Contents

[04 PROTECT CHALLENGE 3](#_Toc11231902)

[4.1 Windows Active Directory 4](#_Toc11231903)

[4.1.1 Login to Windows 4](#_Toc11231904)

[4.1.2 Server Manager 4](#_Toc11231905)

[4.1.3 Orientation Fileshare 5](#_Toc11231906)

[4.1.4 Configuring Permissions I 6](#_Toc11231907)

[4.1.5 Configuring Permissions II 7](#_Toc11231908)

[4.2 Firewall Rules 8](#_Toc11231909)

[4.2.1 Login to Kali 8](#_Toc11231910)

[4.2.2 Login to Pfsense 8](#_Toc11231911)

[4.2.3 Mail Server Rule 9](#_Toc11231912)

[4.2.4 Web Browsing Rule 9](#_Toc11231913)

[4.2.5 Download Configuration 10](#_Toc11231914)

[05 VULNERABILITY ANALYSIS 12](#_Toc11231915)

[5.1 Equipping OpenVAS 12](#_Toc11231916)

[5.1.1 Logging in to Kali 12](#_Toc11231917)

[5.1.2 Opening a Terminal 12](#_Toc11231918)

[5.1.3 Intergace Configuration 12](#_Toc11231919)

[5.1.4 Mapping the Network 12](#_Toc11231920)

[5.1.5 Editing the Report 12](#_Toc11231921)

[5.1.6 Starting OpenVAS 12](#_Toc11231922)

[5.1.7 Printing Network Connections 12](#_Toc11231923)

[5.1.8 Checking Setup 13](#_Toc11231924)

[5.2 Scanning Vulnerabilities in GSA 13](#_Toc11231925)

[5.2.1 Opening a Web Browser 13](#_Toc11231926)

[5.2.2 OpenVAS Web UI 13](#_Toc11231927)

[5.2.3 Learning GSA 13](#_Toc11231928)

[5.2.4 Creating a Target 13](#_Toc11231929)

[5.2.5 Starting a Task 1 13](#_Toc11231930)

[5.2.6 Starting a Task 2 13](#_Toc11231931)

[5.2.7 Running the Scan 13](#_Toc11231932)

[5.2.8 Adding Credentials 1 13](#_Toc11231933)

[5.2.9 Adding Credentials 2 13](#_Toc11231934)

[5.2.10 Creating Second target 13](#_Toc11231935)

[5.2.11 Starting Second Task 1 13](#_Toc11231936)

[5.2.12 Starting Second Task 2 13](#_Toc11231937)

[5.2.13 Running the Second Scan 13](#_Toc11231938)

[5.2.14 Saving Scans 13](#_Toc11231939)

[5.3 Observing Scan Results 13](#_Toc11231940)

[5.3.1 Noting LAN results 1 13](#_Toc11231941)

[5.3.2 Noting LAN results 2 14](#_Toc11231942)

[5.3.3 Noting LAN results 3 14](#_Toc11231943)

[5.3.4 Noting UBUNTU results 1 14](#_Toc11231944)

[5.3.5 Noting UBUNTU results 2 14](#_Toc11231945)

[5.3.6 Noting UBUNTU results 3 14](#_Toc11231946)

[06 DETECT CHALLENGE 15](#_Toc11231947)

[07 NOTIFICATION AND ESCALATION 16](#_Toc11231948)

[08 RESPOND CHALLENGE 17](#_Toc11231949)

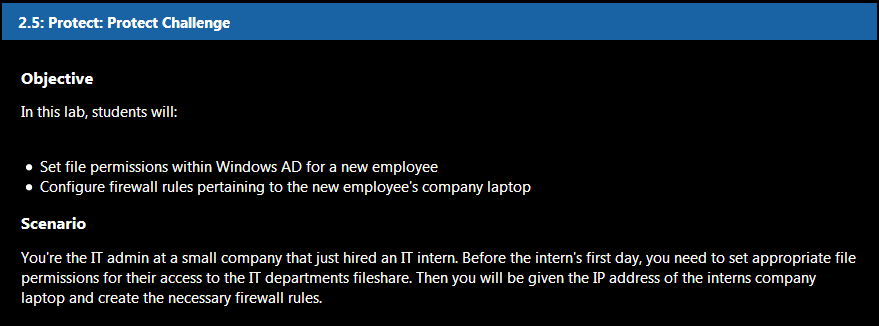
[09 RE-IMAGING 18](#_Toc11231950)

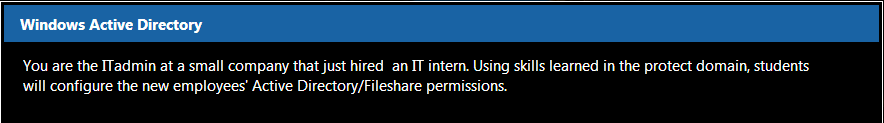
[10 RESTORE POINTS AND PASSWORD RECOVERY 19](#_Toc11231951)

[Appendix 20](#_Toc11231952)

# 04 PROTECT CHALLENGE

|  |  |
| --- | --- |
| TASK | KEY PERFORMANCE INDICATORS |
| Set ITadmin's permissions correctly for Orientation Share | **S0067**: Skill in identifying, modifying, and manipulating applicable system components within Windows, Unix, or Linux (e.g., passwords, user accounts, files).  **S0097**: Skill in applying security controls.  **S0121**: Skill in system, network, and OS hardening techniques. (e.g., remove unnecessary services, password policies, network segmentation, enable logging, least privilege, etc.).  **T0358**: Design and develop system administration and management functionality for privileged access users.  **K0167**: Knowledge of system administration, network, and operating system hardening techniques |
| Set ITintern's permissions correctly for Orientation Share | **K0167**: Knowledge of system administration, network, and operating system hardening techniques.  **T0358**: Design and develop system administration and management functionality for privileged access users.  **S0121**: Skill in system, network, and OS hardening techniques. (e.g., remove unnecessary services, password policies, network segmentation, enable logging, least privilege, etc.) |
| Created IT Projects Share | **S0121:** Skill in system, network, and OS hardening techniques. (e.g., remove unnecessary services, password policies, network segmentation, enable logging, least privilege, etc.).  **T0358:** Design and develop system administration and management functionality for privileged access users.  **K0167:** Knowledge of system administration, network, and operating system hardening techniques |
| Created FW Rule for SMTP to Intern | **K0049:** Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).  **K0202:** Knowledge of the application firewall concepts and functions (e.g., Single point of authentication/audit/policy enforcement, message scanning for malicious content, data anonymization for PCI and PII compliance, data loss protection scanning, accelerated cryptographic operations, SSL security, REST/JSON processing).  **K0487:** Knowledge of network security (e.g., encryption, firewalls, authentication, honey pots, perimeter protection).  **K0516:** Knowledge of physical and logical network devices and infrastructure to include hubs, switches, routers, firewalls, etc. |
| Created FW Rule for Intern Web Browsing | **K0516:** Knowledge of physical and logical network devices and infrastructure to include hubs, switches, routers, firewalls, etc.  **S0076:** Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, antivirus software, anti-spyware).  **S0084:** Skill in configuring and utilizing network protection components (e.g., Firewalls, VPNs, network intrusion detection systems).  **S0170:** Skill in configuring and utilizing computer protection components (e.g., hardware firewalls, servers, routers, as appropriate) |





## 4.1 Windows Active Directory

### 4.1.1 Login to Windows

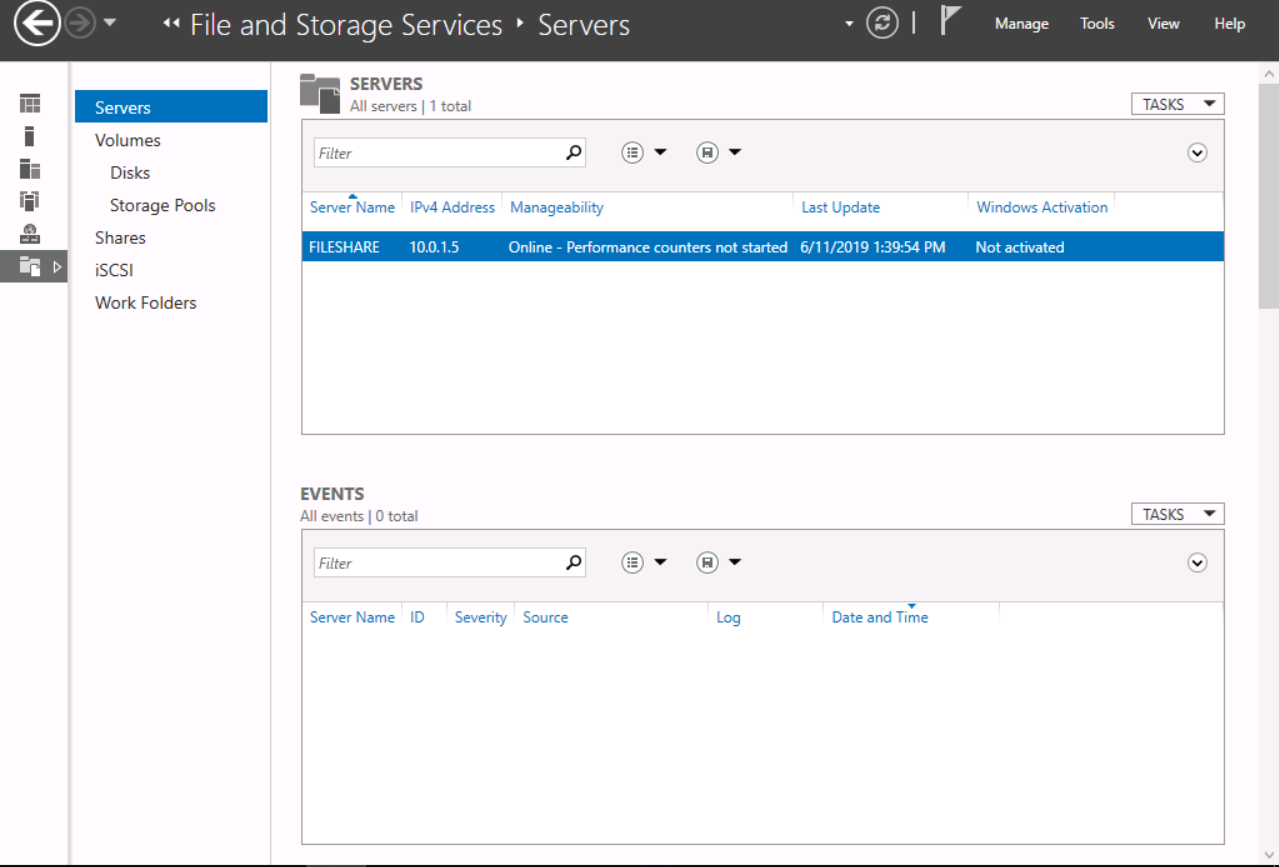
Log in to the Windows Server. User: **itadmin** Password: **IamanIT!**

### 4.1.2 Server Manager

Open **Server Manager** (If it doesn't open upon login). Click on **File and Storage Services**.

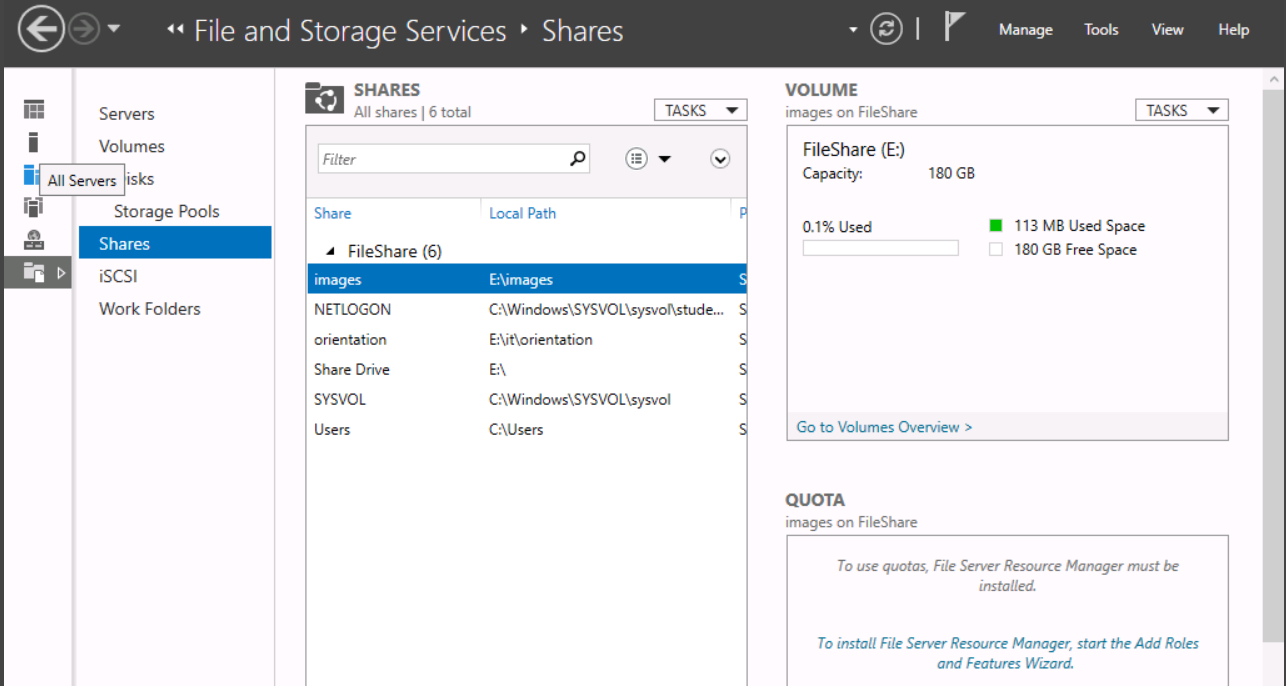
|  |  |
| --- | --- |
|  |  |
|  |  |

|  |  |
| --- | --- |
|  |  |



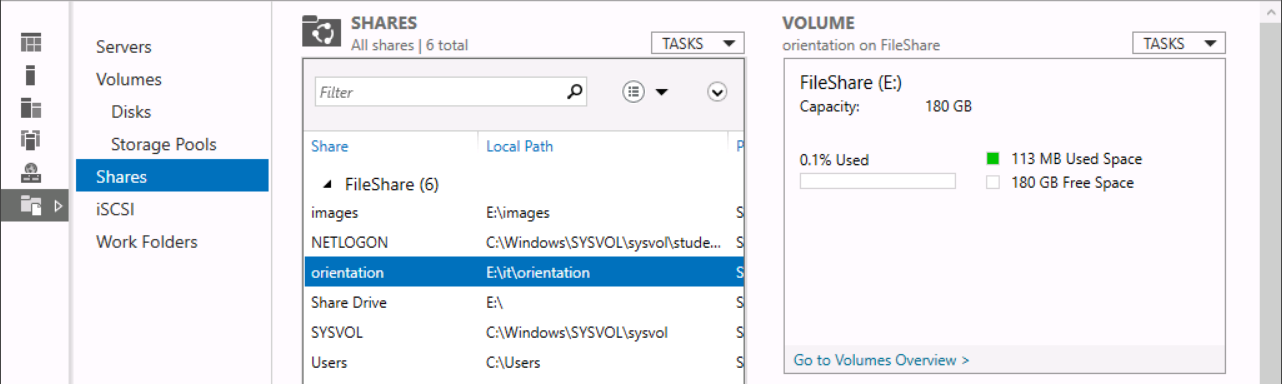
### 4.1.3 Orientation Fileshare

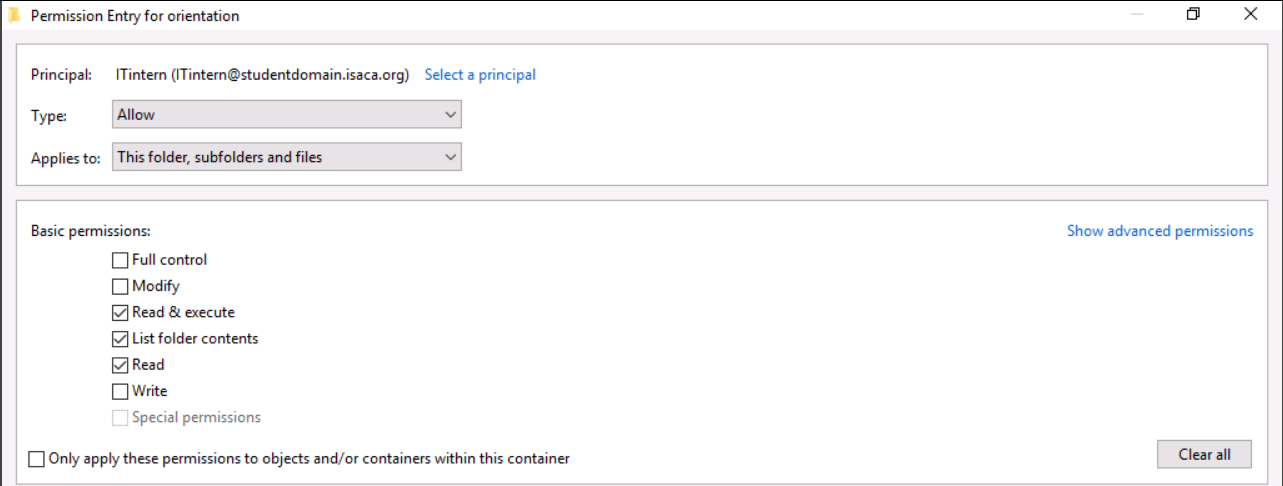
In preparation for their newest team member, the IT team shared an Orientation folder which will contain important documents for their intern's first week. Click **Shares**.

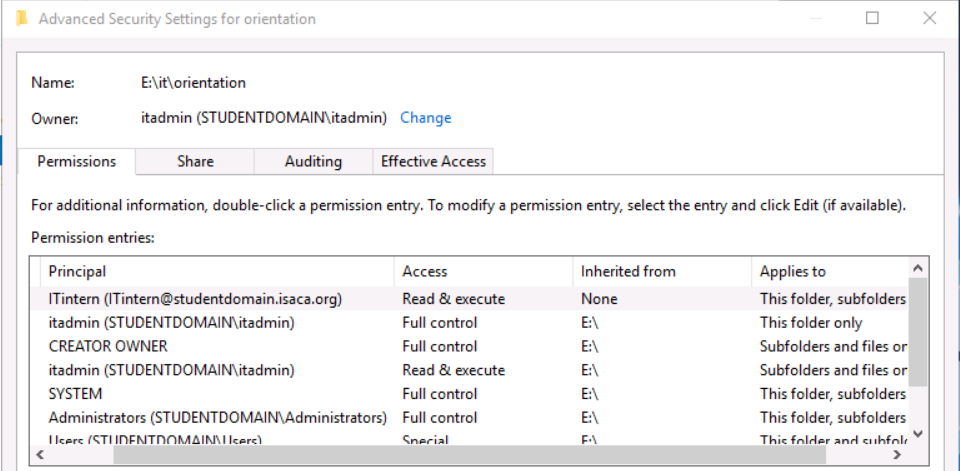


### 4.1.4 Configuring Permissions I

For the **E: --> IT --> Orientation** fileshare, give **ITintern Read** and **Execute** permissions. Give **ITadmin full control**.

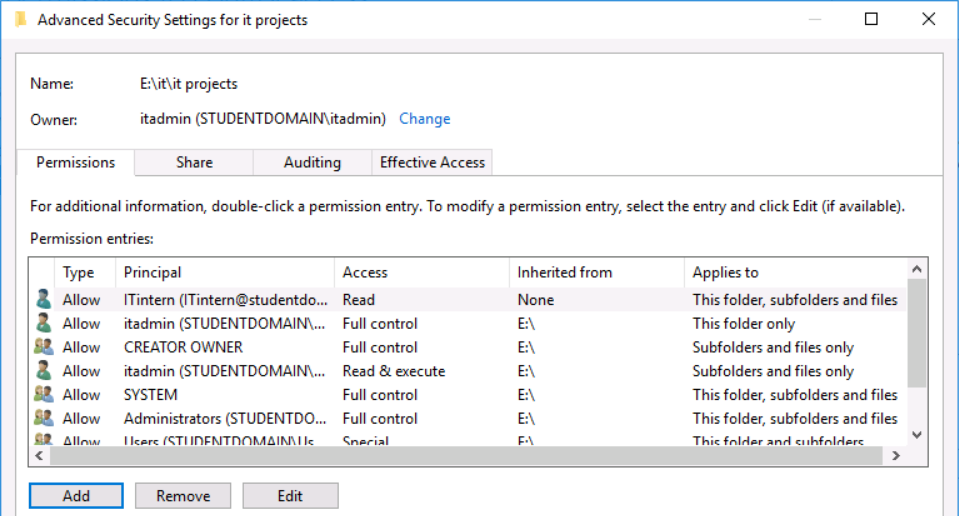


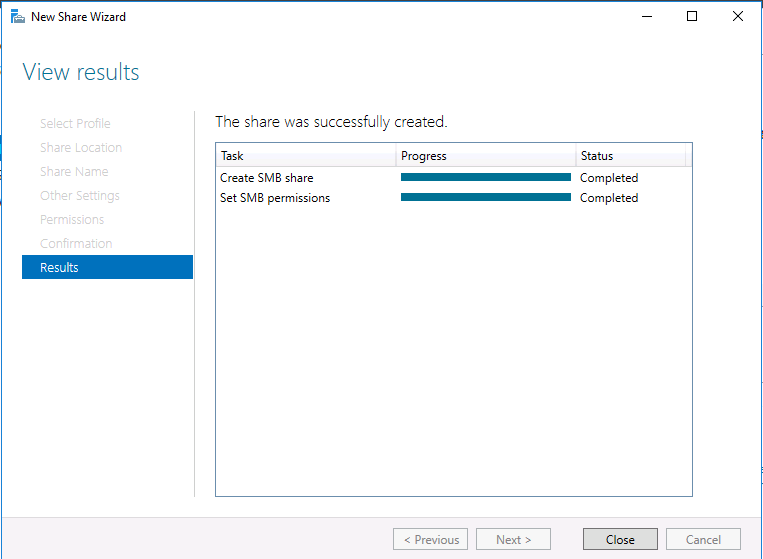


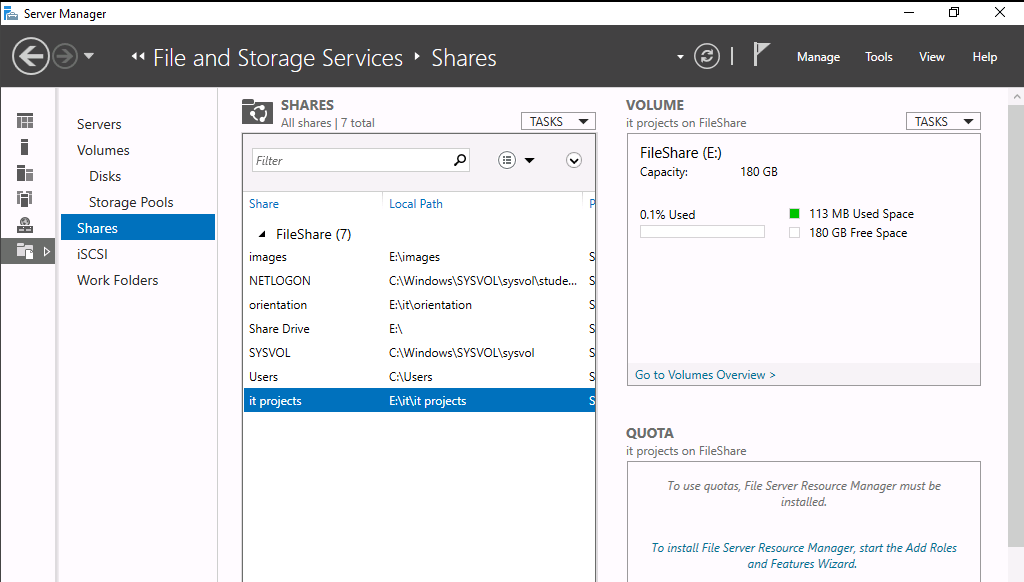


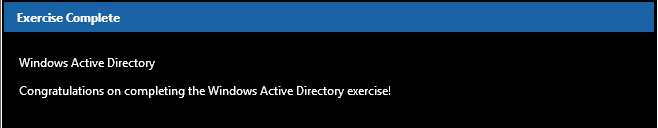
### 4.1.5 Configuring Permissions II

Create a share for the **IT projects folder** within the **IT directory**. Give **ITintern** **read-only** permissions.

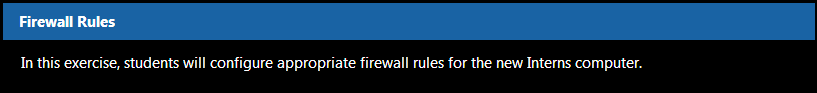








## 4.2 Firewall Rules

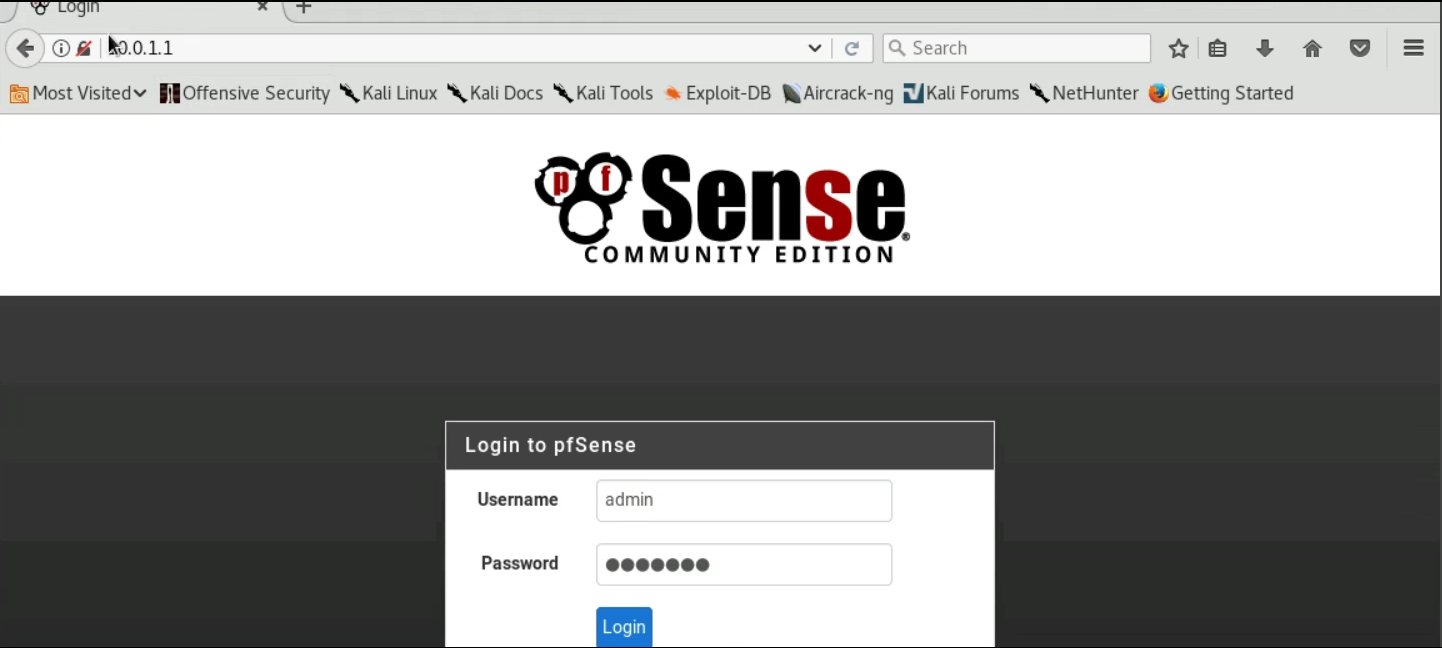


### 4.2.1 Login to Kali

Login to Kali with username **root** and password **isaca**., Then, open a browser and navigate to **http://10.0.1.1**

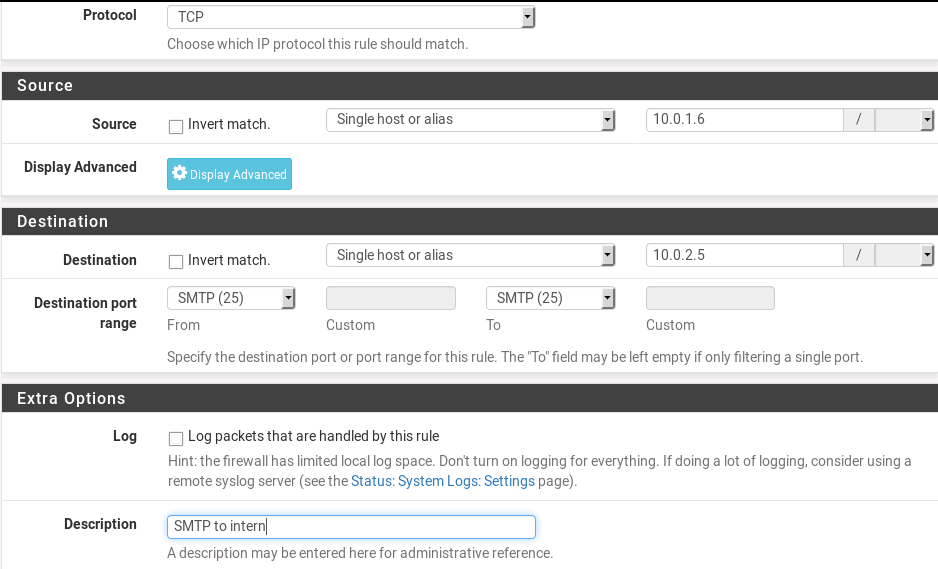
### 4.2.2 Login to Pfsense

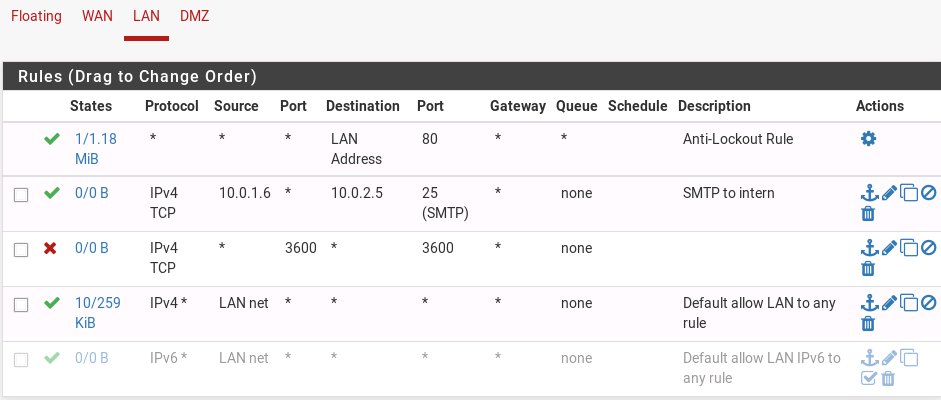
Login to Pfsense with username **admin**, and password **pfsense**



### 4.2.3 Mail Server Rule

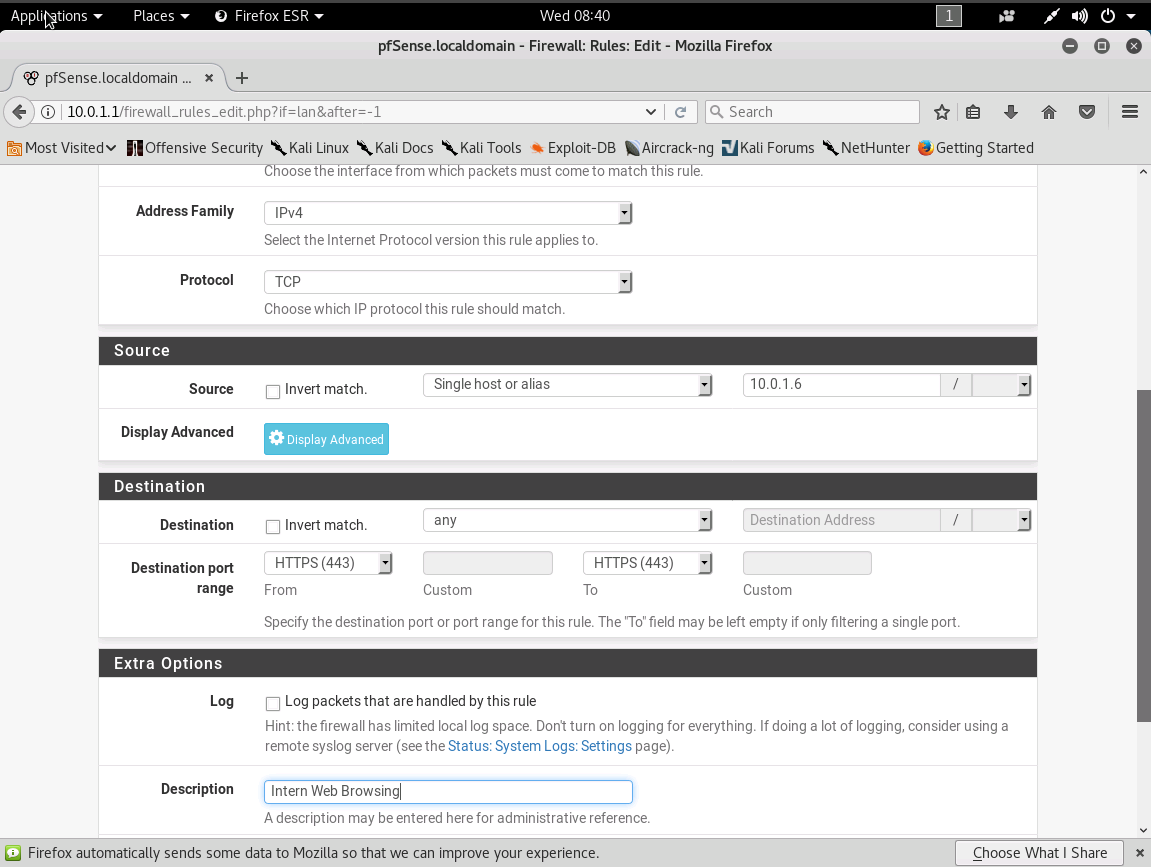
Click **Firewall --> Rules**. Then create a LAN rule allowing the Interns computer to receive mail from our mail server. The mail server is on the **DMZ** with an IP of **10.0.2.5** and uses **SMTP (port 25)** to relay emails. The Intern's new computer has a static IP address of **10.0.1.6** and is on the **LAN**. Set the description as "**SMTP to Intern**".

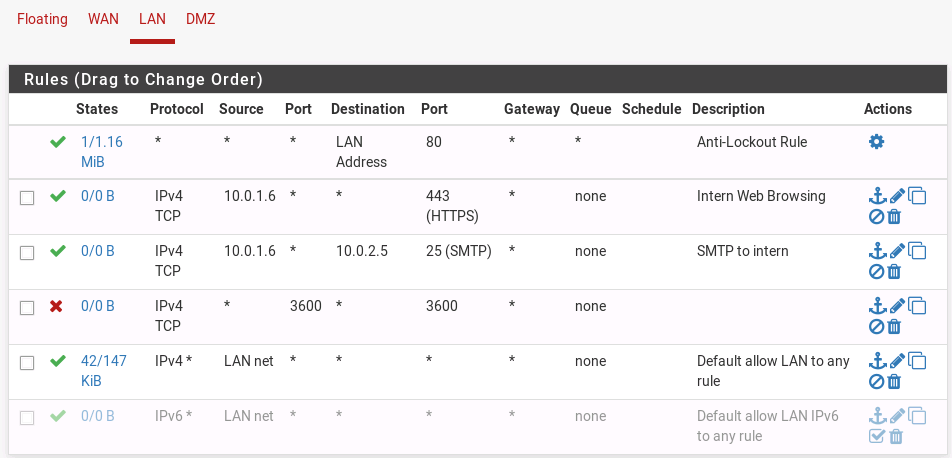




### 4.2.4 Web Browsing Rule

Create another LAN rule, this time allowing the intern to browse the web using **HTTPS**. Set the description as "**Intern Web Browsing**".



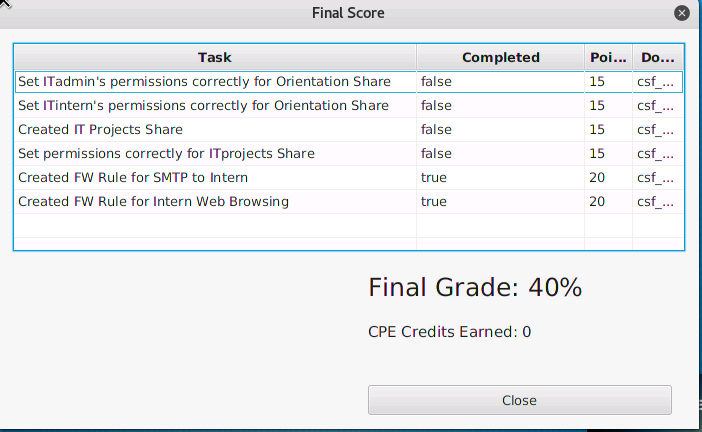


### 4.2.5 Download Configuration

Download your firewall configuration by clicking **Diagnostics --> Backup & Restore**. Then click "**Download configuration as XML**", and rename the file "**InternRules.xml**" and save it to your Desktop.

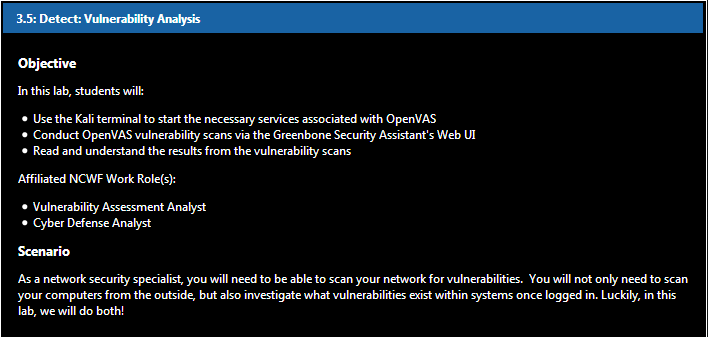
A screenshot of a cell phone

Description automatically generated

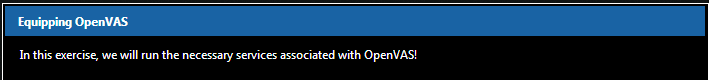


# 05 VULNERABILITY ANALYSIS

|  |  |
| --- | --- |
| TASK | KEY PERFORMANCE INDICATORS |
|  |  |
|  |  |
|  |  |
|  |  |



## 5.1 Equipping OpenVAS



### 5.1.1 Logging in to Kali

Logging into our Kali virtual machine with the following credentials: Username: **root**, Password: **isaca**

### 5.1.2 Opening a Terminal

Open a terminal session by clicking the icon on the left-hand taskbar.

### 5.1.3 Intergace Configuration

Before we begin our data flow identification, type **ifconfig** to take a look at our network interface card (NIC).

It looks like our eth0 interface's IP address is **10.0.1.**2.

### 5.1.4 Mapping the Network

### 5.1.5 Editing the Report

### 5.1.6 Starting OpenVAS

### 5.1.7 Printing Network Connections

### 5.1.8 Checking Setup

## 5.2 Scanning Vulnerabilities in GSA

### 5.2.1 Opening a Web Browser

### 5.2.2 OpenVAS Web UI

### 5.2.3 Learning GSA

### 5.2.4 Creating a Target

### 5.2.5 Starting a Task 1

### 5.2.6 Starting a Task 2

### 5.2.7 Running the Scan

### 5.2.8 Adding Credentials 1

### 5.2.9 Adding Credentials 2

### 5.2.10 Creating Second target

### 5.2.11 Starting Second Task 1

### 5.2.12 Starting Second Task 2

### 5.2.13 Running the Second Scan

### 5.2.14 Saving Scans

## 5.3 Observing Scan Results

### 5.3.1 Noting LAN results 1

### 5.3.2 Noting LAN results 2

### 5.3.3 Noting LAN results 3

### 5.3.4 Noting UBUNTU results 1

### 5.3.5 Noting UBUNTU results 2

### 5.3.6 Noting UBUNTU results 3

# 06 DETECT CHALLENGE

|  |  |
| --- | --- |
| TASK | KEY PERFORMANCE INDICATORS |
|  |  |
|  |  |
|  |  |
|  |  |

# 07 NOTIFICATION AND ESCALATION

|  |  |
| --- | --- |
| TASK | KEY PERFORMANCE INDICATORS |
|  |  |
|  |  |
|  |  |
|  |  |

# 08 RESPOND CHALLENGE

|  |  |
| --- | --- |
| TASK | KEY PERFORMANCE INDICATORS |
|  |  |
|  |  |
|  |  |
|  |  |

# 09 RE-IMAGING

|  |  |
| --- | --- |
| TASK | KEY PERFORMANCE INDICATORS |
|  |  |
|  |  |
|  |  |
|  |  |

# 10 RESTORE POINTS AND PASSWORD RECOVERY

|  |  |
| --- | --- |
| TASK | KEY PERFORMANCE INDICATORS |
|  |  |
|  |  |
|  |  |
|  |  |

# Appendix