Security Testing Report

Testing security controls on the infrastructure

Prepared For:

Marc Hayes

Seneca Polytechnic

Prepared By:

Ornan Roberts

Syed Mujahid Hamid Ali

Ramachandra Muralidhara

Yannish Kumar Ballachandher Sreedevi

December 11, 2023

Table of Contents

Executive Summary

The objective of the report is to showcase the testing of security controls that were applied to the Agricore infrastructure. The security controls are of paramount importance in safeguarding digital assets and sensitive information within the domain. The vulnerabilities and weaknesses in the system need to be proactively addressed and to defend against these weaknesses the controls are the approach to adopt. By conducting security control testing, organizations can stay ahead of evolving cyber threats, while maintaining the integrity of networks, and confidence with clients. The security controls as discussed in the plan, we implemented based on the CIS framework. The aim of the report is to show the addition and testing process of controls onto the infrastructure of Agricore.

Security Controls

Security controls are critical components which can be from a wide range of technical, administrative, and physical measures. As a reference, the CIS controls were used to ensure the best industry recommended measures are considered. These controls are implemented to protect the confidentiality, integrity, and availability of sensitive information and business operations. These controls play a pivotal role in creating a resilient cybersecurity posture. The table below shows the controls applied to the Agricore infrastructure.

Control	Description
Access Management Control	Limit the access to sensitive data and files to only those individuals who require it based on their roles and responsibilities.
Log Management Control	Collecting all the logs for activity and anomalies. The control focuses on the importance of collecting and analyzing log data to monitor for suspicious activities.
Web Browser Protection	The control delves into the protection of the web server and web based resources. SSL Encryption was added to secure the website. A web application firewall

	(WAF) in the network infrastructure to protect against web attacks.
Malware Defense Control	This control protects the endpoint from executing any malicious file. The control is disabling the feature of autorun and autoplay for removable devices.
Network Segmentation Control	Implement VLANs and network segmentation. This control is focused on establishing and maintaining network boundaries.
Data Recovery Control	This control is for deploying a backup plan incase of disaster. It ensures that backups are conducted at scheduled intervals.
Software Assets Inventory Control	This control would allow management and tracking of software assets within the organization. Inventories created for all assets for administrative uses.

Testing Controls

The following section showcases the successful implementation and testing of the controls designed for Agricore.

Access Management Control

The primary goal is to ensure that only authorized individuals or systems are granted access to resources, data, and functionalities. The creation of security groups is a viable method for applying access management. Security groups were created for manager and normal users where RBAC methodology was applied. Specific permissions for each role were assigned based on the OUs. Through the creation of group policy objects we were able to perform identity and access management (IAM) capabilities. For users in Sales & Marketing, the access to network settings/control panel was restricted through GPO which can be maintained by IT admins only. Similarly, some RBAC based rules were created where two security groups for IT admins and IT

managers were created with varying privileges. This access control would prohibit any sort of unauthorized action based on the role. The IT admins group was assigned permissions to only reset the password for users, whereas IT managers would have more privileges.

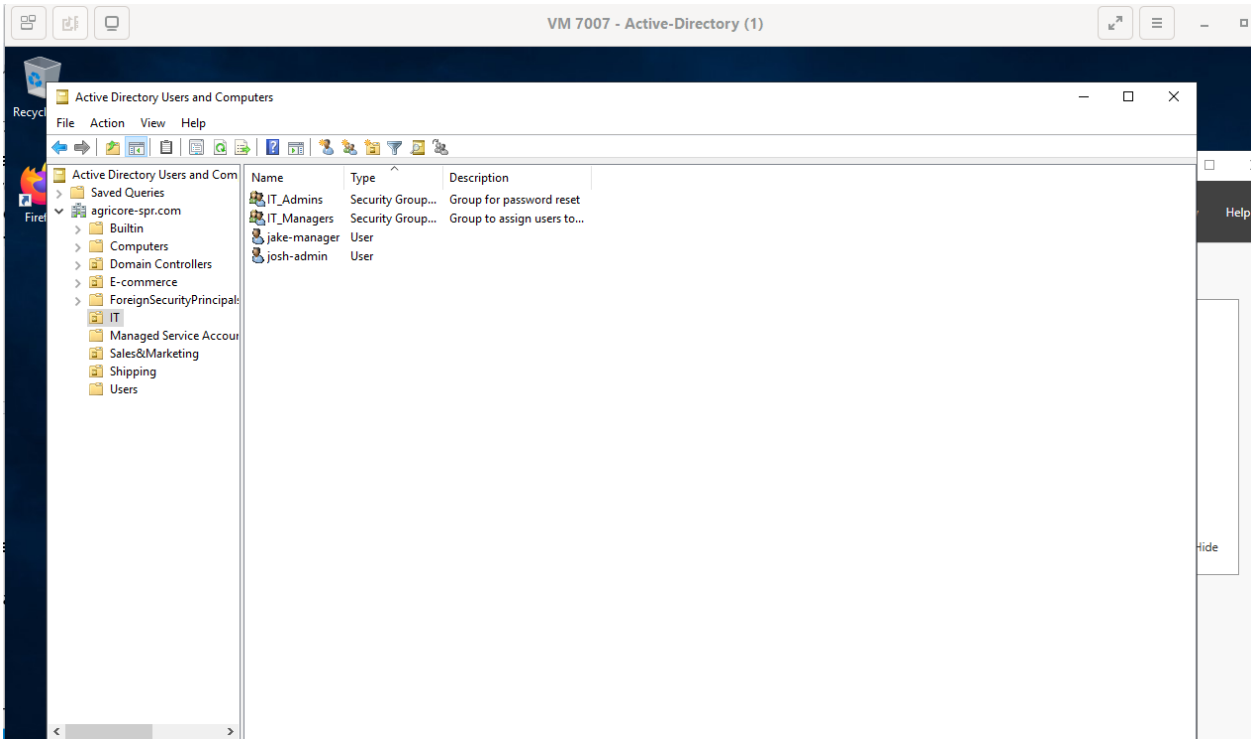


Fig.1 Users and security groups created for IT OU

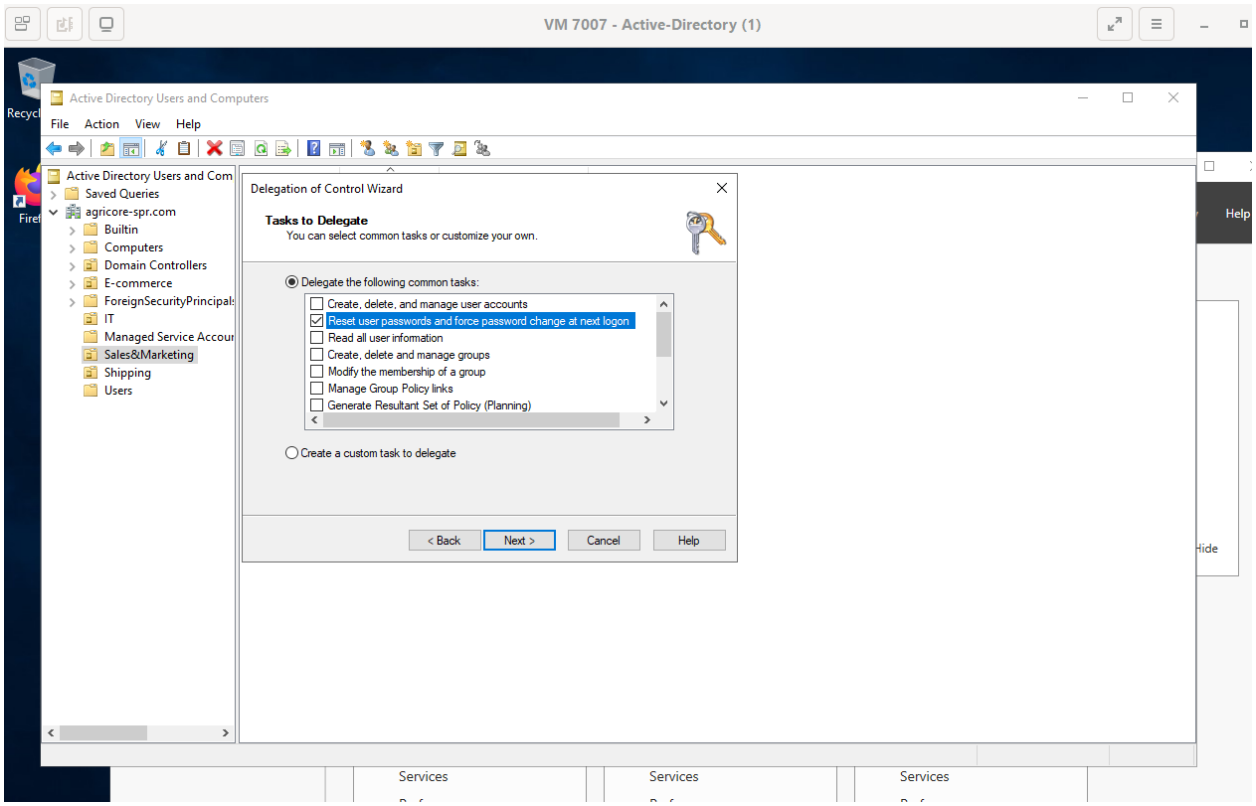


Fig.2 Setting up role based policies for IT admins

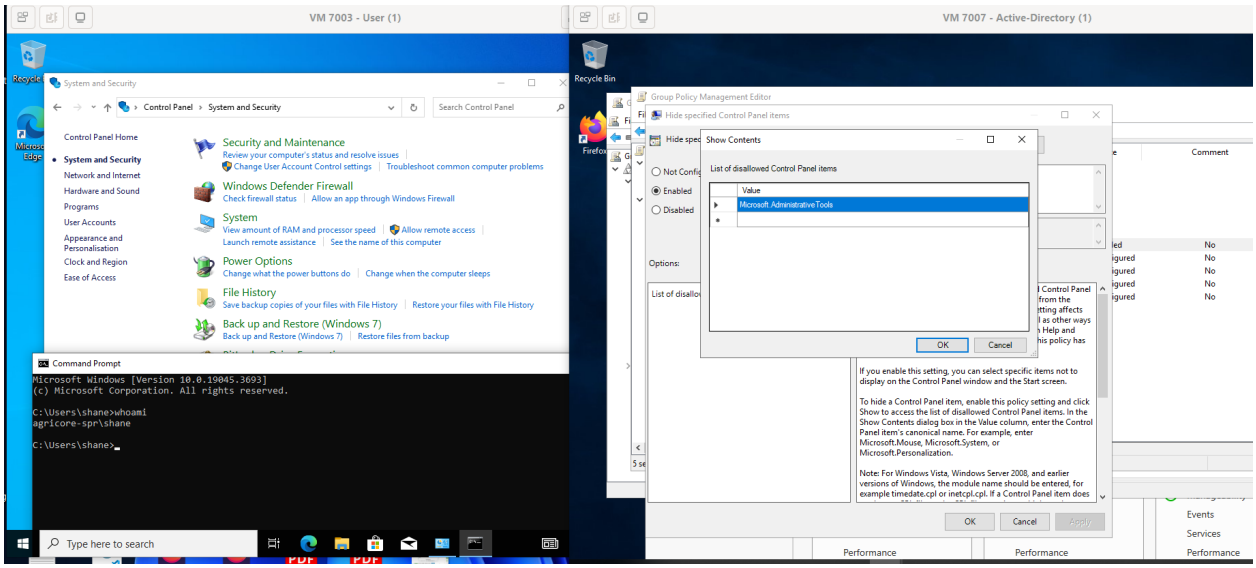


Fig.3 Blocked access for administrative tools for users

Log Management Control

Logs are records generated by software, applications, operating systems, and devices that capture events, activities, and errors. To monitor such traffic, a traffic monitoring system Snort IDS was installed which captured traffic inbound and outbound. Based on common attacks and malicious traffic we researched on the detecting rules and added them into the configuration file. After performing the configurations, we tested the control by generating some traffic.

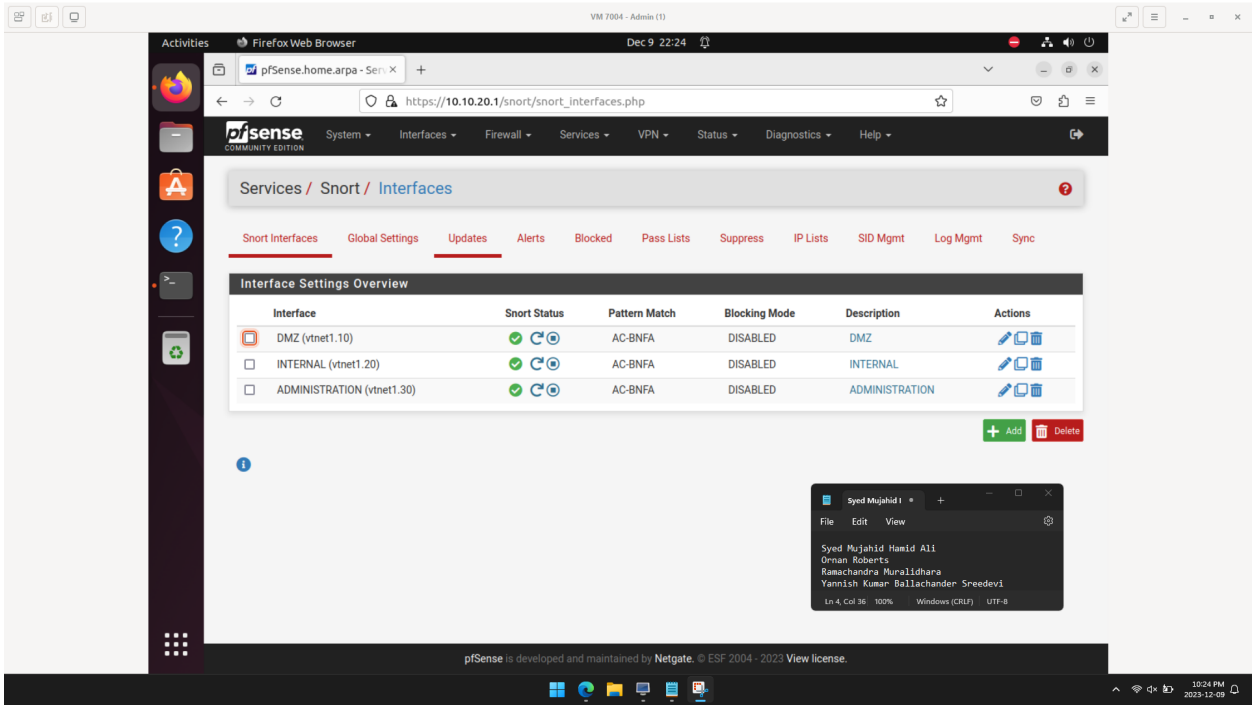


Fig.4 Interfaces added and ran with Snort.

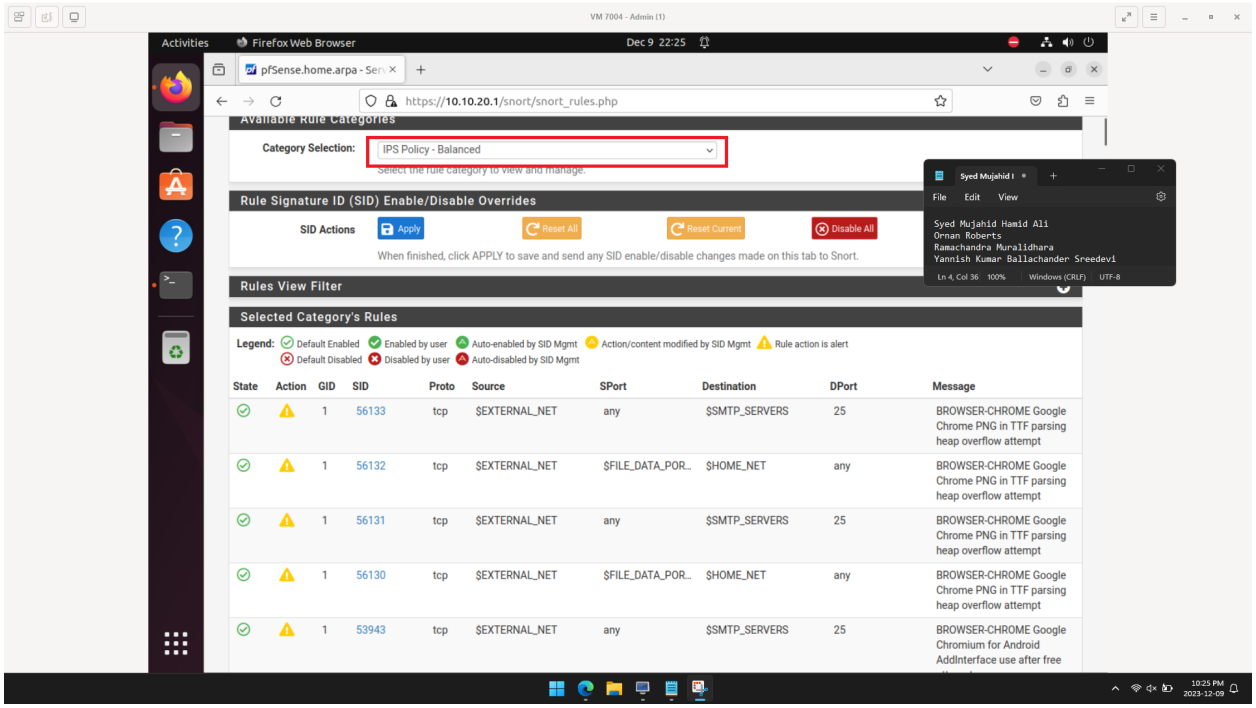


Fig.5 Snort Subscriber rules added and set to Balanced mode for the interfaces.

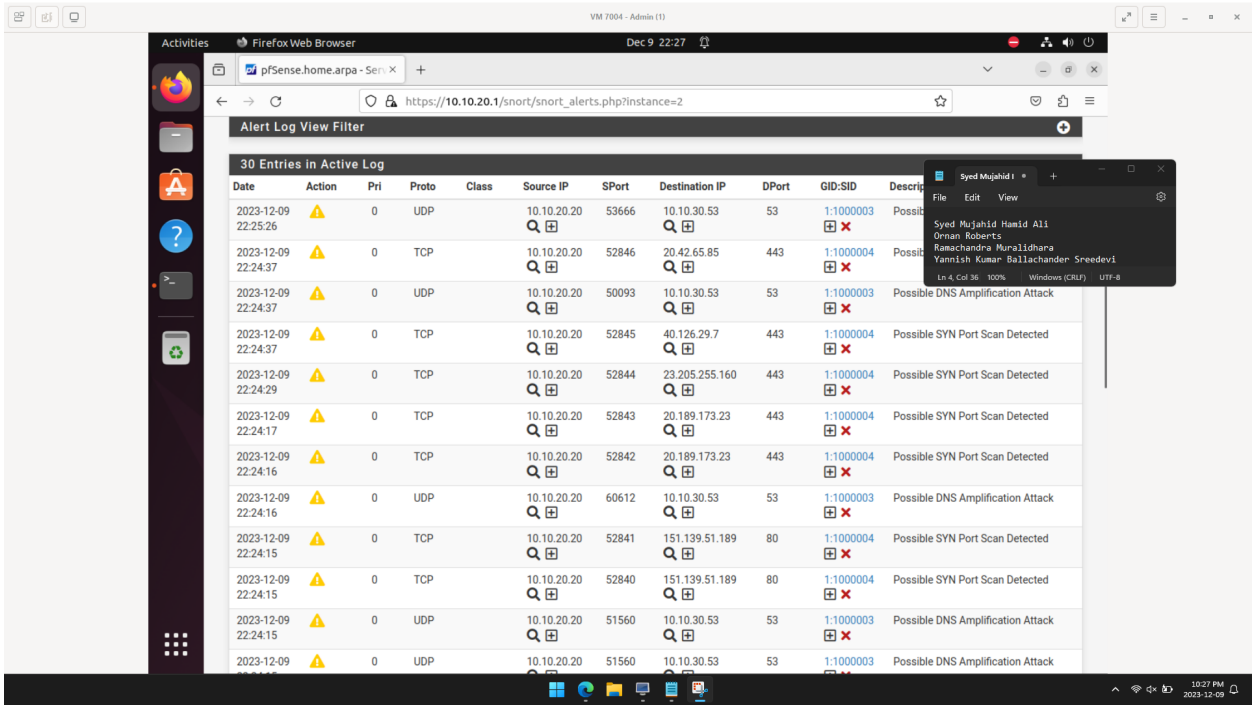


Fig.6 Logs being displayed for any activity in the network.

To test the policies and rules set in Snort, we will perform a port scanning attack, and do a benign ping request scan.

For the port scanning, we will implement Nmap to scan for any open port in the Admin machine.

As we can see, the attempt was blocked and the log showed up in Snort.

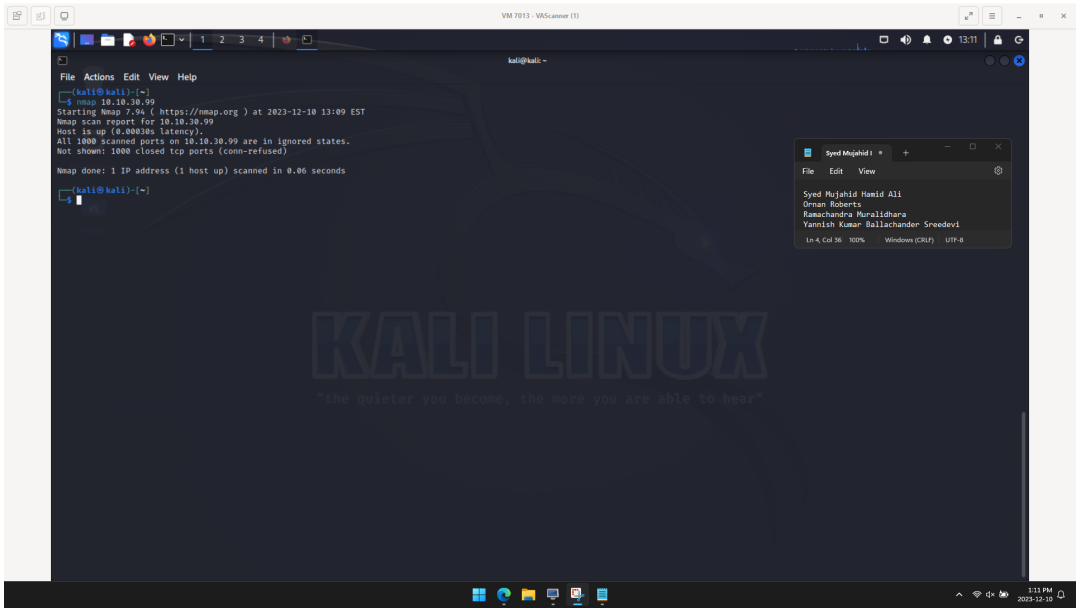


Fig.7 Attempt made to scan ports on the Admin machine.

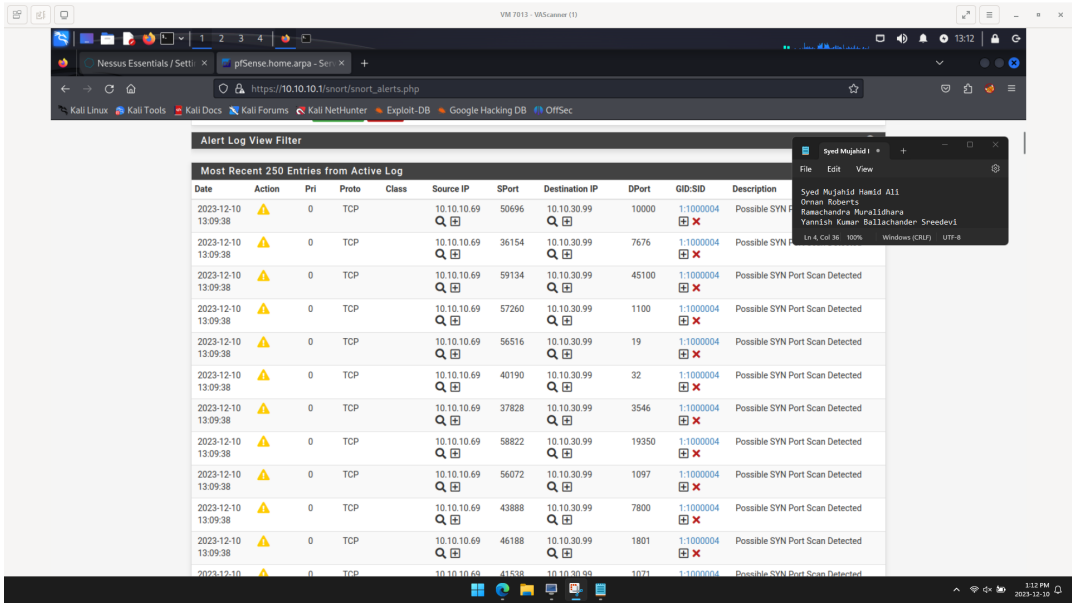


Fig.8 Logs being displayed for Port Scanning attempt.

Next, we will run a benign ping scan where we attempt to connect with a device in the Internal network. We can see that we are able to connect and logs show up for that interface as well.

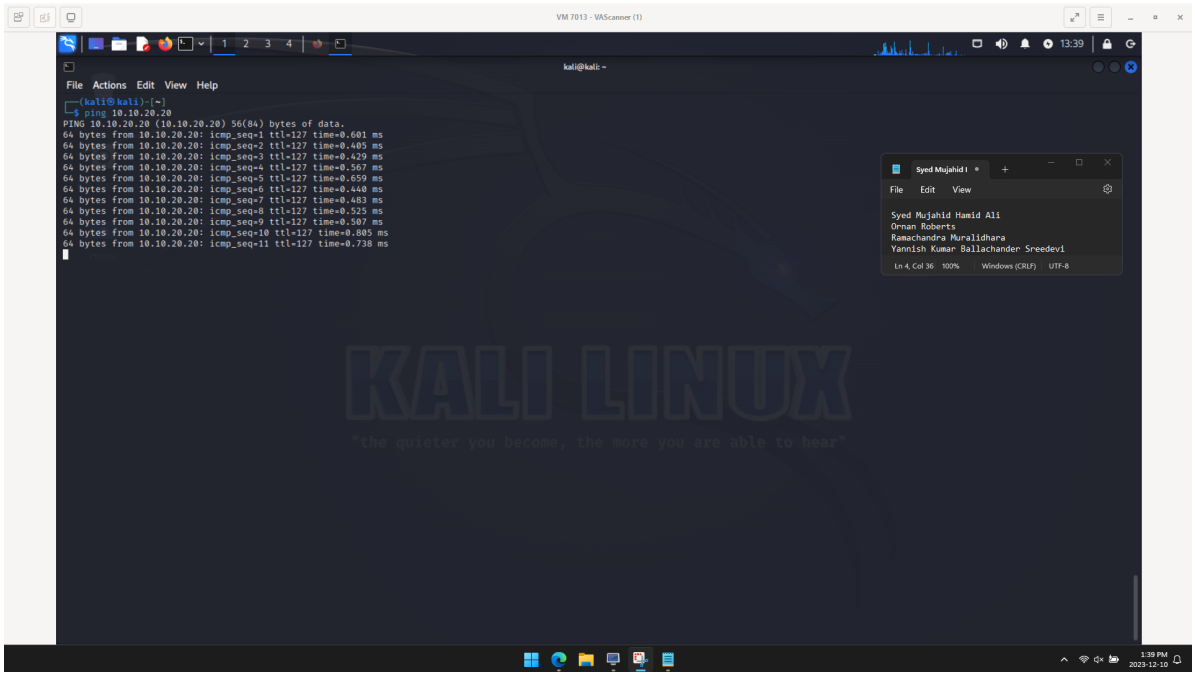


Fig.9 Ping request made to the Internal network.

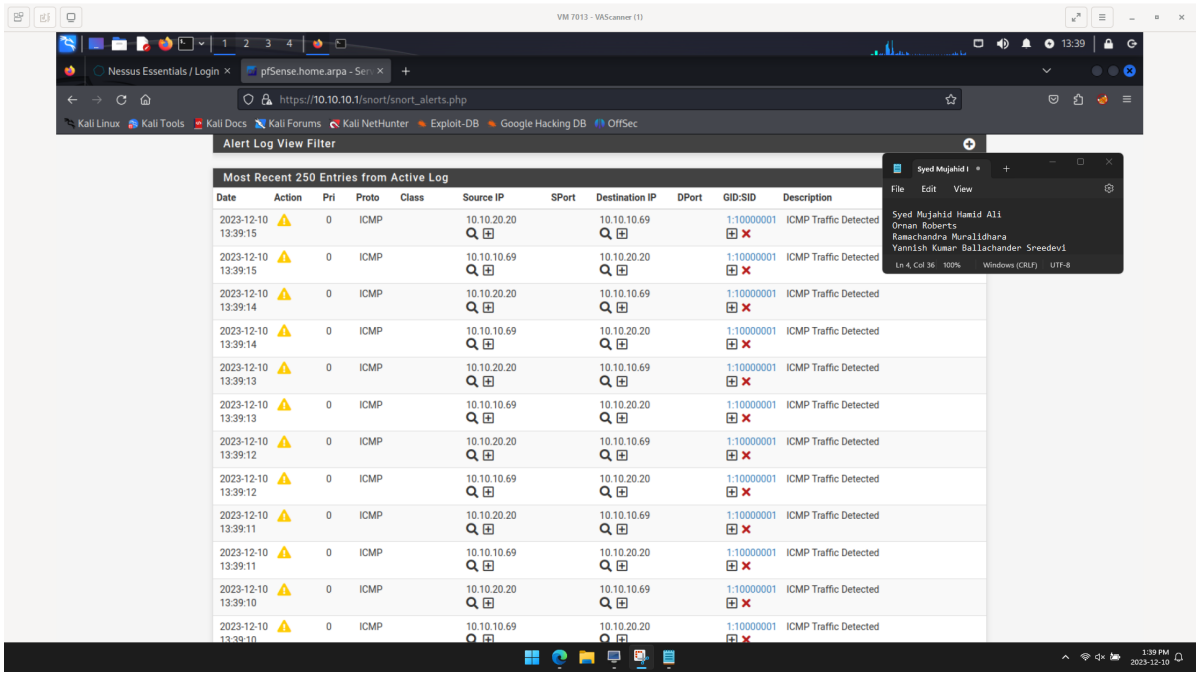


Fig.10 Logs being displayed for ICMP Ping requests.

Web Browser Control

The security of web browsers is crucial for organizations to reduce the risk of malicious activities and protect against web attacks. It is important to keep web browsers up-to-date with the latest security patches and updates. To implement this control we added SSL which provides a mechanism for verifying the identity of the parties involved in a communication. The self-signed certificate was created for the Agricore website and added for all web servers. The SSL certificate was added to all web servers for private and public.

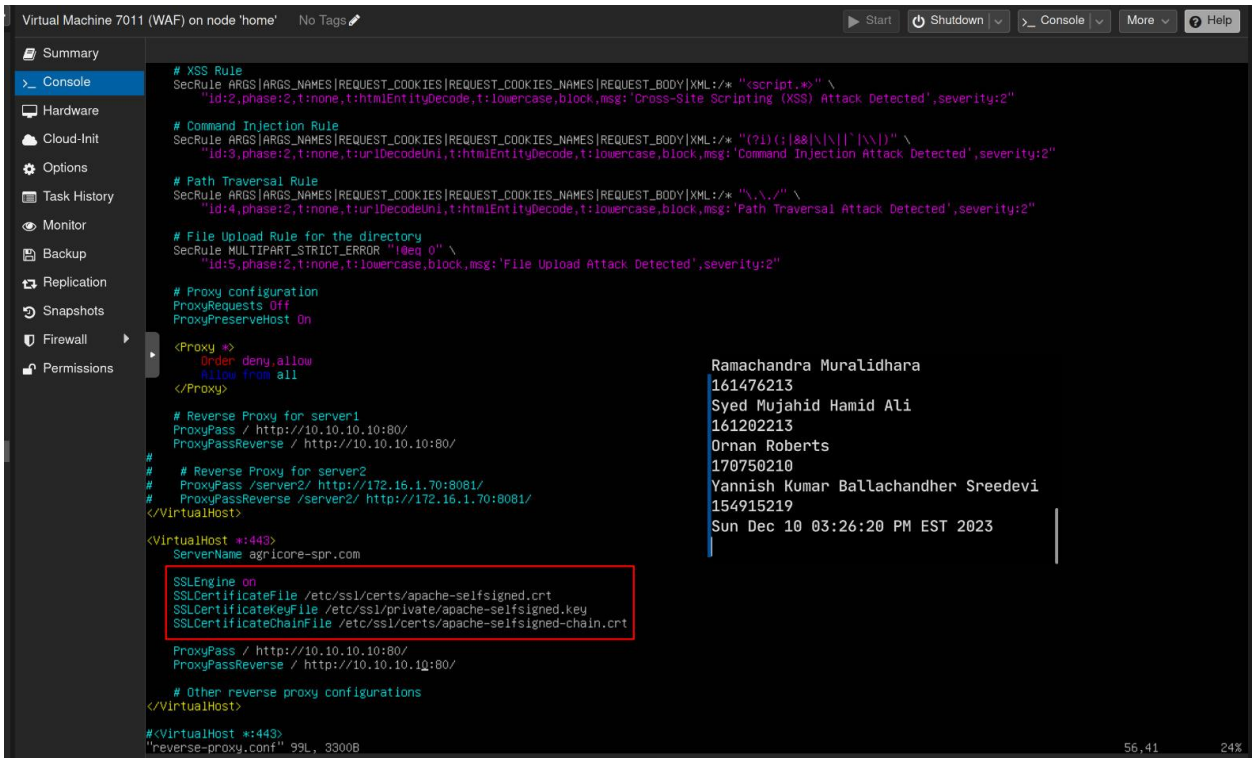


Fig.11 SSL configuration for Agricore website

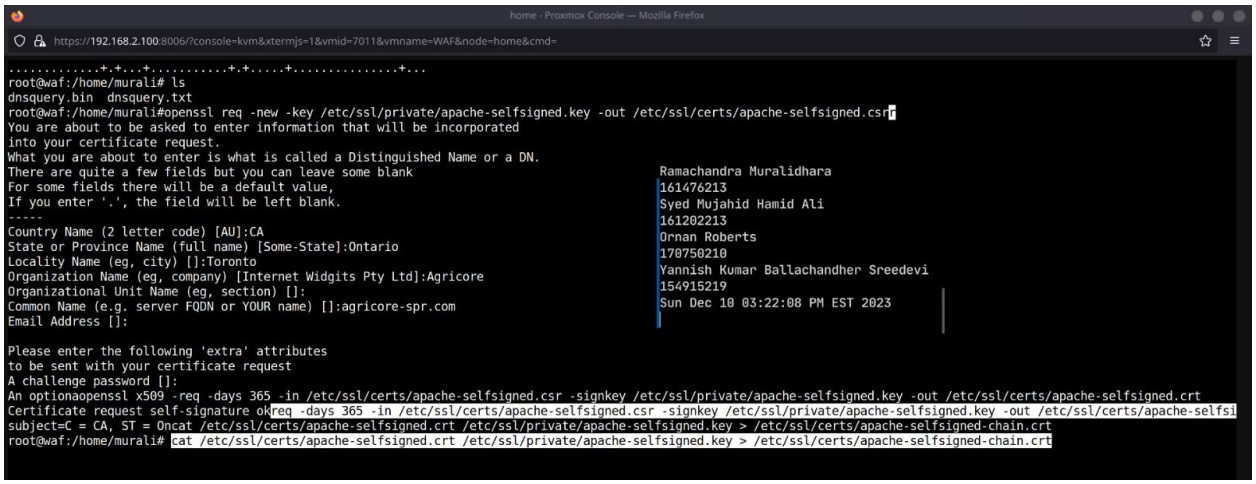


Fig.12 Generating self signed certificate

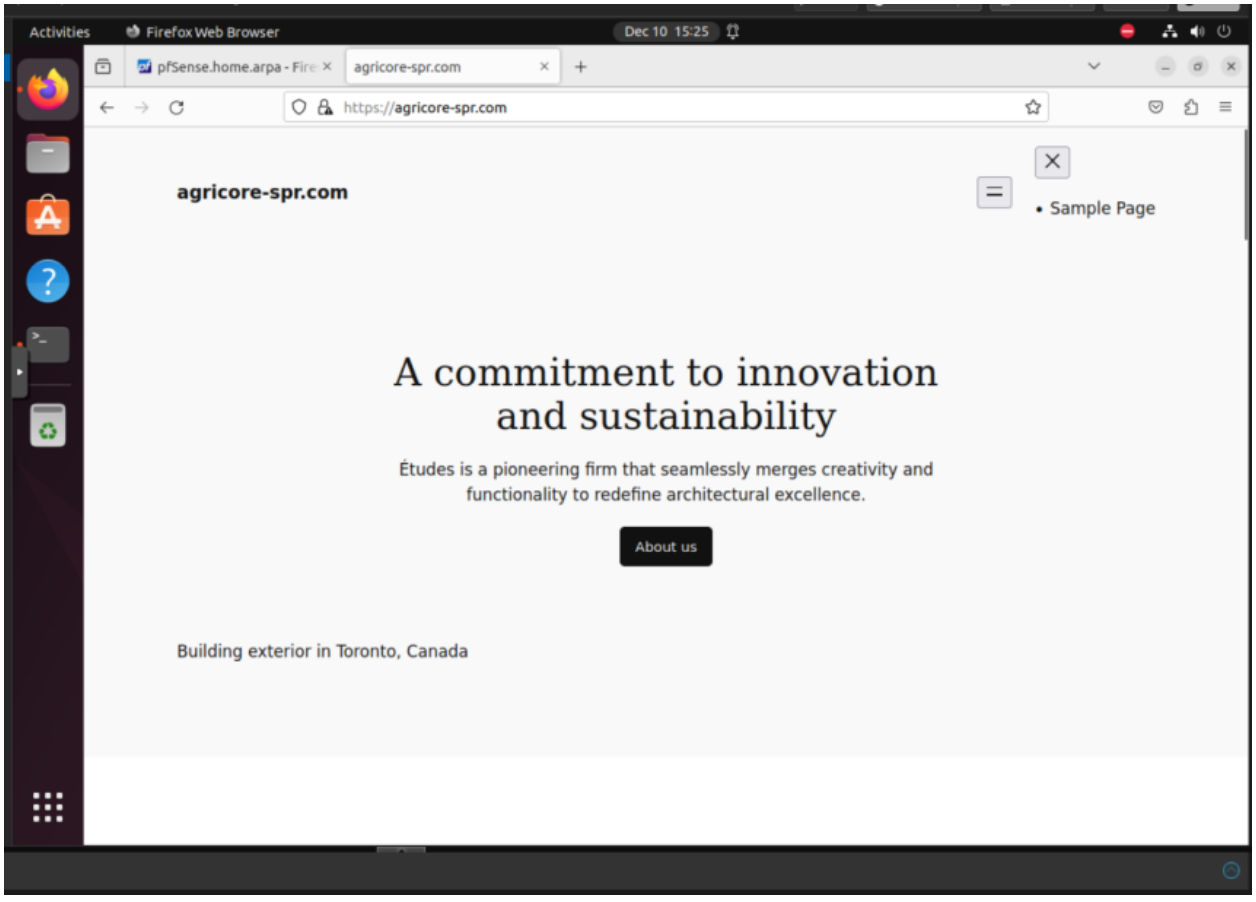


Fig.13 SSL certificate added and site with https

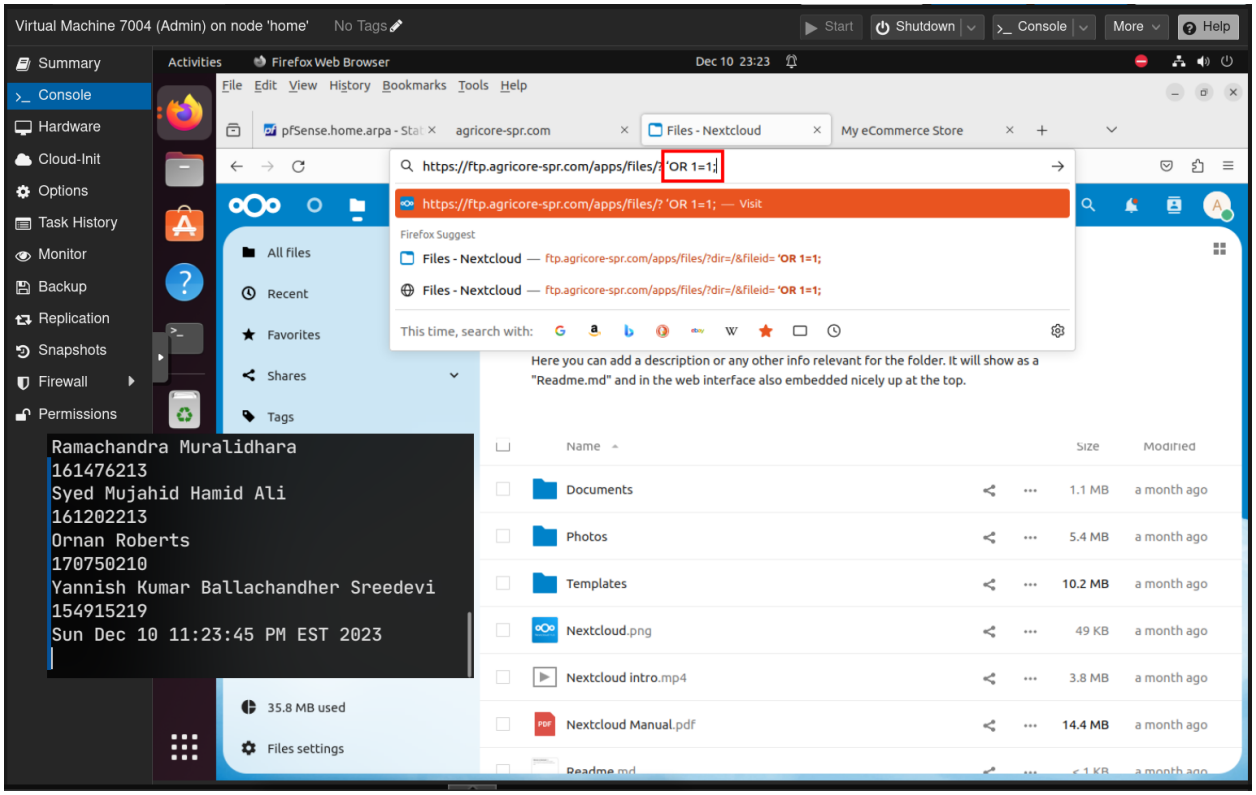
WAF Controls Test

SQL Injection

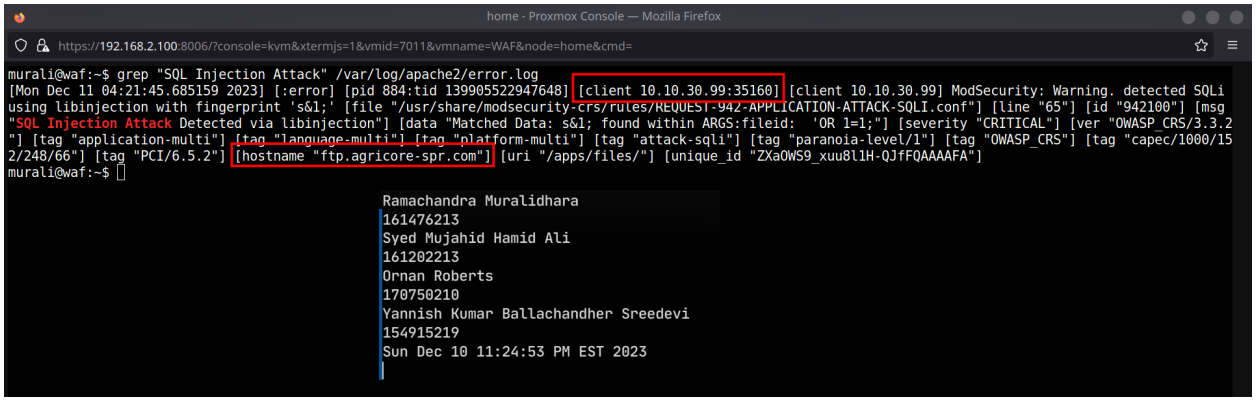
This rule checks for any SQL Injection inputs and blocks them. It shows a 403 page if someone tries to

use SQL Injection.

Payload used: ***'OR 1=1;***



Logs -

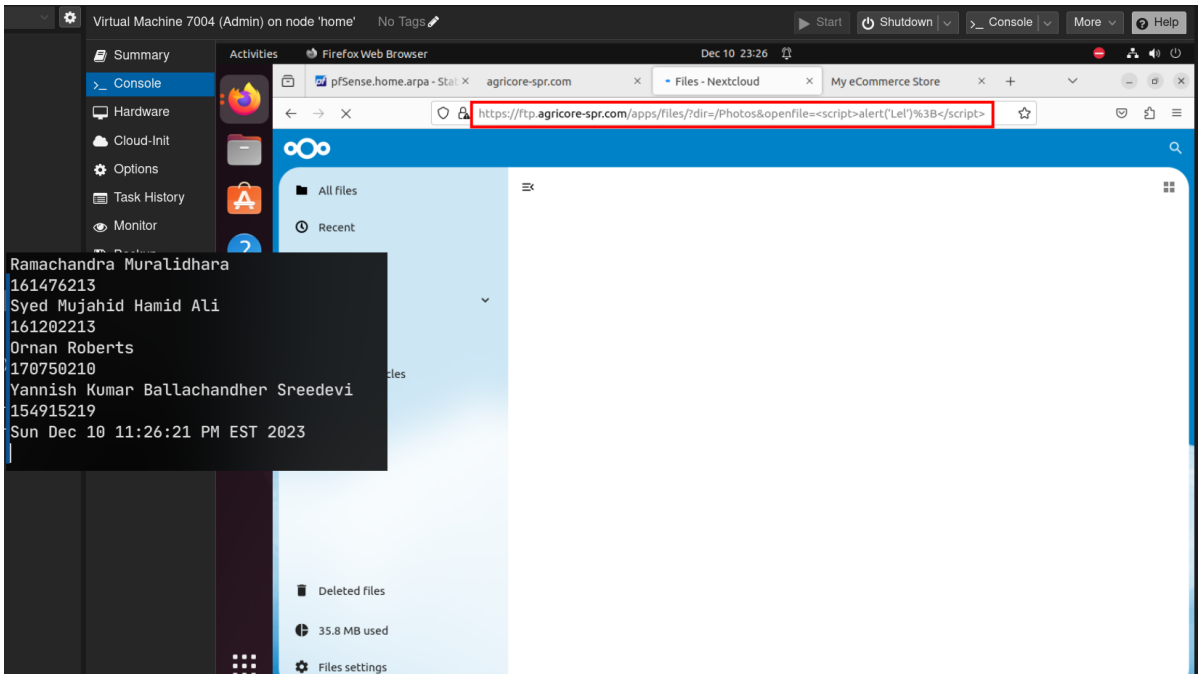


XSS

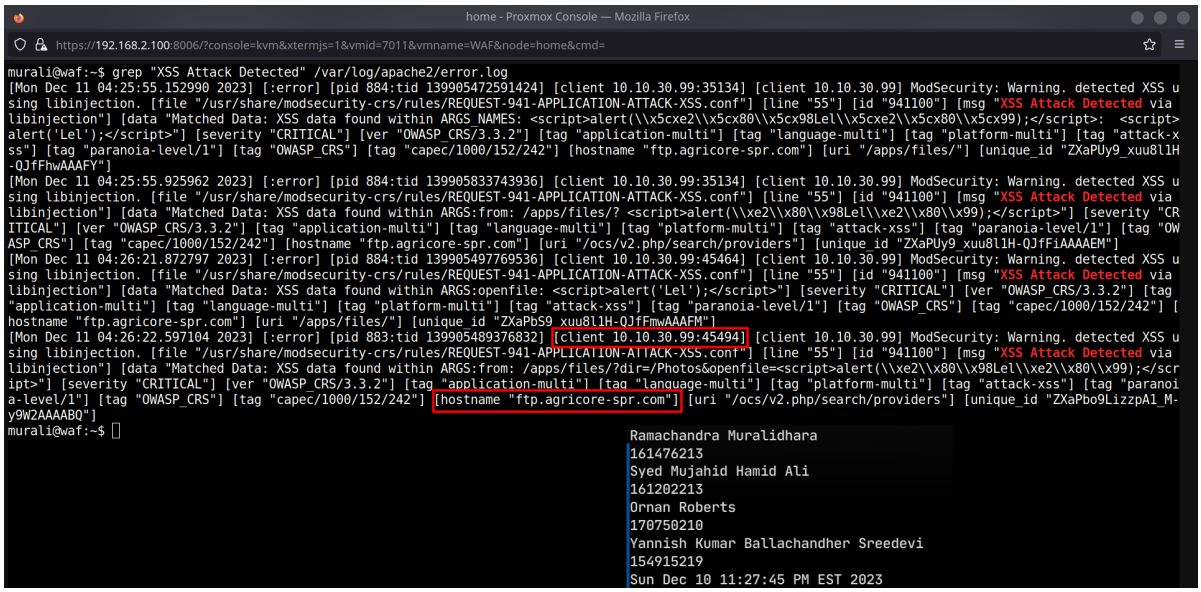
This rule checks for any XSS Injection inputs and blocks them. It shows a 403 page if someone tries to

use XSS Injection.

Payload used - ***<script>alert('Lel');</script>***



Logs -

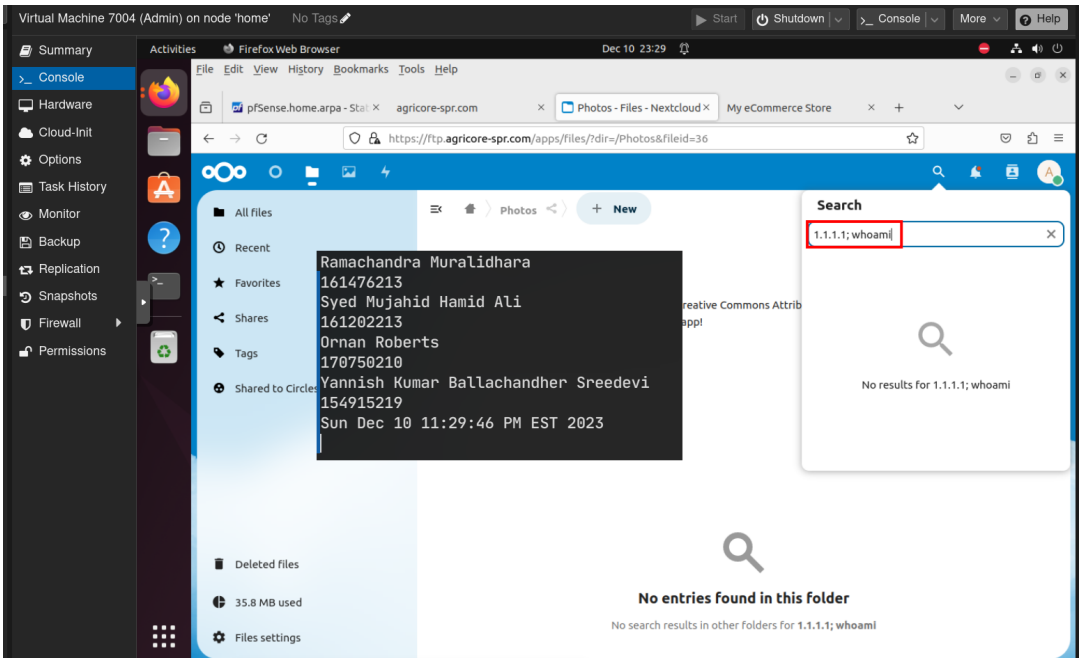


Command Injection

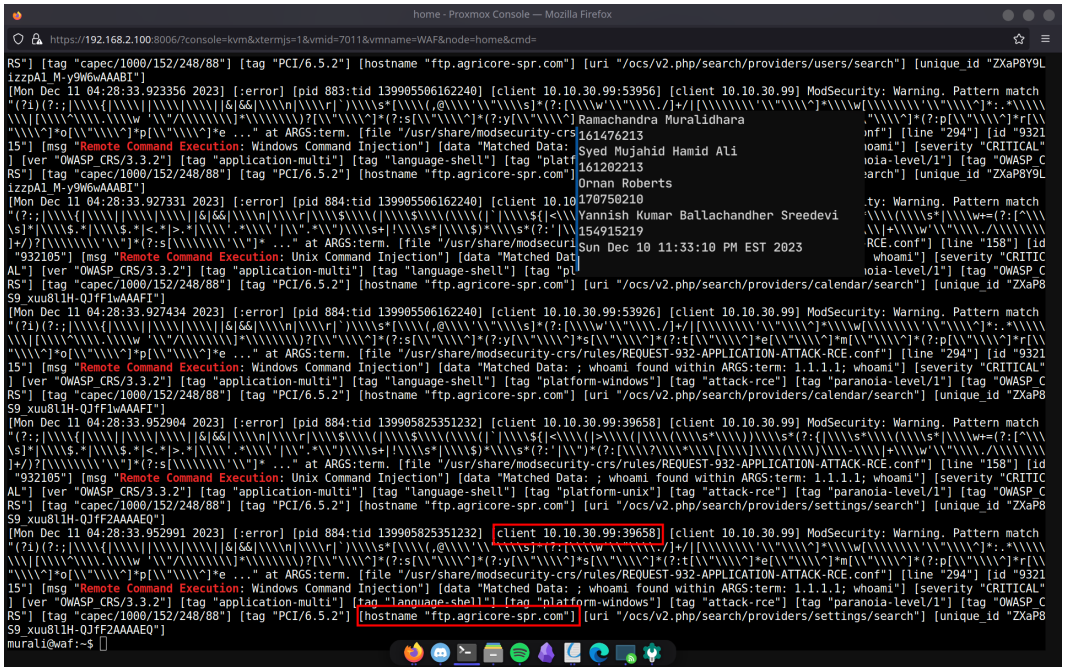
This rule checks for any Command Injection inputs and blocks them. It shows a 403 page if someone tries

to use Command Injection.

Payload Used: ***1.1.1.1; whoami***



Logs

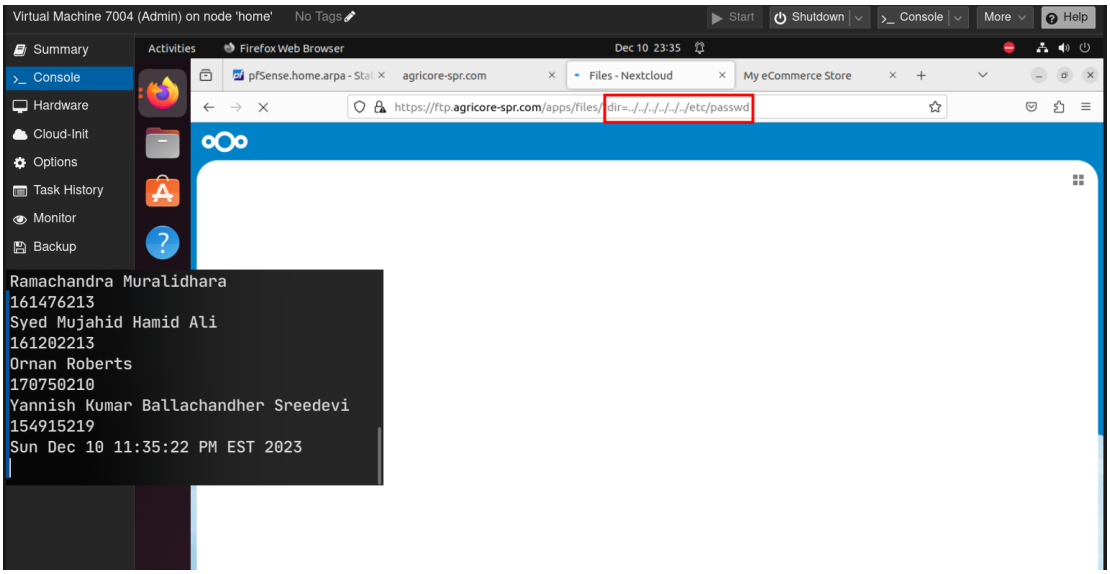


Path Traversal

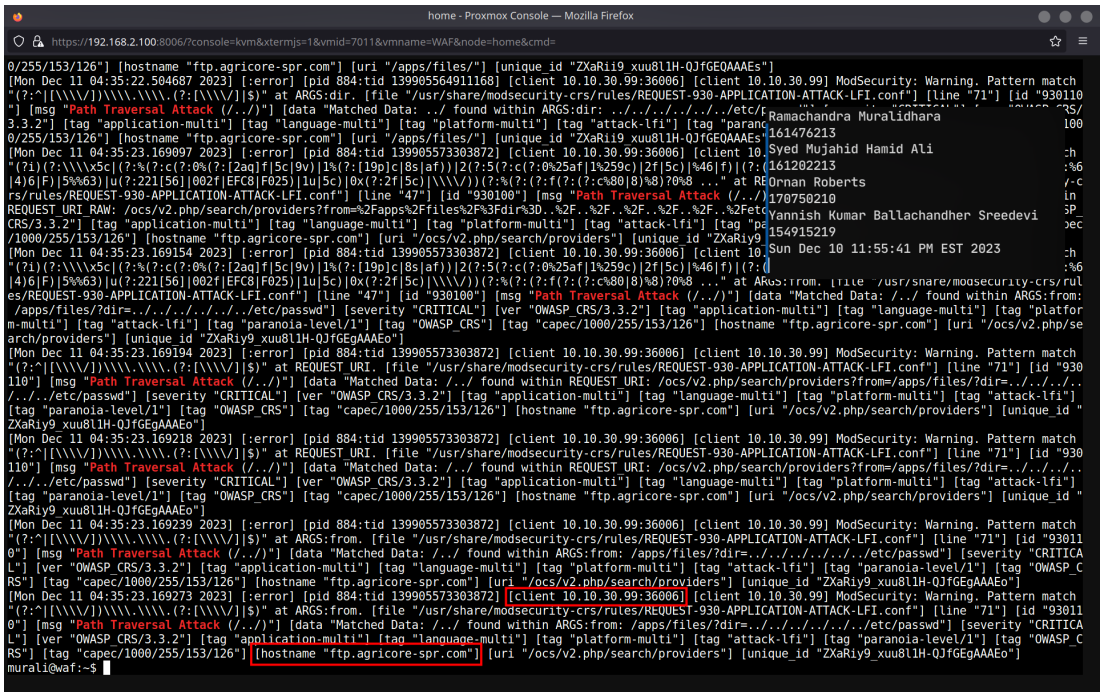
This rule checks for any Path Traversal Injection inputs and blocks them. It shows a 403 page if someone

tries to use Path Traversal Injection.

Payload Used: ***../../../../../../etc/passwd***



Logs

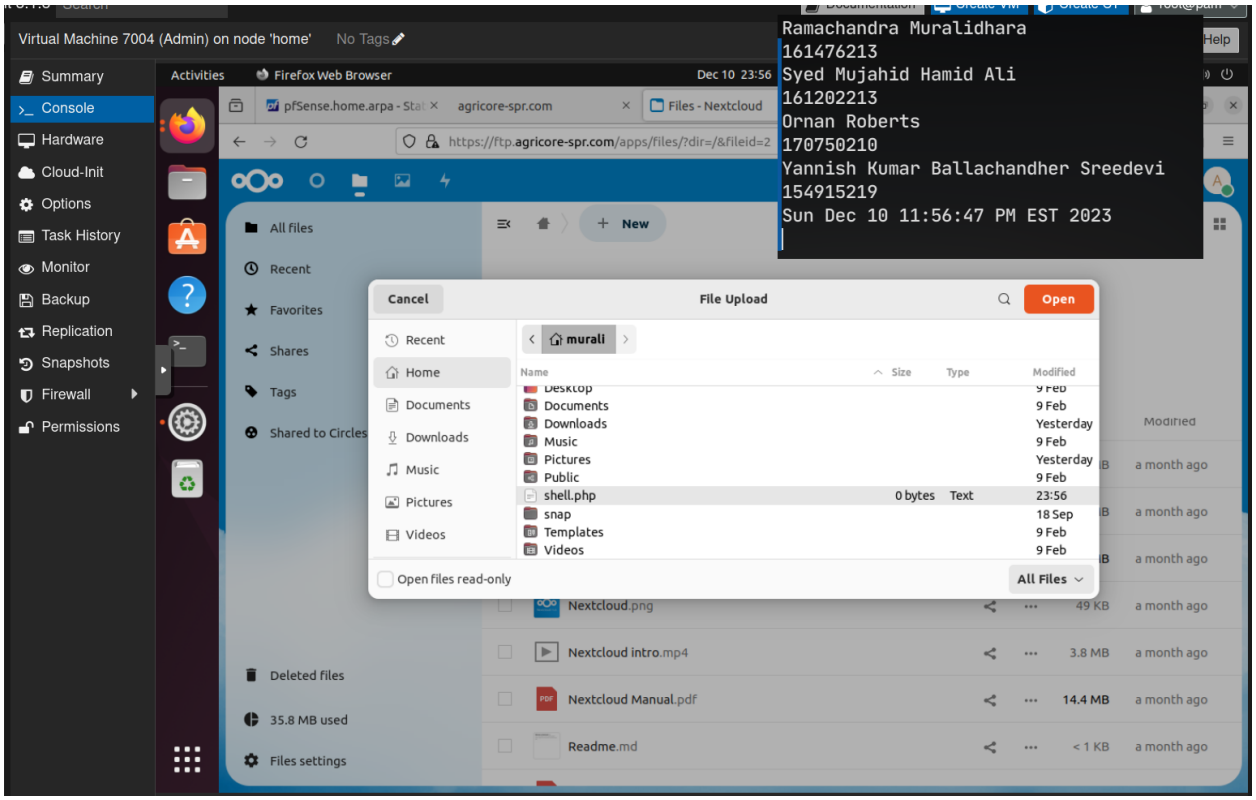


File Upload

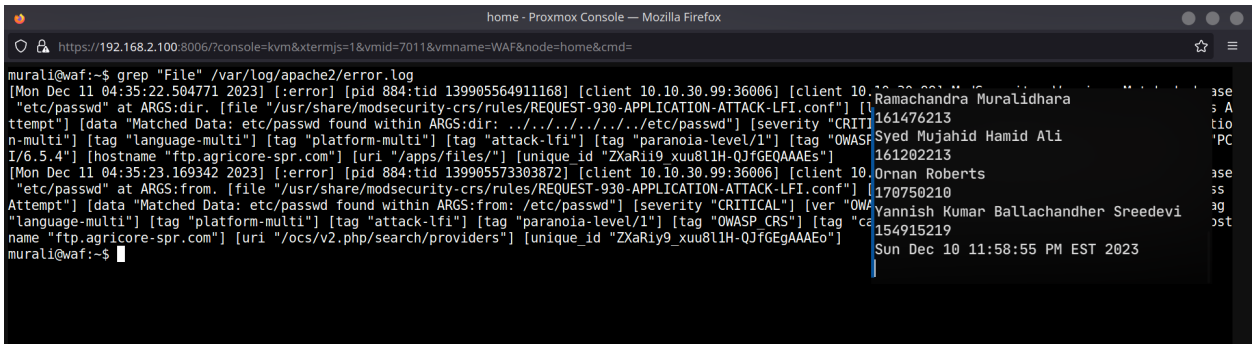
This rule checks for any File Uploads with bad extensions and blocks them. It shows a 403 page if

someone tries to upload a file with a bad extension.

Payload – Create a shell.php file and try to upload it.



Logs



Malware Defense Control

Malware defense is critical to enforce in enterprise to protect the systems from being infected with malware. To do so endpoint safety controls can be implemented where the disabling of autorun across all connected devices is a useful one and it ensures a consistent security posture. By disabling autorun, the automatic execution of malware when a USB drive is connected to a computer is thwarted, reducing the risk of infection. We implemented the control by creating a GPO and disabled function for adding removable devices which protects the devices from auto-running any malicious code. Similarly, we also added the control on infrastructure in Proxmox where attaching removable devices was prohibited.

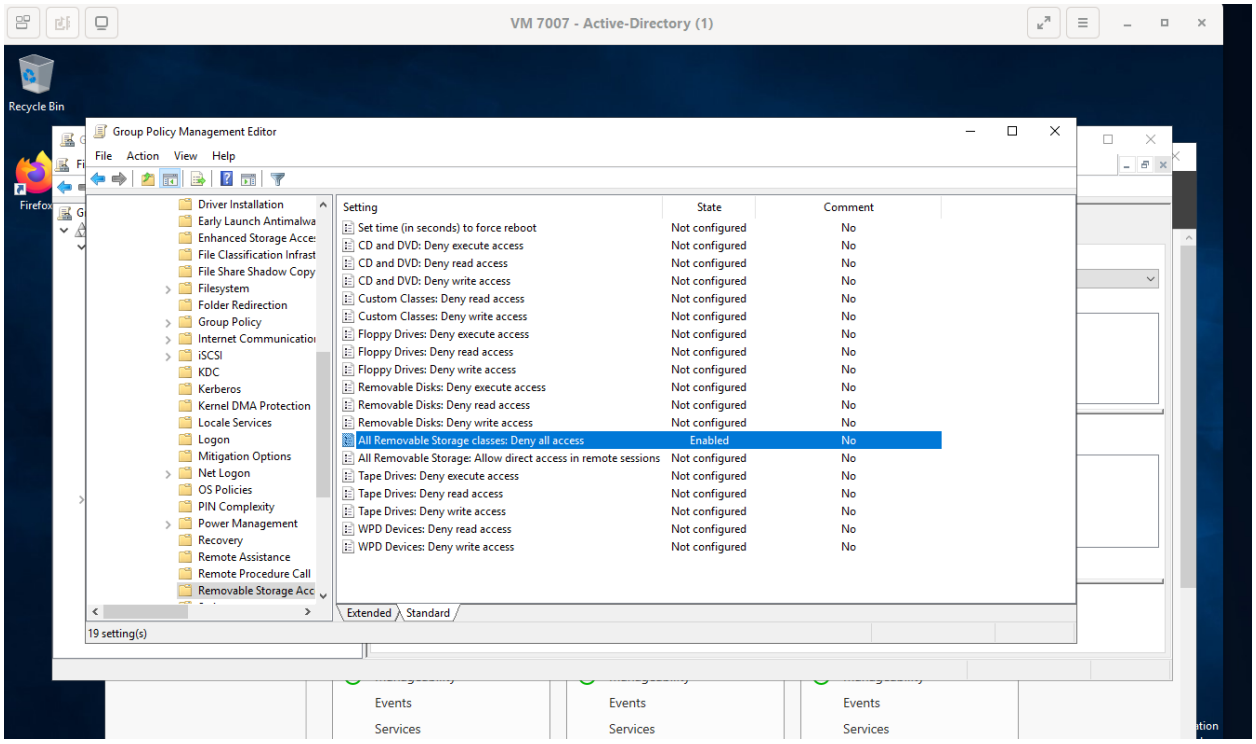


Fig.14 Blocked access for removable devices on endpoints

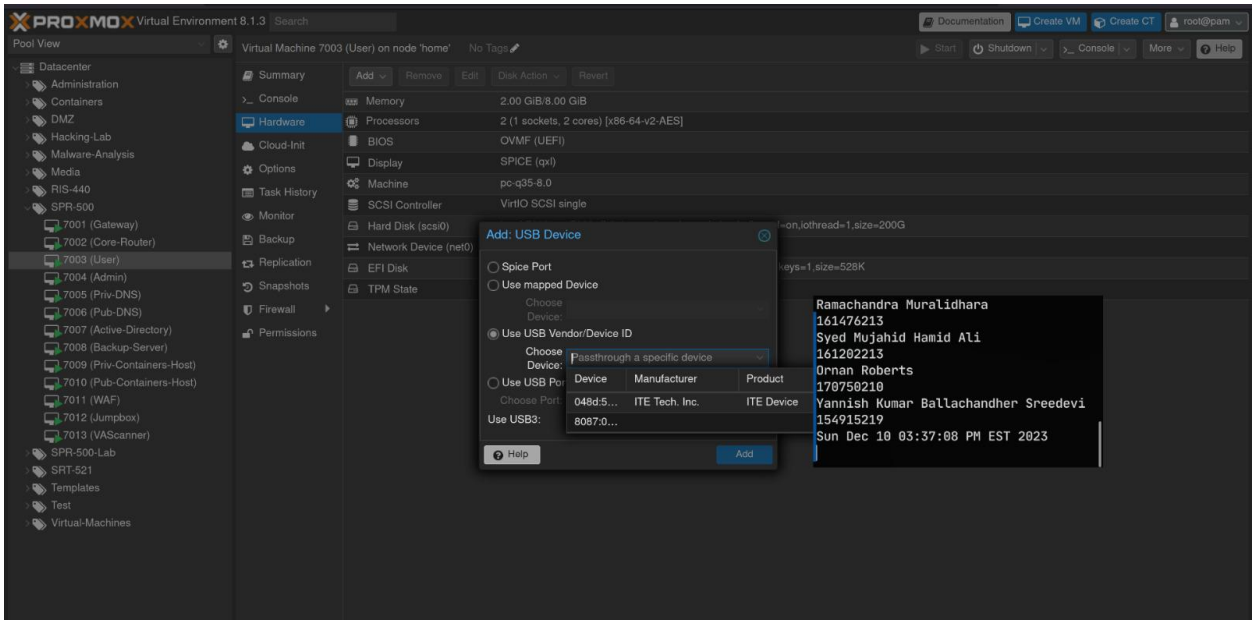


Fig.15 Enabled the blocking of USB device

Network Segmentation Control

The isolated segments or subnetworks of the infrastructure to enhance security and control is a common practice adopted by industry. The ultimate goal of network segmentation is to create barriers within the network, while limiting the potential impact of a security breach. To apply this control, VLANs were created where business resources were assigned to each VLAN based on the use cases.

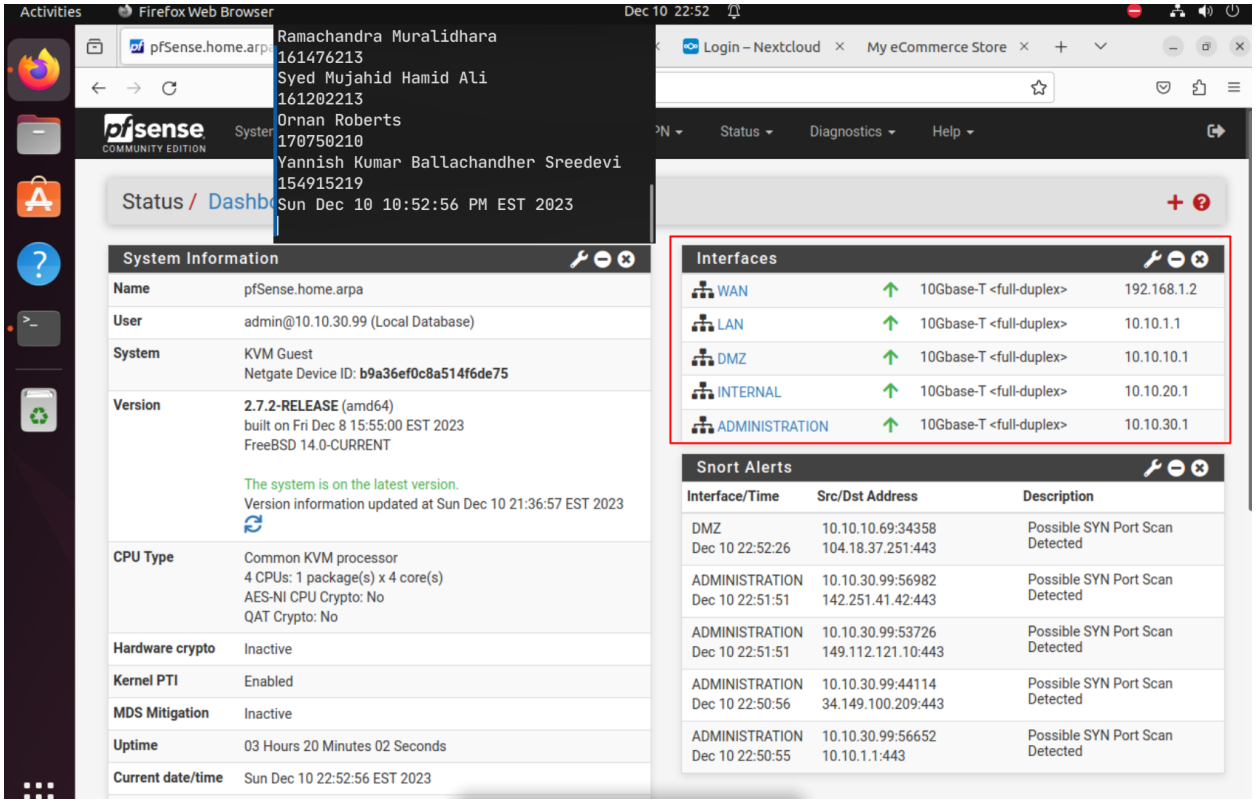


Fig.16 VLANs created for each part of the network on Core Router.

To test our VLANs, we attempted to ping from the .30 (ADMINISTRATION) network to .10 (DMZ) and .20 (INTERNAL) networks.

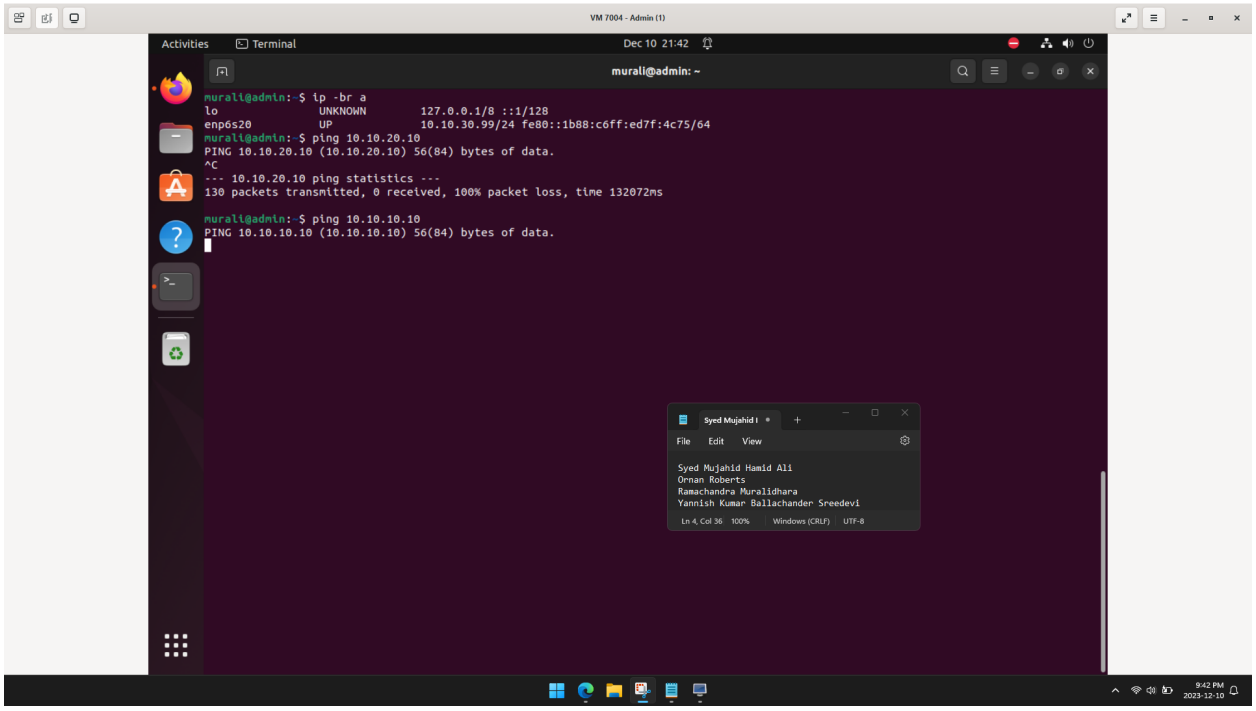


Fig.17 Ping attempts made from .30 to .10 and .20 networks.

Data Recovery Control

Establishing a comprehensive and regular backup strategy for critical data is essential to maintain business continuity in case of an incident. Data recovery controls offer redundancy and failover mechanisms for critical systems and data. A backup or recovery is crucial and so we implemented this control by adding a backup server. A bash script was created which will perform backup of the remote host and store the backup onto the local backup server. The testing of backup was performed where the script ran and created a tar file which contains the backup of the remote server. For each of the remote systems the backup file was created.

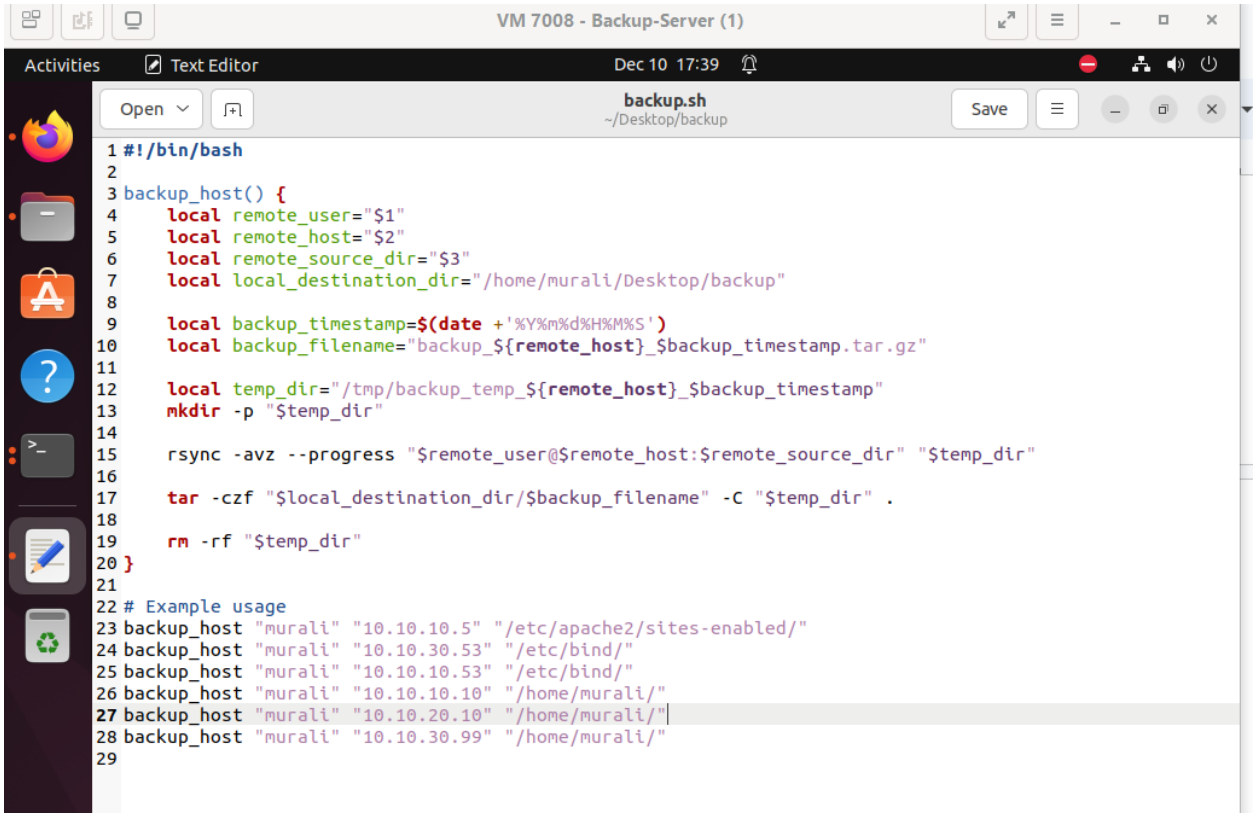


Fig.18 Data backup script

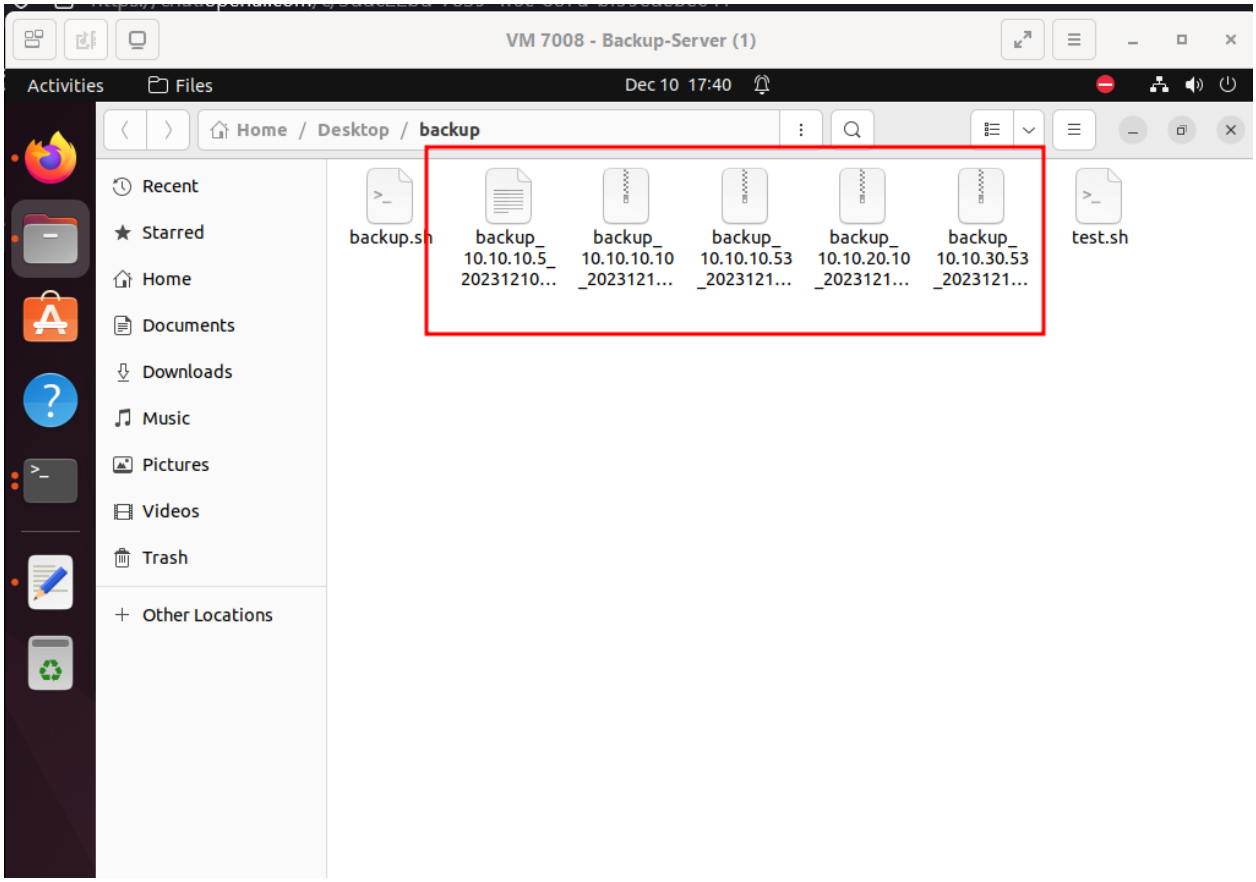


Fig.19 Backup files created for remote systems

Account Management Control

The primary objective of the Account Management control is to ensure that only authorized users have access to systems, applications, and data. Implementing robust account management practices helps organizations comply with regulatory requirements which includes password management. To implement this control, the password policy was created using GPO where the attributes of complexity and length were specified. This control will allow users to have complex passwords.

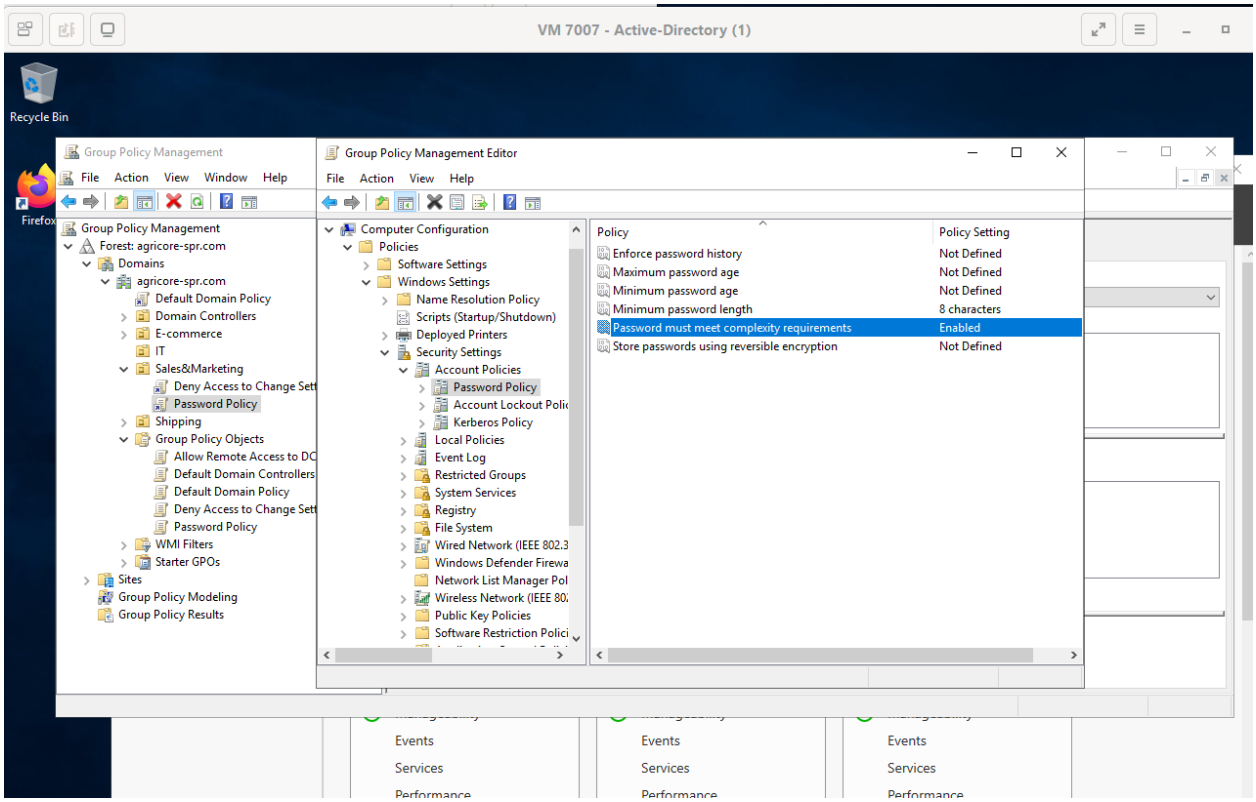


Fig.20 password policy for accounts

Asset Inventory Control

Inventory management is a critical aspect of IT asset management (ITAM) and is essential for ensuring compliance, optimizing costs, and enhancing overall IT governance. It involves tracking and managing software assets throughout their lifecycle. It's a catalog of software assets within the organization that includes installed applications on end-user devices, servers, and virtual environments. A simple method of implementing this control is to have an excel sheet. An excel sheet with all devices and software specifications was created. The Admin PC has the catalog to maintain the assets through this document.

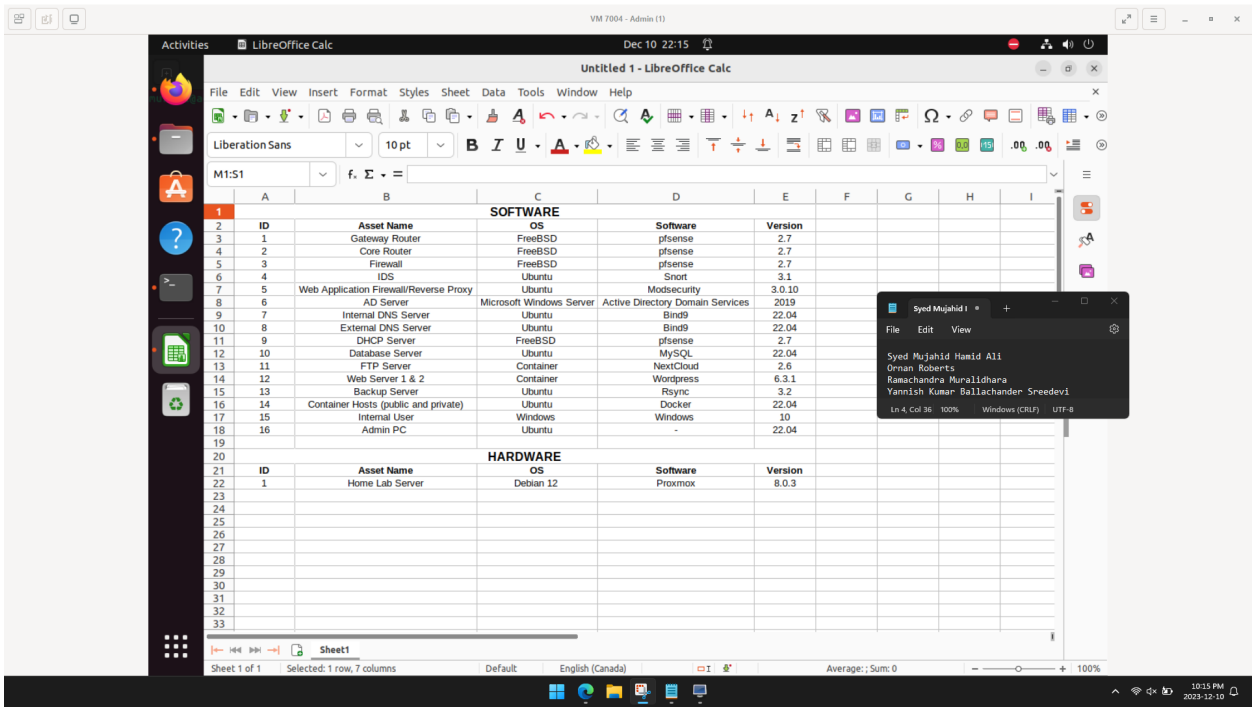


Fig.21 Table showing every asset used for this project (including hardware)

Conclusion

The security testing report for Agricore infrastructure reveals the implementation of security controls based on CIS recommendations. Access management controls such as RBAC were implemented using GPOs. Through this authorized personnel were assigned appropriate access. For audit log management controls, Snort IDS was exhibited and logs were created which ensured the system's ability to monitor and respond to suspicious activities. Similarly, other controls were implemented and tested to protect the web browser where SSL was added. For data backup and recovery, solutions were tested to ensure backups were performed. To conclude, this report confirms a well-designed security control framework for Agricore infrastructure.