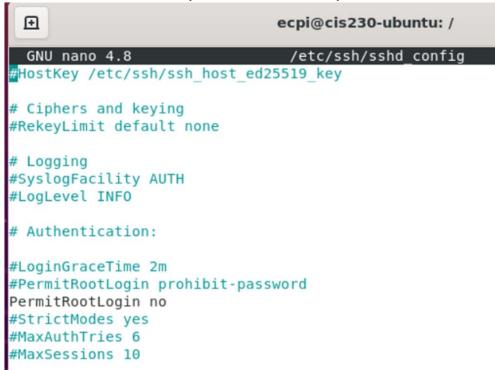
- a. List the commands
- Sudo smbd restart

5. Disable root account use over SSH

- a. List the command
- Sudo nano /etc/ssh/sshd\_config

### Change PermitRootLogin to No

6. Provide screenshots (before and after)



```

ecpi@cis230-ubuntu: ~
GNU nano 4.8          /etc/ssh/sshd_config
HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

```

### Pfsense Firewall Execution Plan

#### Change default admin portal TCP port

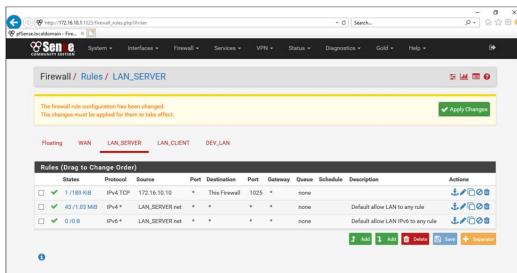
1. System --> Advanced --> TCP number (use port greater than 1024)
2. Provide a screenshot



#### Configure web access to Pfsense GUI to allow only from Windows Server (Note: must be done in a specific order, research vendor documentation)

1. List steps
1. Log into the pfSense Web GUI
  - a. Open a web browser and access the pfSense GUI via: <https://<pfSense-IP>>
  - b. Login with your admin credentials.
2. Go to Firewall Rules
  - a. Navigate to Firewall > Rules.
  - b. Click on LAN (or the interface you want to control access from).

3. **Create a New Rule to Allow Windows Server**
  - a. Click **Add** (**↑** to insert rule at the top).
  - b. **Action: Pass**
  - c. **Interface: LAN**
  - d. **Protocol: TCP**
  - e. **Source: Single host or alias**, then enter the Windows Server's IP
  - f. **Destination: This firewall (self)**
  - g. **Destination Port: HTTPS (443) or HTTP (if enabled, 80)**
  - h. **Description: "Allow Windows Server to access pfSense GUI"**
  - i. Click **Save**, then **Apply Changes**.
  
1. **Create a Blocking Rule**
  - a. Click **Add** (**↓** to insert below the allow rule).
  - b. **Action: Block**
  - c. **Interface: LAN**
  - d. **Protocol: TCP**
  - e. **Source: Any**
  - f. **Destination: This firewall (self)**
  - g. **Destination Port: HTTPS (443) or HTTP (if enabled, 80)**
  - h. **Description: "Block all other access to pfSense GUI"**
  - i. Click **Save**, then **Apply Changes**.
2. **Ensure Rule Order**
  - a. The **allow rule** for the Windows Server **must be above** the block rule.
  - b. If necessary, drag and reorder the rules.



**Create new administrative account and then login to change default admin account password and disable login**

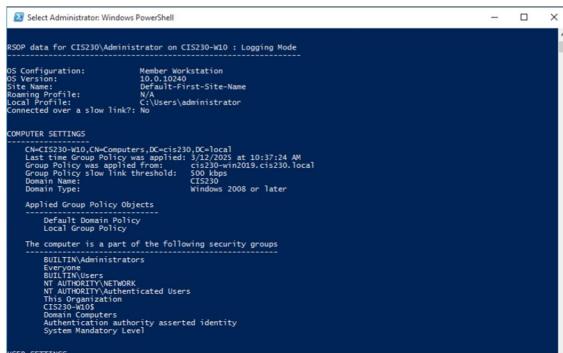
1. List steps  
Add > Username: johan5257 > Password: Password1 > John An

Username	Full name	Status	Groups	Actions
admin	System Administrator	∅	admins	
bharding	W R Harding	✓	admins	
johan5257-ADMIN	John An	✓	admins	

#### Windows Post-Execution and deliverables

7. Log onto Window 10 client as a domain admin
8. Run command prompt or PowerShell as Administrator
  - a. Type **gpresult /R**
  - b. Expand **Computer Configuration** section
  - c. Take screenshot showing settings have applied successfully

9. Lock screen and take screenshot



```
PS C:\Windows\system32> gpresult /info
-----[REDACTED]-----
```

GS Configuration: Member Workstation  
 GS Version: 10.0.10240  
 Roaming Profile: Default-First-Site-Name  
 Local Profile: C:\Users\administrator  
 Connected over a slow link?: No

CENTER SETTINGS  
 CN=CN=GroupPolicyContainer,DC=cis230,DC=local  
 Group Policy was applied From: cis230-wins2009.cis230.local  
 Group Policy slow link threshold: 1000ms  
 Domain Controller: CIS230  
 Domain Type: Windows 2008 or later

Applied Group Policy Objects  
 -----  
 Default Domain Policy  
 Local Group Policy  
 The computer is a part of the following security groups  
 -----  
 BUILTIN\Administrators  
 Everyone  
 BUILTIN\Users  
 NT AUTHORITY\ANONYMOUS  
 NT AUTHORITY\Authenticated Users  
 This Organization  
 CIS230-W05  
 Domain Computers  
 Authorization Authority asserted identity  
 System Mandatory Level

**Linux Post-Execution and deliverables**

5. Screenshots of any configuration changes made through the CLI not captured above

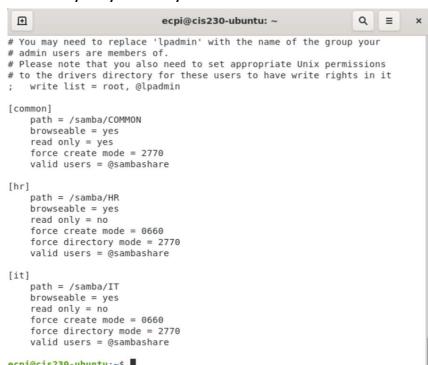
6. Screenshot showing group membership changes

a. cat /etc/groups

```
sambashare:x:134:jadams,mwilder,tevans
common:x:1002:tevans,jadams,mwilder
tr:x:1003:jadams
it:x:1004:tevans
jadams:x:1005:
mwilder:x:1006:
tevans:x:1007:
ntp:x:135:
```

7. Screenshots of samba configuration change:

a. cat /etc/samba/smb.conf



```
ecpi@cis230-ubuntu: ~
# You may need to replace 'lpadmin' with the name of the group your
# admin users are members of.
# Please note that you also need to set appropriate Unix permissions
# to the drivers directory for these users to have write rights in it
; write list = root, @lpadmin

[common]
path = /samba/COMMON
browseable = yes
read only = yes
force create mode = 0660
force directory mode = 2770
valid users = @sambashare

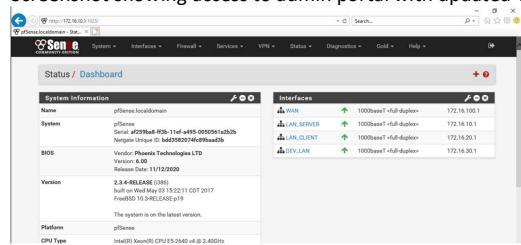
[hr]
path = /samba/HR
browseable = yes
read only = no
force create mode = 0660
force directory mode = 2770
valid users = @sambashare

[IT]
path = /samba/IT
browseable = yes
read only = no
force create mode = 0660
force directory mode = 2770
valid users = @sambashare

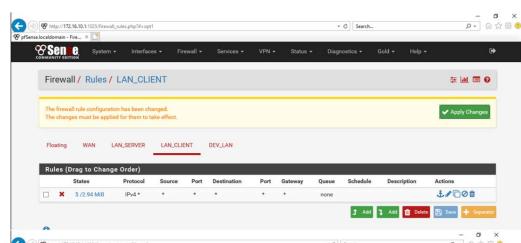
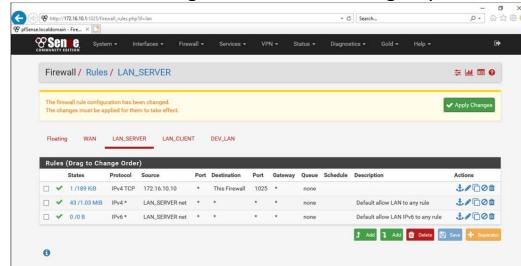
ecpi@cis230-ubuntu:~$
```

## Pfsense Firewall Post-Execution and deliverables

1. Screenshot of configuration changes
  - a. Screenshot showing access to admin portal with updated TCP port



- b. Screenshots of changes to GUI access change: System --> Advanced, and the Firewall rules



- c. Screenshots showing new administrative account and disabled default admin

Users				
Username	Full name	Status	Groups	Actions
admin	System Administrator	∅	admins	
bharding	W R Harding	✓	admins	
johan5257-ADMIN	John An	✓	admins	

### Follow-up

- Update documentation for stakeholders

### Progress Summary

1. Update project remediation plan with a summary of results and related audit findings that were remediated here:

#### The following Security Assessment Findings were remediated:

##### Windows

- No access should be given to HR department.
- Access to IT department should be granted only to their respective group.
- Users in all departments should be granted read-only access to COMMON, except for HR which should have the ability to create, edit, and delete files.

##### Linux

- Only the appropriate department groups should be granted full access, with no access given to the HR department.
- The IT department should only be accessible from its respective group.
- The COMMON network share should be set to read-only access for all users
- HR department should have permission to create, edit, and delete files.
- The root account should be disabled for SSH access to improve security.

##### Firewall

- Create new administrative account {studentid-ADMIN}
- Login and change password for admin and
- Set account properties to disable login.

2. System codes: LR – Linux Risk, WR – Windows Risk, FR – Firewall Risk
3. Submit your document in Canvas.

### Testing Procedures

- Notify Validation Group environment is ready for testing.

### Back out plan - List steps, DO NOT Execute

#### Windows System:

3. Revert settings to original values
4. Run a **gpupdate /force**

#### Linux System:

##### 3. Revert changes for groups

- a. Add users to original groups (add commands below)(Look up)
  - i. ProvideCommand 1:  
sudo usermod -a -G <group> <username>
- b. Remove users from newly assigned groups (add commands below)
  - i. Provide Command 1:  
sudo gpasswd -d tevans common  
sudo gpasswd -d tevans it  
sudo gpasswd -d jadams common  
sudo gpasswd -d jadams hr  
sudo gpasswd -d mwilder common

##### 4. Revert samba configuration change

- a. Set value for allowed users back to sambashares
  - i. Edit /etc/samba/smb.conf file
- b. Save config and restart services
  - i. sudo systemctl restart smbd
  - ii. sudo systemctl restart nmbd
  - iii. sudo service smbd status

### Project notes

Make sure you specify the systems that you are working on configuring as part of the change management process.

Server Info:

**(Virtual) Server Name:** CIS230-UBUNTU

**OS:** Ubuntu 9.4.0-1ubuntu1~20.04.2

**IP Address:** 172.16.30.30

**Server Specs:**

VM

CPU: Intel ® Xeon ® CPU E5-2640 v4 @ 240GHz

RAM: 1.9 GiB

STORAGE: 42.9 GB

NETWORK:

2 vCPU, 2GB RAM

**(Virtual) Server Name:** CIS230-WIN2019

**OS:** Windows Server 2019 Standard, 10.0.17763 Build 177763

**IP Address:** 172.16.10.10

**Server Specs:**

VM

**CPU:** Intel® Xeon® CPU E5-2640 v4 @ 2.40GHz, 2397 Mhz, 2 Core(s), 2 Logical Processor(s)

**RAM:** 4.00 GB

**STORAGE:** 60 GB

**NETWORK:** Intel® 82574L Gigabit Network Connection

2 vCPU, 2GB RAM

**(Virtual) Server Name:** CIS230-WIN10

**OS:** Windows 10 Education, 10.0.10240 Build 10240

**IP Address:** 172.16.20.20

**Server Specs:**

VM

**CPU:** Intel® Xeon® CPU E5-2640 v4 @ 2.40GHz, 2397 Mhz, 1 Core(s), 1 Logical Processor(s)

**RAM:** 2.00 GB

**STORAGE:** 40.00 GB

**NETWORK:** Intel® 82574L Gigabit Network Connection

2 vCPU, 2GB RAM

## Project Scope

### *WEEK 3 Vulnerabilities to Remediate*

**Windows Server** - (Default Domain Policy) Enable Windows Firewall, allow ICMP from internal segments, enable DEP (**Data Execution Prevention**) policies (Default Domain Policy). Same on (Domain Controllers) GPO but block policy inheritance and add allow ssh from Linux to the server. Enable DEP policies (Default Domain Policy)

*Demo:* Enable DEP policies

**Linux** - Enable ufw firewall and allow only NTP from internal segments, allow SSH from Win server and client segments, allow syslog from PfSense for firewall.

*Demo:* Allow syslog from PfSense for firewall

**PfSense** - (Firewall allows all traffic) Match the firewall rules configured for Windows and Linux and then research Active Directory required ports and set up firewall rules that allow both the Windows 10 client and Linux machine to access domain resources.

*Demo:* Create a firewall rule

## Project Lead

John An, johan5257

## Technical Stakeholders

William Harding

## Primary Business Users

Thomas Evans - IT Department

Janet Adams - Human Resources

Mary Wilder - Customer Service

## Project Summary

To achieve compliance with the items discovered in the voluntary security audit, several changes are proposed to address the issues listed in the project scope. The requirements for the necessary changes have been defined and low-level details of the specific changes are listed including validation. Risk has been assessed for contingency and backout plan is defined to respond in the event of an impact.

## Preparation

1. Create project implementation plan per system
  - a. Identify pre and post execution procedures (specific changes to be made and method for validation, i.e., commands or screenshots)
2. \*Notify Stakeholders (Peer review of changes) (Not required, for informational purposes.)

3. \*Schedule project in scheduled maintenance calendar (Not required, for informational purposes.)
4. Capture screenshot of current configuration and environment (i.e, make sure you're logged into the right system)
5. Apply changes (commands or screenshots)
6. Document applied settings (commands or screenshots)
7. Notify Validation Group environment is ready for testing. (Not required for informational purposes.)
8. Summarize scope of remediated vulnerabilities with reference to the specific audit findings for Final Report.
9. Submit completed document in Canvas.

#### VCastle Systems – Usernames and passwords

1. Windows 10	UN: cis230\administrator	PW: Password1	172.16.10.10
2. Ubuntu	UN: ecpi	PW: Password1	172.16.20.20
3. Server 2019	UN: cis230\administrator	PW: Password1	172.16.30.30
4. pfSense	UN: admin	PW: pfSense	172.16.100.1

#### Windows OS Execution Plan

##### Enable DEP policies for domain

1. Edit current **Windows Updates** settings on system Windows Server 2019
  - Go to **Server Manager** --> **Tools** --> **Group Policy Management**
  - Expand tree --> Right-click on **Default Domain Policy** --> **Edit**
  - Expand **Computer Configuration** section
  - Policies --> Windows settings --> Scripts (startup / shutdown)
    - i. Add a command (double-click) **startup** script, browse, and select: "powershell set-execution policy unrestricted.ps1"
    - ii. (Info only)Script has the following:

```
powershell.exe Set-ExecutionPolicy unrestricted
#####
bcdedit /set nx AlwaysOn
#####
```
8. Open command prompt or PowerShell --> Command: **gpupdate /force**

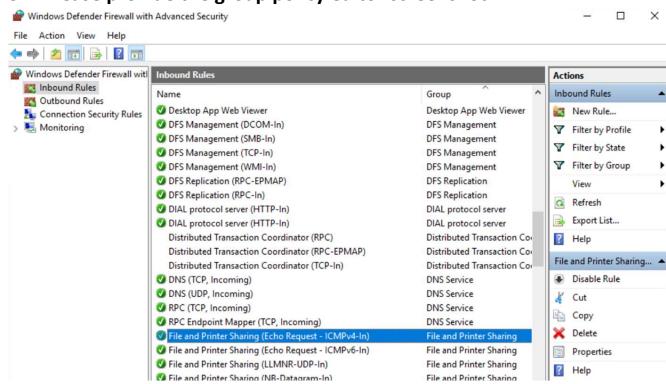
##### (Default Domain Policy) Enable Windows Firewall and allow ICMP from internal networks

1. **Enable Windows Firewall.**  
Tools > Windows Defender Firewall with Advanced Security

**2. Add firewall rule to allow ICMP from internal segments.**

Tools > Windows Defender Firewall with Advanced Security > Inbound > File and Printer Sharing (Echo Request – ICMPv4-In)

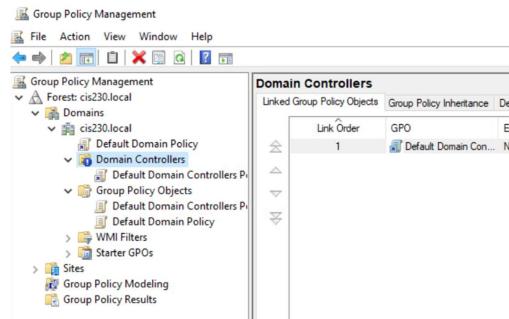
**3. Please provide the group policy editor screenshot**



(Default Domain Controllers Policy) Edit GPO to block policy inheritance, enable firewall, and add allow ping/ssh from Linux to the server

**1. Edit Domain Controllers GPO and disable inheritance –**

Group Policy Management > Forest > Domain Controllers > right click > Block Inheritance  
Provide the result screenshots



**2. Enable DEP policy**

- List all steps (will be same as for Default Domain Policy)

Edit current **Windows Updates** settings on system Windows Server 2019

- Go to **Server Manager** --> **Tools** --> **Group Policy Management**
- Expand tree --> Right-click on **Default Domain Policy** --> **Edit**

- Expand **Computer Configuration** section
- Policies --> Windows settings --> Scripts (startup / shutdown)
  - i. Add a command (double-click) **startup** script, browse, and select: "powershell set-execution policy unrestricted.ps1"
  - ii. (Info only)Script has the following:

```
powershell.exe Set-ExecutionPolicy unrestricted
#####
bcdedit /set nx AlwaysOn
```

### 3. Enable Windows firewall settings

- a. List all steps

Default Domain Controllers Policy > Policies > Computer Configuration > Policies > Windows Setting > Security Setting > Windows Defender Firewall with Advanced Security

### 4. Add firewall rules to allow icmp and ssh from Linux to Windows Server

- a. List all steps

Inbound rules > New Rules > Custom > Next > **Protocol Type: UDP, Local port: 80, Remote port: 22** > Local IP: 172.16.10.1, Remote IP: 172.16.30.1 > Next > Uncheck Public > Name the rule.

## Linux OS Execution Plan

### Add firewall rules

#### 8. Enable Ubuntu firewall

- a. sudo ufw enable

#### 9. Add rule to allow syslog traffic from the PfSense firewall:

- a. sudo ufw allow in on em1 from 172.16.10.1/24 to 172.16.30.1 proto udp port 514 (\*\*Change IP Address to match your network\*\*)

#### 10. Add rule to lock down ssh access to only allow from Windows Server

- a. (add commands)

```
ecpi@cis230-ubuntu:~$ sudo ufw allow in on em1 from 172.16.10.1/24 to 172.16.30.
b. 1 proto tcp port 22
```

#### 11. Add rule to lock down ntp access to only allow from internal networks

- a. (add commands)

```
ecpi@cis230-ubuntu:~$ sudo ufw allow in on em1 from 172.16.10.1/24 to 172.16.30.
1 proto udp port 123
```

## 12. Verify firewall rules

- a. sudo ufw status numbered –  add screenshot

```
ecpi@cis230-ubuntu:~$ sudo ufw status numbered -
Status: active
```

To	Action	From
--	--	--
[ 1] 172.16.30.1 514/udp on em1 ALLOW IN	172.16.10.0/24	
[ 2] 172.16.30.1 22/tcp on em1 ALLOW IN	172.16.10.0/24	
[ 3] 172.16.30.1 123/udp on em1 ALLOW IN	172.16.10.0/24	

## Pfsense Firewall Execution Plan

Allow ICMP between internal segments for each zone (REPEAT 3 TIMES and provide screenshot for each)

- Firewall --> Rules --> Click on LAN1/LAN2/LAN3 --> Click on Add with down arrow
  - Action: Pass
  - Interface: LAN1 em1 - LAN2 em2 - LAN3 em3
  - Protocol: ICMP
  - ICMP Subtypes: Select Echo Reply and Echo Request
  - Source: Network 172.16.0.0/22
  - Destination: Interface: LAN1- 172.16.10.1 - LAN2 - 172.16.20.1 -LAN3 172.16.30.1
  - Extra Options/Log: Check box for “Log packets that are handled by this rule”
  - Click Save at the bottom

Floating	WAN	LAN_SERVER	LAN_CLIENT	DEV_LAN						
<b>Rules (Drag to Change Order)</b>										
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 / 0 B	IPv4 ICMP echorep, echoreq	LAN_CLIENT net	*	LAN_CLIENT address	*	*	none		  
<b>Rules (Drag to Change Order)</b>										
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 / 0 B	IPv4 ICMP echorep, echoreq	DEV_LAN net	*	DEV_LAN address	*	*	none		  
<b>Rules (Drag to Change Order)</b>										
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 / 0 B	IPv4 ICMP echorep, echoreq	LAN_SERVER net	*	LAN_SERVER address	*	*	none		 

Add firewalls rules to lock down access between network segments

1. Firewall rule(s) allow traffic from Windows Server to Window 10 Client
  - a. Research is required for these firewall rules
  - b. Check Microsoft resources for required ports for Active Directory
2. Firewall rule allowing traffic from Windows 10 Client to Windows Server
  - a. Research is required for these firewall rules
  - b. Check Microsoft resources for required ports for Active Directory
3. Firewall rule(s) allowing traffic from Linux to Windows Server
  - a. Permit ports required for Active Directory
  - b. Permit HTTPS
4. Firewall rule(s) allowing traffic from Windows Server to Linux
  - a. Permit ports required for Active Directory
  - b. Permit SSH
  - c. Permit NTP
5. Firewall rule allowing traffic from Windows 10 Client to Linux
  - a. Permit NTP
  - b. Permit ports required for Windows/Samba shares (research for answer)
6. Three screenshots: Windows Server, Windows Client, and Linux.

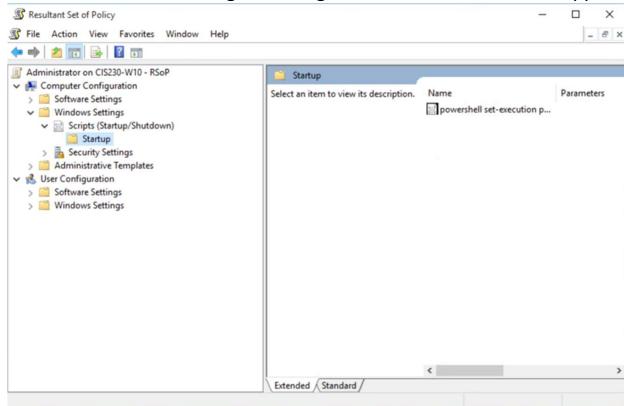
Rules (Drag to Change Order)										Actions
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/> ✓	0 / 0 B	IPv4 TCP/UDP	LAN_SERVER address	*	DEV_LAN address	22 - 389	*	none	3.8 Project: Pfsense execution 4	
<input type="checkbox"/> ✓	0 / 0 B	IPv4 TCP/UDP	DEV_LAN address	*	LAN_SERVER address	21 - 389	*	none	3.8 Project: Pfsense execution 3	
<input type="checkbox"/> ✓	0 / 0 B	IPv4 TCP/UDP	LAN_CLIENT address	*	LAN_SERVER address	21 - 5900	*	none	3.8 Project: Pfsense execution 2	
<input type="checkbox"/> ✓	0 / 0 B	IPv4 TCP/UDP	LAN_SERVER address	*	LAN_CLIENT address	21 - 5900	*	none	3.8 Project: Pfsense execution 1	
<input type="checkbox"/> ✓	0 / 0 B	IPv4 ICMP	LAN_SERVER net	*	LAN_SERVER address	*	*	none		
<input type="checkbox"/> ✓	0 / 3.36 MiB	IPv4 TCP	172.16.10.10	*	This Firewall	1025	*	none		
<input type="checkbox"/> ✓	5 / 131 KiB	IPv4 *	LAN_SERVER net	*	*	*	*	none	Default allow LAN to any rule	
<input type="checkbox"/> ✓	0 / 0 B	IPv6 *	LAN_SERVER net	*	*	*	*	none	Default allow LAN IPv6 to any rule	

Rules (Drag to Change Order)										Actions
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/> ✓	0 / 0 B	IPv4 TCP/UDP	LAN_CLIENT address	*	DEV_LAN address	123 - 465	*	none	3.8 Project: Pfsense execution 5	
<input type="checkbox"/> ✓	0 / 0 B	IPv4 TCP/UDP	LAN_SERVER address	*	LAN_CLIENT address	21 - 5900	*	none	3.8 Project: Pfsense execution 1	
<input type="checkbox"/> ✓	0 / 0 B	IPv4 TCP/UDP	LAN_SERVER address	*	DEV_LAN address	123 - 445	*	none	3.8 Project: Pfsense execution 4	
<input type="checkbox"/> ✓	0 / 0 B	IPv4 TCP/UDP	LAN_CLIENT address	*	LAN_SERVER address	21 - 5900	*	none	3.8 Project: Pfsense execution 2	
<input type="checkbox"/> ✓	0 / 0 B	IPv4 ICMP	LAN_CLIENT net	*	LAN_CLIENT address	*	*	none		
<input type="checkbox"/> ✓	0 / 0 B	IPv4 *	*	*	*	*	*	*	none	

Floating	WAN	LAN_SERVER	LAN_CLIENT	DEV_LAN						
Rules (Drag to Change Order)										
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/> <input checked="" type="checkbox"/>	0/0 B	IPv4 TCP/UDP LAN_CLIENT address	*	DEV_LAN address	123 - 465	*	none	3.8 Project: PfSense execution	5	
<input type="checkbox"/> <input checked="" type="checkbox"/>	0/0 B	IPv4 TCP/UDP LAN_SERVER address	*	DEV_LAN address	22 - 389	*	none	3.8 Project: PfSense execution	4	
<input type="checkbox"/> <input checked="" type="checkbox"/>	0/0 B	IPv4 TCP/UDP LAN_CLIENT address	*	DEV_LAN address	123 - 445	*	none			
<input type="checkbox"/> <input checked="" type="checkbox"/>	0/0 B	IPv4 TCP/UDP DEV_LAN address	*	LAN_SERVER address	21 - 389	*	none	3.8 Project: PfSense execution	3	
<input type="checkbox"/> <input checked="" type="checkbox"/>	0/0 B	IPv4 ICMP echoes, echoes	*	DEV_LAN net	*	*	*	none		
<input type="checkbox"/> <input checked="" type="checkbox"/>	0/0 B	IPv4 *	*	*	*	*	*	none		

### Windows Post-Execution and deliverables

10. For the server show screenshots of all group policy settings that were changed
11. Log onto Windows 10 client and run command prompt or PowerShell as Administrator
  - a. Type `rsop.msc`
  - b. Expand Computer Configuration section
  - c. Take screenshots showing all settings made on the server have applied successfully



### Linux Post-Execution and deliverables

8. Screenshots of all configuration changes made through the CLI
9. Screenshot showing firewall status and rules
  - a. `sudo ufw status numbered`

```
ecpi@cis230-ubuntu:~$ sudo ufw status numbered
[sudo] password for ecpi:
Status: active

To                         Action      From
--                         --          --
[ 1] 172.16.30.1 514/udp on em1 ALLOW IN   172.16.10.0/24
[ 2] 172.16.30.1 22/tcp on em1  ALLOW IN   172.16.10.0/24
[ 3] 172.16.30.1 123/udp on em1 ALLOW IN   172.16.10.0/24

ecpi@cis230-ubuntu:~$
```

## Pfsense Firewall Post-Execution and deliverables

### 2. Screenshots of firewall configurations

Rules (Drag to Change Order)										
State	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/> ✓	0 /0 B	IPv4 TCP	LAN_SERVER address	*	DEV_LAN address	22 - 389	*	none	3.8 Project: Pfsense execution 4	
<input type="checkbox"/> ✓	0 /0 B	IPv4 TCP	DEV_LAN address	*	LAN_SERVER address	21 - 389	*	none	3.8 Project: Pfsense execution 3	
<input type="checkbox"/> ✓	0 /0 B	IPv4 TCP	LAN_CLIENT address	*	LAN_SERVER address	21 - 5900	*	none	3.8 Project: Pfsense execution 2	
<input type="checkbox"/> ✓	0 /0 B	IPv4 TCP	LAN_SERVER address	*	LAN_CLIENT address	21 - 5900	*	none	3.8 Project: Pfsense execution 1	
<input type="checkbox"/> ✓	0 /0 B	IPv4 ICMP	echoreq, echores	net	*	LAN_SERVER address	*	*	none	
<input type="checkbox"/> ✓	0 /3.35 MIB Kib	IPv4 TCP	172.16.10.10	*	This Firewall	1025	*	none		
<input type="checkbox"/> ✓	0 /109	IPv4 *	LAN_SERVER net	*	*	*	*	none	Default allow LAN to any rule	
<input type="checkbox"/> ✓	0 /0 B	IPv6 *	LAN_SERVER net	*	*	*	*	none	Default allow LAN IPv6 to any rule	

Floating WAN LAN\_SERVER LAN\_CLIENT DEV\_LAN

Rules (Drag to Change Order)										
State	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/> ✓	0 /0 B	IPv4 TCP	LAN_CLIENT address	*	DEV_LAN address	123 - 465	*	none	3.8 Project: Pfsense execution 5	
<input type="checkbox"/> ✓	0 /0 B	IPv4 TCP	LAN_SERVER address	*	LAN_CLIENT address	21 - 5900	*	none	3.8 Project: Pfsense execution 1	
<input type="checkbox"/> ✓	0 /0 B	IPv4 TCP/UDP	LAN_SERVER address	*	DEV_LAN address	123 - 445	*	none		
<input type="checkbox"/> ✓	0 /0 B	IPv4 TCP	LAN_CLIENT address	*	LAN_SERVER address	21 - 5900	*	none	3.8 Project: Pfsense execution 2	
<input type="checkbox"/> ✓	0 /0 B	IPv4 ICMP	echoreq, echores	net	*	LAN_CLIENT address	*	*	none	
<input type="checkbox"/> ✓	0 /0 B	IPv4 *	*	*	*	*	*	*	none	

Floating WAN LAN\_SERVER LAN\_CLIENT DEV\_LAN

Floating	WAN	LAN_SERVER	LAN_CLIENT	DEV_LAN						
Rules (Drag to Change Order)										
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> B	0 /0	IPv4 TCP/UDP	LAN_CLIENT address	*	DEV_LAN address	123 - 465	*	none	3.8 Project: PfSense execution	
<input type="checkbox"/> <input checked="" type="checkbox"/> B	0 /0	IPv4 TCP/UDP	LAN_SERVER address	*	DEV_LAN address	22 - 389	*	none	3.8 Project: PfSense execution	
<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> B	0 /0	IPv4 TCP/UDP	LAN_CLIENT address	*	DEV_LAN address	123 - 445	*	none		
<input type="checkbox"/> <input checked="" type="checkbox"/> B	0 /0	IPv4 TCP/UDP	DEV_LAN address	*	LAN_SERVER address	31 - 389	*	none	3.8 Project: PfSense execution	
<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> B	0 /0	IPv4 ICMP	DEV_LAN net	*	DEV_LAN address	*	*	none		
<input type="checkbox"/> <input checked="" type="checkbox"/> B	0 /0	(IPv4 *)	*	*	*	*	*	none		

## Follow-up

Update documentation for stakeholders

## Progress Summary

1. Update project implementation plan with a summary of results and related audit findings that were remediated here:

### The following Security Assessment Findings were remediated:

**Windows Server** - (Default Domain Policy) Enable Windows Firewall, allow ICMP from internal segments, enable DEP (**Data Execution Prevention**) policies (Default Domain Policy). Same on (Domain Controllers) GPO but block policy inheritance and add allow ssh from Linux to the server. Enable DEP policies (Default Domain Policy)

**Linux** - Enable ufw firewall and allow only NTP from internal segments, allow SSH from Win server and client segments, allow syslog from PfSense for firewall.

**Pfsense** - (Firewall allows all traffic) Match the firewall rules configured for Windows and Linux and then research Active Directory required ports and set up firewall rules that allow both the Windows 10 client and Linux machine to access domain resources.

**System codes: LR – Linux Risk, WR – Windows Risk, FR – Firewall Risk**

2. Submit in Canvas

## Testing Procedures

- Notify Validation Group environment is ready for testing.

**Back out plan: revise each week as necessary. List steps, do not execute**

**Windows Server:**

5. Revert Default Domain Policy and Default Domain Controllers Policy GPO settings to original values
6. Run a **gpupdate /force**

**Linux System:**

5. **Disable firewall**
  - a. sudo ufw disable

**Pfsense System:**

1. **Revert configuration to previous version**

a. Diagnostics --> Config History --> select restore point and click 

### Project notes

Make sure you specify the systems that you are working on configuring as part of the change management process.

Server Info:

**(Virtual) Server Name:** CIS230-UBUNTU

**OS:** Ubuntu 9.4.0-1ubuntu1~20.04.2

**IP Address:** 172.16.30.30

**Server Specs:**

VM  
 CPU: Intel® Xeon® CPU E5-2640 v4 @ 240GHz  
 RAM: 1.9 GiB  
 STORAGE: 42.9 GB  
 NETWORK:  
 2 vCPU, 2GB RAM

**(Virtual) Server Name:** CIS230-WIN2019

**OS:** Windows Server 2019 Standard, 10.0.17763 Build 177763

**IP Address:** 172.16.10.10

**Server Specs:**

VM  
 CPU: Intel® Xeon® CPU E5-2640 v4 @ 2.40GHz, 2397 Mhz, 2 Core(s), 2 Logical Processor(s)  
 RAM: 4.00 GB  
 STORAGE: 60 GB  
 NETWORK: Intel® 82574L Gigabit Network Connection  
 2 vCPU, 2GB RAM

**(Virtual) Server Name:** CIS230-WIN10

**OS:** Windows 10 Education, 10.0.10240 Build 10240

**IP Address:** 172.16.20.20

**Server Specs:**

VM

**CPU:** Intel® Xeon® CPU E5-2640 v4 @ 2.40GHz, 2397 Mhz, 1 Core(s), 1 Logical Processor(s)

**RAM:** 2.00 GB

**STORAGE:** 40.00 GB

**NETWORK:** Intel® 82574L Gigabit Network Connection

2 vCPU, 2GB RAM

## Project Scope

### *WEEK 4 Vulnerabilities to Remediate*

**Windows Server** - Missing password policies, missing account lockout policies, all users member of Domain Admins

*Demo:* Review how/where to edit GPO's and Active Directory Users and Computers console

**Linux** - Disable root password, remove sudo access from non-admin users, enable and enforce secure password policies on Ubuntu local users

*Demo:* Enable and enforce secure password policies on Ubuntu local users

**Pfsense** - Create two groups, one with read only and one with admin privileges, create two users {studentID}-ro and {studentID}-rw privileges

*Demo:* Navigate GUI sections related to requirements

## Project Lead

John An

## Technical Stakeholders

Bill Harding

## Primary Business Users

Thomas Evans - IT Department

Janet Adams - Human Resources

Mary Wilder - Customer Service

## Project Summary

To achieve compliance with the items discovered in the voluntary security audit, several changes are proposed to address the issues listed in the project scope. The requirements for the necessary changes have been defined and low-level details of the specific changes are listed including validation. Risk has been assessed for contingency and backout plan is defined to respond in the event of an impact.

## Preparation

1. Create project remediation plan per system
  - a. Identify pre and post execution procedures (specific changes to be made and method for validation, i.e., commands or screenshots)
2. \*Notify Stakeholders (Peer review of changes) (Not required, for informational purposes.)
3. \*Schedule project in scheduled maintenance calendar (Not required, for informational purposes.)
4. Capture screenshot of current configuration and environment (i.e, make sure you're logged into the right system)
5. Apply changes (commands or screenshots)
6. Document applied settings (commands or screenshots)
7. Notify Validation Group environment is ready for testing. (Not required for informational purposes.)
8. Summarize scope of remediated vulnerabilities with reference to the specific audit findings for Final Report.
9. Submit completed document in Canvas.

### VCastle Systems – Usernames and passwords:

1. Windows 10	UN: cis230\administrator	PW: Password1	172.16.10.10
2. Ubuntu	UN: ecpi	PW: Password1	172.16.20.20
3. Server 2019	UN: cis230\administrator	PW: Password1	172.16.30.30
4. pfSense	UN: admin	PW: pfSense	172.16.100.1

### Windows OS Execution Plan

#### All users member of Domain Admins

Edit and update existing Active Directory user/group configurations

#### Conditions:

\*(Remove non IT users from IT group, Create an IT\_AdminAccess group and add to Domain Admins, create separate account for IT users' administrative actions, add to new group, and remove the "IT" user group from Domain Admins)

#### 1. Edit Active Directory Users and Computers configuration

- Go to Server Manager --> Tools --> Active Directory Users and Computers
- List remaining steps:

##### Create IT\_AdminAccess group:

- Right-click Users > New > Group > Group Name: IT\_AdminAccess

##### Add to Domain Admin:

- Right-click IT\_AdminAccess > Properties > Members > Remove IT user

##### Create IT Admin user:

- Right-click User > Properties > New > User > First name: IT Admin, User logon name: ITAdmin, Password: Password1

**Remove Domain Admin from IT group:**

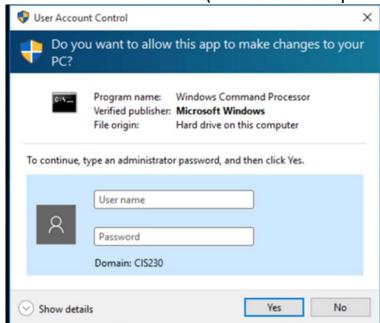
- Right-click the group IT > Properties > Member Of > Remove **Domain Admins**

**Add John An to IT group:**

- Right-click **User** > **Properties** > **New** > **User** > First name: **John**, User logon name: **jan**, Password: **Password1**

## 2. Verify administrative login on Windows 10 client

- Log in as normal IT user account
- Complete an admin function and take screenshots of successful action with new admin actions account for and execution (include admin prompt login)



**Enable and set password policies:**

Password History = 24

Maximum password age = 90 days

Minimum password age = 5 days

Enable Complexity requirements

Minimum password length = 12 characters

### 1. List steps & provide screenshot:

Right-click Default Domain Controller Policy > Edit > Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy

- Enforce Password history: 24
- Max password age: 90
- Min password age: 5
- Password must meet complexity requirements: Enabled
- Min password length: 12

**Enable and set account lockout policies**

### 1. List steps & provide screenshot:

Right-click Default Domain Controller Policy > Edit > Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Account Lockout Policy

- Account lockout duration: 45 mins
- Account lockout threshold: 5 invalid logon attempts
- Reset account lockout counter after: 30 mins

## Linux OS Execution Plan

### Enable and enforce secure password policies

The following is also an example of how you can manually change the explicit expiration date (-E) to 01/31/2030, minimum password age (-m) of 5 days, maximum password age (-M) of 90 days, inactivity period (-I) of 30 days after password expiration, and a warning time period (-W) of 14 days before password expiration:

```
sudo chage -E 01/31/2030 -m 5 -M 90 -I 30 -W 14 username
```

*Before:*

```
ecpi@cis230-ubuntu:~$ sudo chage -l jadams
Last password change : Dec 07, 2021
Password expires     : never
Password inactive   : never
Account expires      : never
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires: 7
ecpi@cis230-ubuntu:~$
```

### Edit user accounts with password settings and expiry

1. List steps

Terminal > **sudo chage -E 01/31/2030 -m 5 -M 90 -I 30 -W 14 jadams**

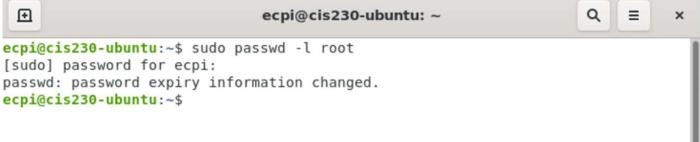
Screenshot:

```
ecpi@cis230-ubuntu:~$ sudo chage -E 01/31/2030 -m 5 -M 90 -I 30 -W 14 jadams
ecpi@cis230-ubuntu:~$ sudo chage -l jadams
Last password change          : Dec 07, 2021
Password expires              : Mar 07, 2022
Password inactive             : Apr 06, 2022
Account expires                : Jan 31, 2030
Minimum number of days between password change : 5
Maximum number of days between password change : 90
Number of days of warning before password expires: 14
ecpi@cis230-ubuntu:~$
```

### Disable root password

1. List steps

Terminal > sudo passwd -l root



```
ecpi@cis230-ubuntu:~$ sudo passwd -l root
[sudo] password for ecpi:
passwd: password expiry information changed.
ecpi@cis230-ubuntu:~$
```

### Remove sudo access from non-admin users

1. List steps

sudo deluser jadams sudo  
sudo deluser mwilder sudo

```
ecpi@cis230-ubuntu:~$ getent group sudo
sudo:x:27:ecpi,administrator,jadams,mwilder,tevans
ecpi@cis230-ubuntu:~$ sudo deluser jadams sudo
Removing user `jadams' from group `sudo' ...
Done.
ecpi@cis230-ubuntu:~$ sudo deluser mwilder sudo
Removing user `mwilder' from group `sudo' ...
Done.
ecpi@cis230-ubuntu:~$
```

### Pfsense Firewall Execution Plan

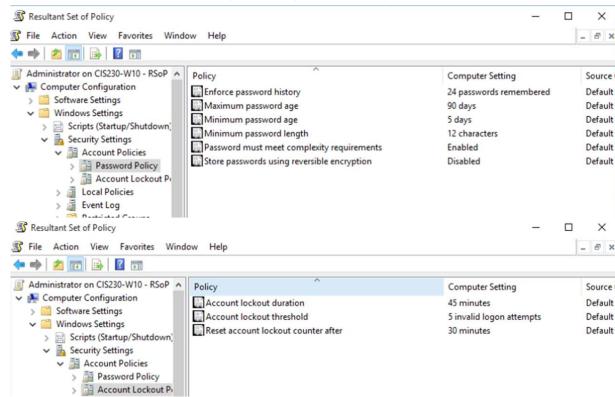
#### Configure access users and groups for read-only and read-write levels of administrative access

2. System --> User Manager -->

- a. Create RO and RW administrative groups
  - i. RO is read only
  - ii. RW allows admin/write access
- b. Create two user accounts and add to respective groups
  - i. studentID-ro
  - ii. studentID-rw
- c. Log in with RO account and confirm unable to make changes
- d. Log in with RW account and confirm changes can be made

### Windows Post-Execution and deliverables:

12. Log onto Window 10 client as a domain admin
13. Run command prompt or PowerShell as Administrator
  - a. Type **rsop.msc**
  - b. Expand Computer Configuration section
  - c. Take screenshot showing settings have applied successfully



### Linux Post-Execution and deliverables:

10. Screenshots of all configuration changes made through the CLI

```
ecpi@cis230-ubuntu:~$ sudo chage -E 01/31/2030 -m 5 -M 90 -I 30 -W 14 jadams
ecpi@cis230-ubuntu:~$ sudo chage -l jadams
Last password change : Dec 07, 2021
Password expires       : Mar 07, 2022
Password inactive     : Apr 06, 2022
Account expires        : Jan 31, 2030
Minimum number of days between password change : 5
Maximum number of days between password change : 90
Number of days of warning before password expires : 14
ecpi@cis230-ubuntu:~$
```

```
ecpi@cis230-ubuntu:~$ sudo passwd -l root
[sudo] password for ecpi:
passwd: password expiry information changed.
ecpi@cis230-ubuntu:~$
```

```

ecpi@cis230-ubuntu:~$ getent group sudo
sudo:x:27:ecpi,administrator,jadams,mwilder,tevans
ecpi@cis230-ubuntu:~$ sudo deluser jadams sudo
Removing user `jadams' from group `sudo' ...
Done.
ecpi@cis230-ubuntu:~$ sudo deluser mwilder sudo
Removing user `mwilder' from group `sudo' ...
Done.
ecpi@cis230-ubuntu:~$ 

```

11. Screenshot showing

- a. sudo ufw status numbered

```

ecpi@cis230-ubuntu:~$ sudo ufw status numbered
[sudo] password for ecpi:
Status: active

To                         Action      From
--                         --          --
[ 1] 172.16.30.1 514/udp on em1 ALLOW IN   172.16.10.0/24
[ 2] 172.16.30.1 22/tcp on em1  ALLOW IN   172.16.10.0/24
[ 3] 172.16.30.1 123/udp on em1 ALLOW IN  172.16.10.0/24

ecpi@cis230-ubuntu:~$ 

```

### Pfsense Firewall Post-Execution and deliverables:

3. Screenshots of firewall configurations

**Group creation for johan5257-ro / johan5257-rw:**

Group name	Description	Member Count	Actions
admins	System Administrators	3	
all	All Users	5	
johan5257-ro		1	
johan5257-rw		2	

Group Properties											
Group name	<input type="text" value="johan5257-ro"/>										
Scope	Local										
Description											
Group description, for administrative information only											
Group membership	<table border="1"> <tr> <td>admin</td> <td><input type="checkbox"/></td> </tr> <tr> <td>bharding</td> <td><input type="checkbox"/></td> </tr> <tr> <td>johan5257-ADMIN</td> <td><input type="checkbox"/></td> </tr> <tr> <td>johan5257-ro</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>Not members</td> <td><input type="checkbox"/></td> </tr> </table>	admin	<input type="checkbox"/>	bharding	<input type="checkbox"/>	johan5257-ADMIN	<input type="checkbox"/>	johan5257-ro	<input checked="" type="checkbox"/>	Not members	<input type="checkbox"/>
admin	<input type="checkbox"/>										
bharding	<input type="checkbox"/>										
johan5257-ADMIN	<input type="checkbox"/>										
johan5257-ro	<input checked="" type="checkbox"/>										
Not members	<input type="checkbox"/>										
<input type="button" value="More to Members"/> <input type="button" value="More to Non-members"/>											

Assigned Privileges		
Name	Description	Action
User - Config: Deny Config Write	If present, ignores requests from this user to write config.xml.	
WebCfg - Dashboard (all)	Allow access to all pages required for the dashboard.	

### User creation for johan5257-ro / johan5257-rw:

The screenshot shows the 'Group Properties' page in a web-based user management interface. The 'Groups' tab is active. A group named 'johan5257-ro' is selected. The 'Group membership' section lists members: 'admin' and 'johan5257-ro'. The 'Assigned Privileges' section shows a single privilege: 'Allow access to all pages'.

### Follow-up

- Update documentation for stakeholders

### Progress Summary

1. Update project remediation plan with a summary of results and related audit findings that were remediated here:

**The following Security Assessment Findings were remediated:**

1. Windows Server – Domain Admins Group Misconfiguration
2. Windows Server – Missing Password Policies
3. Windows Server – Missing Account Lockout Policies
4. Linux – Weak User Access Control
5. Linux – Weak Password Policies
6. pfSense Firewall – Lack of Role-Based Access Control

**System codes: LR – Linux Risk, WR – Windows Risk, FR – Firewall Risk**

2. Submit in Canvas

### Testing Procedures

Notify Validation Group environment is ready for testing.

### Back out plan: revise each week as necessary. List steps, do not execute

#### Windows Server:

7. Revert settings to original values
8. Run a **gpupdate /force**

#### Linux System:

6. **Disable firewall**
  - a. sudo ufw disable

**Pfsense Firewall:****2. Revert configuration to previous version**

- a. Diagnostics --> Config History --> select restore point and click 

**Project notes**

Make sure you specify the systems that you are working on configuring as part of the change management process.

Server Info:

**(Virtual) Server Name:** CIS230-UBUNTU

**OS:** Ubuntu 9.4.0-1ubuntu1~20.04.2

**IP Address:** 172.16.30.30

**Server Specs:**

VM

CPU: Intel® Xeon® CPU E5-2640 v4 @ 240GHz

RAM: 1.9 GiB

STORAGE: 42.9 GB

NETWORK:

2 vCPU, 2GB RAM

**(Virtual) Server Name:** CIS230-WIN2019

**OS:** Windows Server 2019 Standard, 10.0.17763 Build 177763

**IP Address:** 172.16.10.10

**Server Specs:**

VM

CPU: Intel® Xeon® CPU E5-2640 v4 @ 2.40GHz, 2397 Mhz, 2 Core(s), 2 Logical Processor(s)

RAM: 4.00 GB

STORAGE: 60 GB

NETWORK: Intel® 82574L Gigabit Network Connection

2 vCPU, 2GB RAM

**(Virtual) Server Name:** CIS230-WIN10

**OS:** Windows 10 Education, 10.0.10240 Build 10240

**IP Address:** 172.16.20.20

**Server Specs:**

VM

CPU: Intel® Xeon® CPU E5-2640 v4 @ 2.40GHz, 2397 Mhz, 1 Core(s), 1 Logical Processor(s)

RAM: 2.00 GB



52

**STORAGE:** 40.00 GB

**NETWORK:** Intel® 82574L Gigabit Network Connection

2 vCPU, 2GB RAM

## Project Scope

### *WEEK 5 Vulnerabilities to Remediate*

**Windows Server** - Add SSL to IIS website, configure public key logon to Linux server (generate ssh keys and copy over to Linux).

*Demo:* Configure CA role and certificate templates.

**Linux** - Configure sshd\_config to allow public key authentication, create two users {studentID}-ro and {studentID}-rw with passwords and generate RSA keys for each for access to the Pfsense firewall.

*Demo:* Add Windows CA certificate as a trusted Root CA.

**Pfsense** - Enable secured SSH access and require public key authentication, add generated SSH keys from Linux users {studentID}-ro and {studentID}-rw, change to custom port 2022.

*Demo:* Navigate GUI sections related to requirements.

## Project Lead

John An

## Technical Stakeholders

Bill Harding

## Primary Business Users

Thomas Evans - IT Department

Janet Adams - Human Resources

Mary Wilder - Customer Service

## Project Summary

To achieve compliance with the items discovered in the voluntary security audit, several changes are proposed to address the issues listed in the project scope. The requirements for the necessary changes have been defined and low-level details of the specific changes are listed including validation. Risk has been assessed for contingency and backout plan is defined to respond in the event of an impact.

## Preparation

1. Create project remediation plan per system
  - a. Identify pre and post execution procedures (specific changes to be made and method for validation, i.e., commands or screenshots)
2. \*Notify Stakeholders (Peer review of changes) (Not required, for informational purposes.)
3. \*Schedule project in scheduled maintenance calendar (Not required, for informational purposes.)
4. Capture screenshot of current configuration and environment (i.e, make sure you're logged into the right system)
5. Apply changes (commands or screenshots)
6. Document applied settings (commands or screenshots)
7. Notify Validation Group environment is ready for testing. (Not required for informational purposes.)
8. Summarize scope of remediated vulnerabilities with reference to the specific audit findings for Final Report.
9. Submit completed document in Canvas.

### VCastle Systems – Usernames and passwords:

1. Windows 10	UN: cis230\administrator	PW: Password1	172.16.10.10
2. Ubuntu	UN: ecpi	PW: Password1	172.16.20.10
3. Server 2019	UN: cis230\administrator	PW: Password1	172.16.30.10
4. pfSense	UN: admin	PW: pfSense	172.1.100.1

## Icon Legend

You will see the following icons to indicate if the project step or activity will be done with the instructor, in your group, or independently.



: Represents Instructor Led activities



: Represents group activities



: Represents individual activities



: Represents screenshot requirement

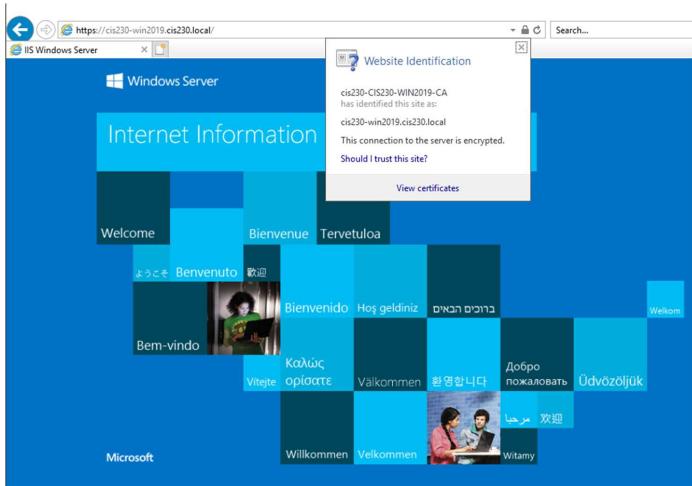
## Windows OS Execution Plan

### Configure Certification Authority Role on Windows Server

1. Server Manager -> Add the Role
  - a. **Next** on first screen
  - b. Leave “Role-based or Feature-based installation” selected and click next
  - c. Leave default for “Destination Server” and **Click next**
  - d. **Select**
    - i. Active Directory Certificate Services
    - ii. Certification Authority and Web Enrollment should be Selected
    - iii. --> on prompt click “Add Features”
    - iv. Click next and then next again
  - e. Leave defaults and continue through to install
2. Once install is complete click on the  and then on “Configure Active Directory...”
  - a. Leave default on first prompt and **Click Next**
  - b. Check the box for Certification Authority and select Web Enrollments.
  - c. **Click Next** through all of the remaining prompts
3. **Configure web server template and issue certificate**
  - a. Server Manager --> Tools --> Certification Authority – Expand cis230
  - b. **Right-click** on Certificate Templates --> select Manage (opens Certificate Template Console)
  - c. Find and Right-click on Web Server --> select Duplicate Template
    - i. **Click** on General tab
    - ii. **Change** Template display name: Web-Server-Template -->
    - iii. **Check** box for “Publish certificate in Active Directory”
    - iv. **Click** on Subject Name tab
    - v. **Select** “Build from this Active Directory Information”
    - vi. **Select** from dropdown Subject name format: DNS name --> under Include this information in alternate subject name: check DNS name box
    - vii. **Click** on Security tab --> with Authenticated Users selected --> Permissions for Authenticated Users: check Enroll box in Allow column
    - viii. **Close** Certificate Template Console by selecting OK and you’re back at Certification Authority
  - d. Issue Certificate Template
    - i. **Right-click** on Certificate Templates -->
    - ii. **Select** New - Certificate Template to Issue (opens Enable Certificate Templates prompt) -->
    - iii. **Select** Web-Server-Template and click OK.
    - iv. **Close** dialog box.
  - e. Create new certificate for Web Server
    - i. **Right Click** on Windows start. Select Run and type **mmc**. Click OK(openes empty console)
    - ii. **Click on File** --> Add/Remove snap-in (opens prompt) --> select Certificates **Select** Add and Computer Account. Select Local computer.

- iii. **Click Finish and OK.** (closes prompt and back at main window)
  - iv. **Expand Certificates** - Personal --> Certificates (you see one certificate and we will add a new one to use in IIS) -->
  - v. **Right-click** All Tasks --> Request New Certificate (prompt opens).
  - vi. **Select** next.Certificate Enrollment prompt -->
  - vii. **Click** next for following two prompt --> Request Certificates -->
  - viii. **Select** and right-click on Web-Server-Template --> Certificate Properties --> Friendly name: CIS230-SSL-WEB and click ok --> click Enroll and then Finish
  - ix. **Save Root CA Certificate to file (**DO NOT EXPORT PRIVATE KEY**)**
  - x. On PowerShell type the following command
    1. cd into where you saved the cert file: scp .\fileName  
<student@192.168.1.10:/home/student/>
    2. Check the firewall if cannot connect
  - xi. **Close mmc**
  - xii. **Na**
- 4. Enable SSL and set new certificate**
- i. Server Manager --> Tools --> Internet Information Services -->
  - ii. **Expand** LAB-SRV-DC01 --> expand Sites -->
  - iii. **Click on** Default Web Site --> on right side under “Actions” and “Edit Site”
  - iv. **Click on “Bindings...”** --> prompt opens for Site Bindings -->
  - v. **Click Add....**--> prompt opens Add Site Binding -->
  - vi. Set Type to https (SSL Certificate: will now show) and select CIS230-SSL-Web and click OK -->
  - vii. Click Close on Site Bindings --> back on main IIS window on the right side and under “Manage Website”, click on Restart
- b. Verify SSL on Web Server**
- i. Open up an Internet browser and go to <https://lab-srv-dc01-cis230-lab.local> (may show as cis230-win2019.cis230.local) and the little lock should show as trusted site.  
<lab-srv-dc01.cis230-lab.local/>

**Commented [QL1]: This was not included in the original document.**



### Configure RSA keys for Administrator and copy to Linux for public key logon. (Powershell)

1. ssh-keygen -t rsa
2. Accept all prompts (pay attention to where the files are saved)

```
PS C:\Users\Administrator> ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (C:/Users/Administrator/.ssh/id_rsa):
Created directory 'C:/Users/Administrator/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:/Users/Administrator/.ssh/id_rsa.
Your public key has been saved in C:/Users/Administrator/.ssh/id_rsa.pub.
The key's randomart image is:
+---[RSA 2048]---+
|oo.o
|oo+...
|+++.o
|+. .o o
|=B .o S
|+=o .
|o* .+o X o
|o..oE * *
|+o. .
+---[SHA256]-----+
PS C:\Users\Administrator>
```

3. scp copy file from the server to the appropriate director
4. You should log in to the Linux server without password

**Note:**Linux part must be completed to validate public key login.

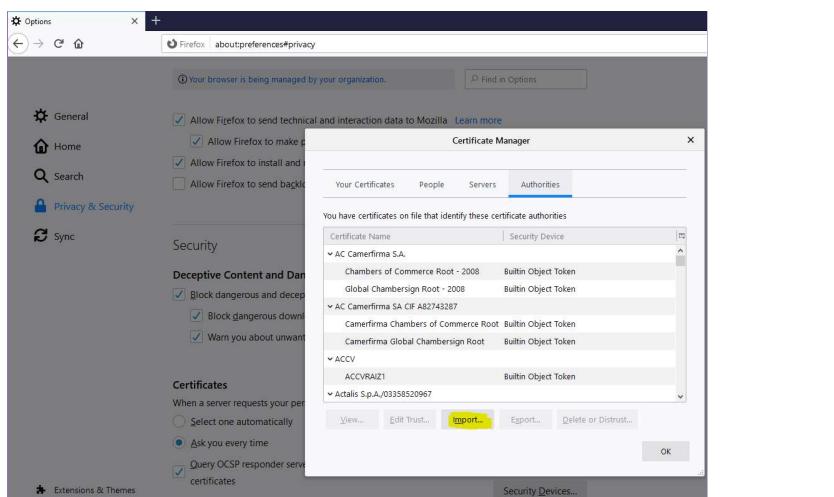


### Linux OS Execution Plan

Modify /etc/hosts to Resolve Windows webpage



3. Open Internet browser and go to the IIS website
  - a. On Firefox, you will manually add the win-ca-cert.crt file to Trusted Root Certification Authority (located in Downloads)
    - i. Open Firefox and go to Options:
    - ii. Click Privacy & Security in the left-hand menu and scroll down to Certificates.
    - iii. Click View Certificates... and the Certificate Manager window displays.
    - iv. Click Authorities and then Import
    - v. Browse to locate the downloaded ca
    - vi. Click OK



### Configure users with RSA keys for access to Pfsense firewall over SSH

1. Create users {studentID}-ro and {studentID}-rw and set passwords that meet complexity requirements
  - a. List steps and provide screenshots

Create user with **johan5257-ro** and **johan5257-rw**  
Create password: **Password1**



## 2. Generate RSA keys for new users (with no passphrase)

- List steps and provide screenshots
  - Type: ssh-keygen -b 4096 in powershell on Windows Server.
  - Go to C:\Users\Administrator/.ssh/id\_rsa
  - Copy the content
  - On the pfSense firewall configurator, go to System > User Manager > Users
  - Paste into the RSA SSH key in the users Johan5257-ro/Johan5257-rw input for the SSH key.

```
S C:\Users\Administrator> ssh-keygen -b 4096
enerating public/private rsa key pair.
enter file in which to save the key (C:\Users\Administrator/.ssh/id_rsa):
:Users\Administrator/.ssh/id_rsa already exists.
overwrite (y/n)? y
enter passphrase (empty for no passphrase):
enter same passphrase again:
our identification has been saved in C:\Users\Administrator/.ssh/id_rsa.
our public key has been saved in C:\Users\Administrator/.ssh/id_rsa.pub.
he key fingerprint is:
HA256:vHZeYa5Ggq8sshBHL04X1TVvK6hw5TKhGCrD2cjigC0 cis230\administrator@cis230-win2019
he key's randomart image is:
---[RSA 4096]---
. . +
=*= . * + .
E++* o =
*= + +.. .
.o... .S
.o . ....
... . .oo. o
.o . .o+ .
.o . .o+ .
---[SHA256]---+
S C:\Users\Administrator>
```



### Configure sshd\_config to allow public key authentication

- List steps

To configure the `sshd\_config` file to allow public key authentication, follow these steps:

#### Step 1: Open the SSH Daemon Configuration File

Use your favorite text editor to open the `sshd\_config` file. You may need root privileges to edit this file.

```
```bash
```

```
sudo nano /etc/ssh/sshd_config
```

...

### Step 2: Enable Public Key Authentication

Locate the following lines and make sure they are configured as shown:

```
```bash
# Ensure the following options are set to "yes"
PubkeyAuthentication yes
AuthorizedKeysFile .ssh/authorized_keys
````
```

If these lines are commented out (with a '#'), remove the '#' at the beginning.

### Step 3: Disable Password Authentication (Optional but recommended for security)

To increase security, you can disable password authentication:

```
```bash
PasswordAuthentication no
````
```

### ### Step 4: Save and Exit

Press 'CTRL + O' to save the file and 'CTRL + X' to exit the editor.

### ### Step 5: Restart the SSH Service

Restart the SSH daemon to apply changes:

```
```bash
sudo systemctl restart sshd
````
```

### Step 6: Check SSH Service Status

To ensure the SSH service is running without issues:

```
```bash
sudo systemctl status sshd
```
```

```

#### Step 7: Upload Your Public Key

Copy your public key to the server's authorized keys file using the `ssh-copy-id` command:

```
```bash
ssh-copy-id user@server_ip
```
```

```

#### Step 8: Test the Configuration

Try logging in to your server via SSH to ensure that public key authentication works:

```
```bash
ssh user@server_ip
```
```

```

You should be able to log in without being prompted for a password, provided your private key is loaded or accessible.

#### Pfsense Firewall Execution Plan: - logon to pfSense from Ubuntu



Enable SSH access to firewall and change default port to 2022

3. List steps and provide screenshot

**Source**

Source  Invert match. DEV\_LAN address

**Destination**

Destination  Invert match. any

Destination Port Range (other) 2022 (other)

From To

Firewall / Rules / WAN

The firewall rule configuration has been changed.  
The changes must be applied for them to take effect.

Floating WAN LAN\_SERVER LAN\_CLIENT DEV\_LAN

**Rules (Drag to Change Order)**

Status	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	DEV_LAN address	*	2022	*	none			
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	*	*	*	*	none			

Add Edit Delete Save Separate



Add SSH Keys for accounts {studentID}-ro and studentID)-rw for public key authentication

1. List steps and provide screenshot

Go to C:\Users\Administrator/.ssh/id\_rsa

Copy the content

On the pfSense firewall configurator, go to System > User Manager > Users

Paste into the RSA SSH key in the users Johan5257-ro/Johan5257-rw input for the SSH key.

File Home Share View

This PC Local Disk (C:) Users Administrator .ssh

Name	Date modified	Type	Size
id_rsa	4/2/2025 11:26 AM	File	4 KB
id_rsa.pub	4/2/2025 11:26 AM	PUB File	1 KB

id\_rsa.pub - Notepad

```
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQAC65v701s2y+IMayKmuBhKhVXPKI1r2h2ij84D0d0qynK7pSEgaziZQN9gRb
```

The screenshot shows the pfSense user manager interface. On the left, there's a sidebar with 'User Manager' and 'Groups'. The main area has tabs for 'Users' and 'Groups'. Under 'Users', there are sections for 'Inherited from', 'Name', 'Description', 'User Certificates', 'Keys', and 'IPsec Pre-Shared Key'. The 'Keys' section contains two fields: 'Authorized SSH Keys' and 'Authorized IPsec Keys'. Both fields show placeholder text for RSA and DSA keys respectively. On the right, there's a 'User Certificates' section with a table showing a single entry for 'CA'.



### Update firewall rules to allow Linux and port 2022

1. List steps and provide screenshot

#### Access Firewall Rules:

Go to Firewall → Rules → WAN.

#### Add a New Rule:

Click Add to create a new rule.

#### Rule Configuration:

Action: Pass

Interface: WAN

Address Family: IPv4 (or IPv4+IPv6 if applicable)

Protocol: TCP

Source: Any (or specify your Linux system's IP/subnet)

Destination: This Firewall (self)

Destination Port Range: Custom, enter 2022

Description: Allow SSH on port 2022

#### Save and Apply Changes:

Click Save and Apply Changes.

#### Verify the Rule:

Go to Diagnostics → States and check if the rule is applied correctly.

The screenshot shows the pfSense Diagnostic States interface. At the top, there are tabs for 'Floating', 'WAN', 'LAN\_SERVER', 'LAN\_CLIENT', and 'DEV\_LAN'. The 'WAN' tab is selected. Below the tabs is a table titled 'Rules (Drag to Change Order)'. The table has columns for States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, and Des. There is one row listed: '0 / 0 B' for IPv4 TCP, source '\*', destination 'This Firewall', port 2022, gateway '\*', queue 'none', and schedule 'none'.



### Windows Post-Execution and deliverables:

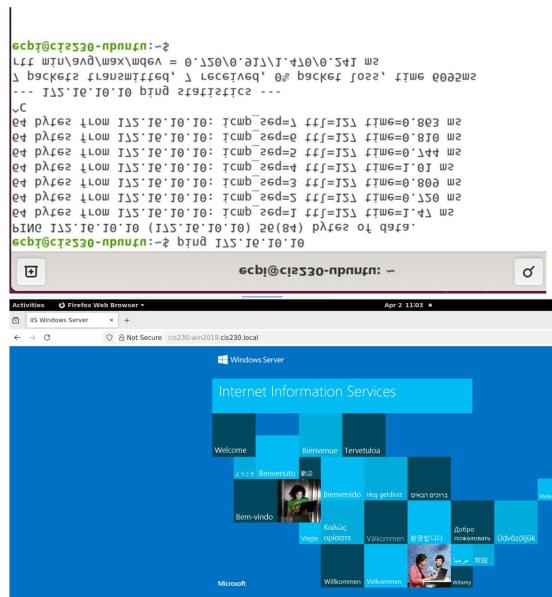
14. Log onto Window 10 client for screenshot showing the browser accessing the FQDN of the domain controller and shows as trusted site
15. On the Windows Server screenshots
  - a. All configurations made through the CLI
  - b. Logon to Linux server with password and then after with public key authentication enabled

**Cannot Verify and Screenshot because the public key authentication was not successful and the instruction was not sufficient.**



### Linux Post-Execution and deliverables:

1. Screenshots of all configuration changes made through the CLI
2. Screenshot showing generated RSA keys
3. Screenshot showing the browser accessing FQDN of the domain controller and shows as trusted site



**These screenshot to verify connection to Windows Server's IIS.**

**Screenshot for RSA was not provided because the instruction was not sufficient.**



### Pfsense Firewall Post-Execution and deliverables:

#### 4. Screenshots of firewall configurations

The screenshots show the configuration of a firewall with five zones: Floating, WAN, LAN\_SERVER, LAN\_CLIENT, and DEV\_LAN. Each zone has its own set of rules defined in a table with columns for State, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions.

- Floating Zone:**

State	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions				
0 / 0 B	IPv4 TCP	*	*	This Firewall	2022	*	none							
0 / 0 B	IPv4 TCP	DEV_LAN address	*	*	2022	*	none							
0 / 0 B	IPv4 *	*	*	*	*	*	none							
- WAN Zone:**

State	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions				
0 / 0 B	IPv4 TCP	*	*	DEV_LAN net (SSH)	22	*	none							
0 / 0 B	IPv4 TCP	LAN_SERVER address	*	DEV_LAN address	22 - 389	*	none	3.8 Project: Pfsense execution	4					
0 / 0 B	IPv4 TCP/UDP	DEV_LAN address	*	LAN_SERVER address	21 - 389	*	none	3.8 Project: Pfsense execution	3					
0 / 0 B	IPv4 TCP/UDP	LAN_CLIENT address	*	LAN_SERVER address	21 - 5900	*	none	3.8 Project: Pfsense execution	2					
0 / 0 B	IPv4 TCP/UDP	LAN_SERVER address	*	LAN_CLIENT address	21 - 5900	*	none	3.8 Project: Pfsense execution	1					
0 / 0 B	IPv4 ICMP	LAN_SERVER net 10.20.0.0/24	*	LAN_SERVER adminstr	*	*	none							
0 / 352 KB	IPv4 TCP	172.16.10.10	*	This Firewall	1025	*	none							
0 / 162 KB	IPv4 *	LAN_SERVER net	*	*	*	*	none	Default allow LAN to any rule						
0 / 0 B	IPv6 *	LAN_SERVER net	*	*	*	*	none	Default allow LAN IPv6 to any rule						
- LAN\_SERVER Zone:**

State	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions				
0 / 0 B	IPv4 TCP	LAN_CLIENT address	*	DEV_LAN address	123 - 465	*	none	3.8 Project: Pfsense execution 5						
0 / 0 B	IPv4 TCP/UDP	LAN_SERVER address	*	LAN_CLIENT address	21 - 5900	*	none	3.8 Project: Pfsense execution 1						
0 / 0 B	IPv4 TCP/UDP	LAN_SERVER address	*	DEV_LAN address	123 - 445	*	none	3.8 Project: Pfsense execution 4						
0 / 0 B	IPv4 TCP/UDP	LAN_CLIENT address	*	LAN_SERVER address	21 - 5900	*	none	3.8 Project: Pfsense execution 2						
0 / 0 B	IPv4 ICMP	LAN_CLIENT net 10.20.0.0/24	*	LAN_CLIENT address	*	*	none							
2 / 481 KB	IPv4 *	*	*	*	*	*	none							
- LAN\_CLIENT Zone:**

State	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions				
0 / 0 B	IPv4 TCP	*	*	DEV_LAN net (SSH)	*	*	none	3.8 Project: Pfsense execution 5						
0 / 0 B	IPv4 TCP/UDP	LAN_CLIENT address	*	DEV_LAN address	123 - 465	*	none	3.8 Project: Pfsense execution 5						
0 / 0 B	IPv4 TCP/UDP	LAN_SERVER address	*	DEV_LAN address	22 - 389	*	none	3.8 Project: Pfsense execution 4						
0 / 0 B	IPv4 TCP/UDP	LAN_CLIENT address	*	DEV_LAN address	123 - 445	*	none	3.8 Project: Pfsense execution 3						
0 / 0 B	IPv4 ICMP	DEV_LAN net 10.20.0.0/24	*	DEV_LAN address	*	*	none							
0 / 120 KB	IPv4 *	*	*	*	*	*	none	Activate WiFi						
- DEV\_LAN Zone:**

State	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions				
0 / 0 B	IPv4 TCP	*	*	DEV_LAN net (SSH)	*	*	none	3.8 Project: Pfsense execution 5						
0 / 0 B	IPv4 TCP/UDP	LAN_CLIENT address	*	DEV_LAN address	123 - 465	*	none	3.8 Project: Pfsense execution 5						
0 / 0 B	IPv4 TCP/UDP	LAN_SERVER address	*	DEV_LAN address	22 - 389	*	none	3.8 Project: Pfsense execution 4						
0 / 0 B	IPv4 TCP/UDP	DEV_LAN address	*	LAN_CLIENT address	21 - 389	*	none	3.8 Project: Pfsense execution 3						
0 / 0 B	IPv4 ICMP	DEV_LAN net 10.20.0.0/24	*	DEV_LAN address	*	*	none							
0 / 120 KB	IPv4 *	*	*	*	*	*	none	Activate WiFi						

The screenshot shows the Pfsense User Manager interface. It displays two main sections: 'Inherited from' and 'User Certificates'. Under 'Inherited from', 'johan0257-ro' is listed with 'User - Config Deny Config Write' and 'johan0257-rw' with 'WebCtg - Dashboard (all)'. A note states: 'If present, ignores requests from this user to write config' and 'Allow access to all pages required for the dashboard.' Under 'User Certificates', there is a table with one row for 'CA' under 'Name'. Under 'Keys', there are two sections: 'Authorized SSH Keys' and 'Authorized SSH Keys'. Both sections show a large hex string of RSA keys. Below each section is a text input field labeled 'Enter authorized SSH keys for this user'.

## Follow-up

Update documentation for stakeholders

## Progress Summary

Update project remediation plan with a summary of results and related audit findings that were remediated here:

### The following Security Assessment Findings were remediated:

1. Configure Certification Authority Role on Windows Server
2. Configure RSA keys for Administrator and copy to Linux for public key logon
3. Add Windows CA certificate as a trusted Root CA
4. Configure users with RSA keys for access to Pfsense firewall over SSH
5. Configure sshd\_config to allow public key authentication
6. Enable SSH access to firewall and change default port to 2022
7. Add SSH Keys for accounts {studentID}-ro and studentID)-rw for public key authentication
8. Update firewall rules to allow Linux and port 2022

**System codes: LR – Linux Risk, WR – Windows Risk, FR – Firewall Risk**

**Submit to Canvas**

## Testing Procedures

Notify Validation Group environment is ready for testing.

## Back out plan: revise each week as necessary. NOTE: List steps, do not execute.

**Windows Server:**

9. Revert settings to original values
10. Run a **gpupdate /force**

**Linux System:**

7. **Disable firewall**
  - a. sudo ufw disable

**Pfsense Firewall:**

3. **Revert configuration to previous version**

a. Diagnostics --> Config History --> select restore point and click 

**Project notes**

Make sure you specify the systems that you are working on configuring as part of the change management process.

Server Info:

**(Virtual) Server Name:** CIS230-UBUNTU

**OS:** Ubuntu 9.4.0-1ubuntu1~20.04.2

**IP Address:** 172.16.30.30

**Server Specs:**

VM

CPU: Intel® Xeon® CPU E5-2640 v4 @ 240GHz

RAM: 1.9 GiB

STORAGE: 42.9 GB

NETWORK:

2 vCPU, 2GB RAM

**(Virtual) Server Name:** CIS230-WIN2019

**OS:** Windows Server 2019 Standard, 10.0.17763 Build 177763

**IP Address:** 172.16.10.10

**Server Specs:**

VM

CPU: Intel® Xeon® CPU E5-2640 v4 @ 2.40GHz, 2397 Mhz, 2 Core(s), 2 Logical Processor(s)

RAM: 4.00 GB

STORAGE: 60 GB

NETWORK: Intel® 82574L Gigabit Network Connection

2 vCPU, 2GB RAM

**(Virtual) Server Name:** CIS230-WIN10

**OS:** Windows 10 Education, 10.0.10240 Build 10240

**IP Address:** 172.16.20.20

**Server Specs:**

VM

**CPU:** Intel® Xeon® CPU E5-2640 v4 @ 2.40GHz, 2397 Mhz, 1 Core(s), 1 Logical Processor(s)

**RAM:** 2.00 GB

**STORAGE:** 40.00 GB

**NETWORK:** Intel® 82574L Gigabit Network Connection

2 vCPU, 2GB RAM