**Accelerated CSX Cybersecurity Practitioner Certification**

[04 PROTECT CHALLENGE 2](#_Toc11425452)

[4.1 Windows Active Directory 3](#_Toc11425453)

[4.1.1 Login to Windows 3](#_Toc11425454)

[4.1.2 Server Manager 3](#_Toc11425455)

[4.1.3 Orientation Fileshare 4](#_Toc11425456)

[4.1.4 Configuring Permissions I 5](#_Toc11425457)

[4.1.5 Configuring Permissions II 6](#_Toc11425458)

[4.2 Firewall Rules 7](#_Toc11425459)

[4.2.1 Login to Kali 8](#_Toc11425460)

[4.2.2 Login to Pfsense 8](#_Toc11425461)

[4.2.3 Mail Server Rule 8](#_Toc11425462)

[4.2.4 Web Browsing Rule 9](#_Toc11425463)

[4.2.5 Download Configuration 10](#_Toc11425464)

[05 VULNERABILITY ANALYSIS 12](#_Toc11425465)

[5.1 Equipping OpenVAS 12](#_Toc11425466)

[5.1.1 Logging in to Kali 12](#_Toc11425467)

[5.1.2 Opening a Terminal 12](#_Toc11425468)

[5.1.3 Intergace Configuration 12](#_Toc11425469)

[5.1.4 Mapping the Network 13](#_Toc11425470)

[5.1.5 Editing the Report 13](#_Toc11425471)

[5.1.6 Starting OpenVAS 13](#_Toc11425472)

[5.1.7 Printing Network Connections 13](#_Toc11425473)

[5.1.8 Checking Setup 13](#_Toc11425474)

[5.2 Scanning Vulnerabilities in GSA 15](#_Toc11425475)

[5.2.1 Opening a Web Browser 15](#_Toc11425476)

[5.2.2 OpenVAS Web UI 15](#_Toc11425477)

[5.2.3 Learning GSA 16](#_Toc11425478)

[5.2.4 Creating a Target 16](#_Toc11425479)

[5.2.5 Starting a Task 1 16](#_Toc11425480)

[5.2.6 Starting a Task 2 16](#_Toc11425481)

[5.2.7 Running the Scan 16](#_Toc11425482)

[5.2.8 Adding Credentials 1 16](#_Toc11425483)

[5.2.9 Adding Credentials 2 16](#_Toc11425484)

[5.2.10 Creating Second target 16](#_Toc11425485)

[5.2.11 Starting Second Task 1 16](#_Toc11425486)

[5.2.12 Starting Second Task 2 16](#_Toc11425487)

[5.2.13 Running the Second Scan 17](#_Toc11425488)

[5.2.14 Saving Scans 17](#_Toc11425489)

[5.3 Observing Scan Results 17](#_Toc11425490)

[5.3.1 Noting LAN results 1 17](#_Toc11425491)

[5.3.2 Noting LAN results 2 17](#_Toc11425492)

[5.3.3 Noting LAN results 3 17](#_Toc11425493)

[5.3.4 Noting UBUNTU results 1 17](#_Toc11425494)

[5.3.5 Noting UBUNTU results 2 17](#_Toc11425495)

[5.3.6 Noting UBUNTU results 3 17](#_Toc11425496)

[06 DETECT CHALLENGE 18](#_Toc11425497)

[6.1 Detect Challenge 18](#_Toc11425498)

[6.1.1 Starting Services 18](#_Toc11425499)

[6.1.2 Creating a File 19](#_Toc11425500)

[6.1.3 Opening the Web UI 19](#_Toc11425501)

[6.1.4 Conducting a Scan 20](#_Toc11425502)

[07 NOTIFICATION AND ESCALATION 21](#_Toc11425503)

[08 RESPOND CHALLENGE 22](#_Toc11425504)

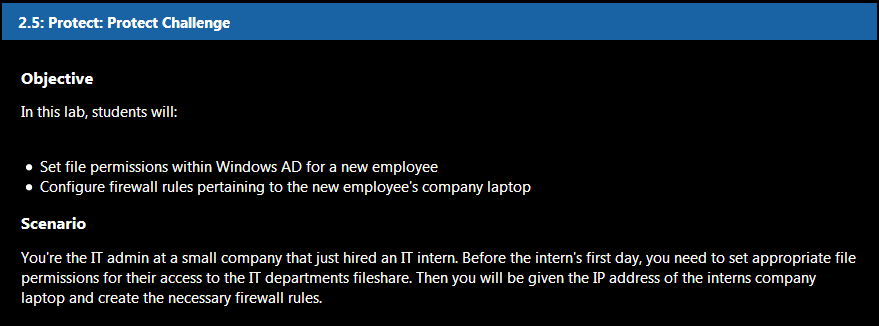
[09 RE-IMAGING 23](#_Toc11425505)

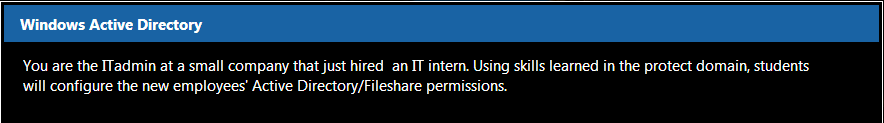
[10 RESTORE POINTS AND PASSWORD RECOVERY 24](#_Toc11425506)

[Appendix 25](#_Toc11425507)

# 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

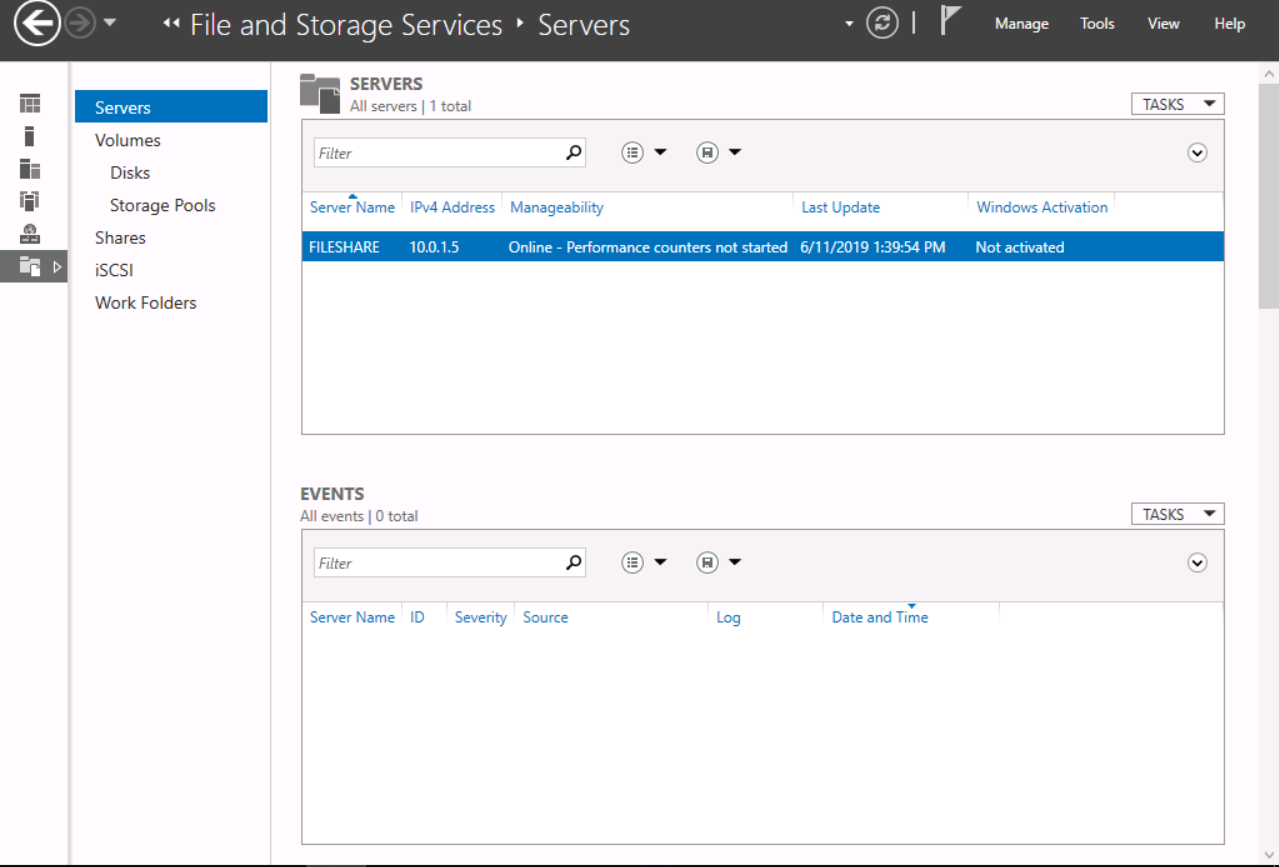
Log in to the Windows Server. User: **itadmin** Password: **IamanIT!**

### 4.1.2 Server Manager

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

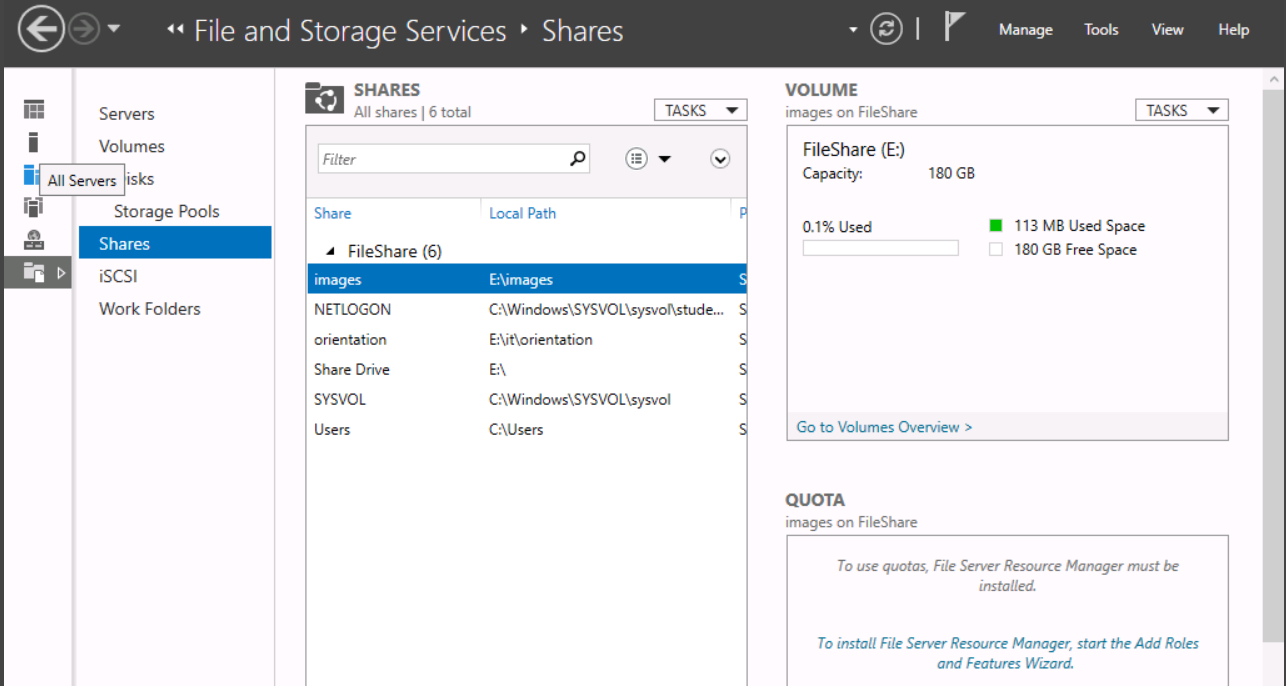
|  |  |
| --- | --- |
|  |  |
|  |  |

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



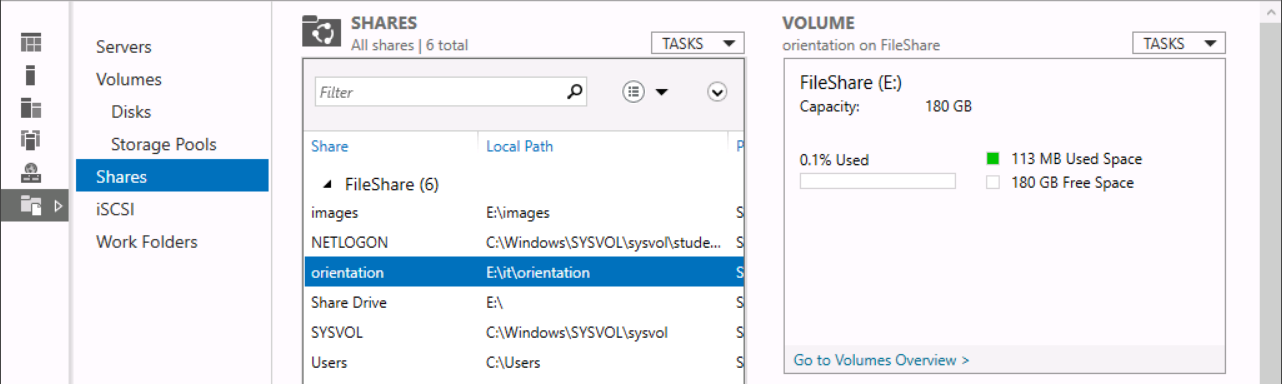
### 4.1.3 Orientation Fileshare

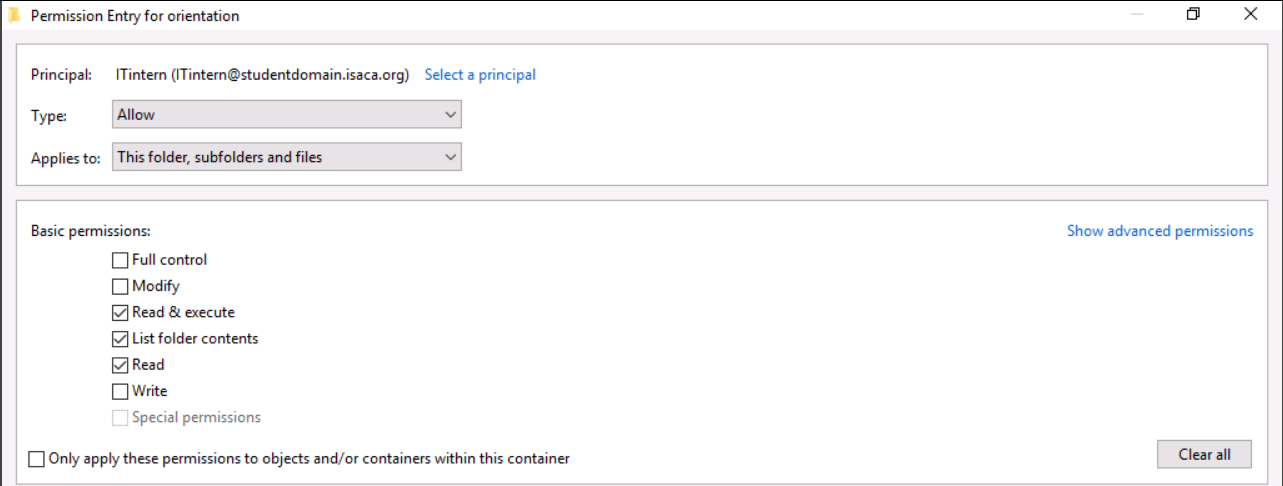
In preparation for their newest team member, the IT team shared an Orientation folder which will contain important documents for their intern's first week. Click **Shares**.

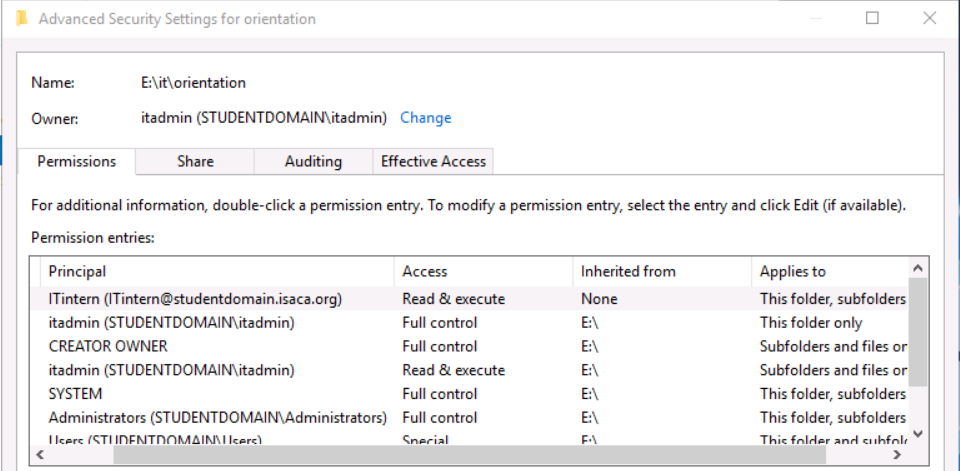


### 4.1.4 Configuring Permissions I

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

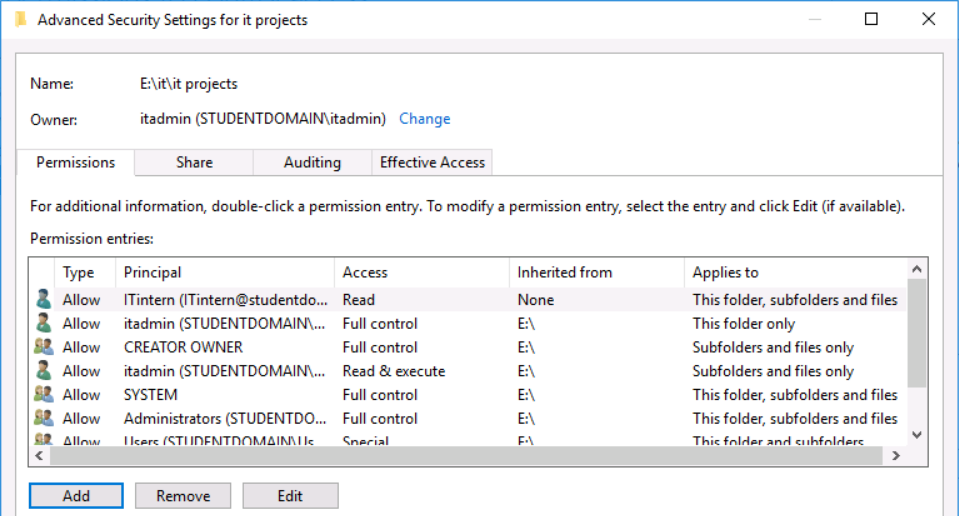


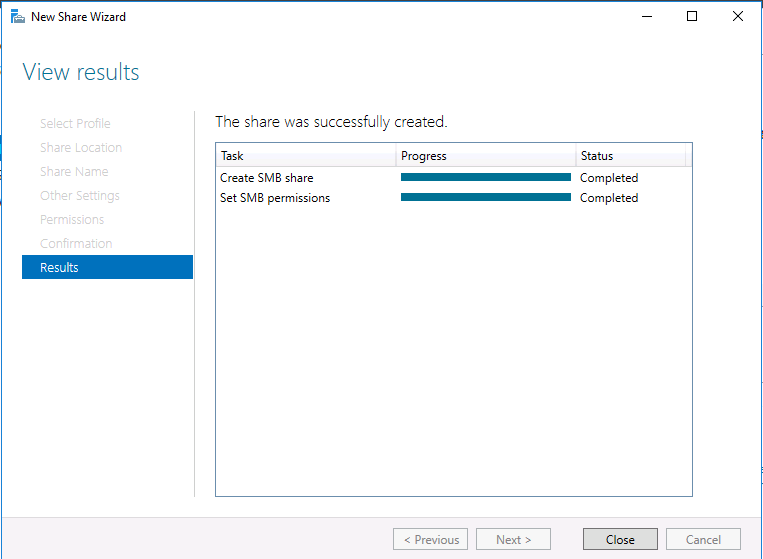


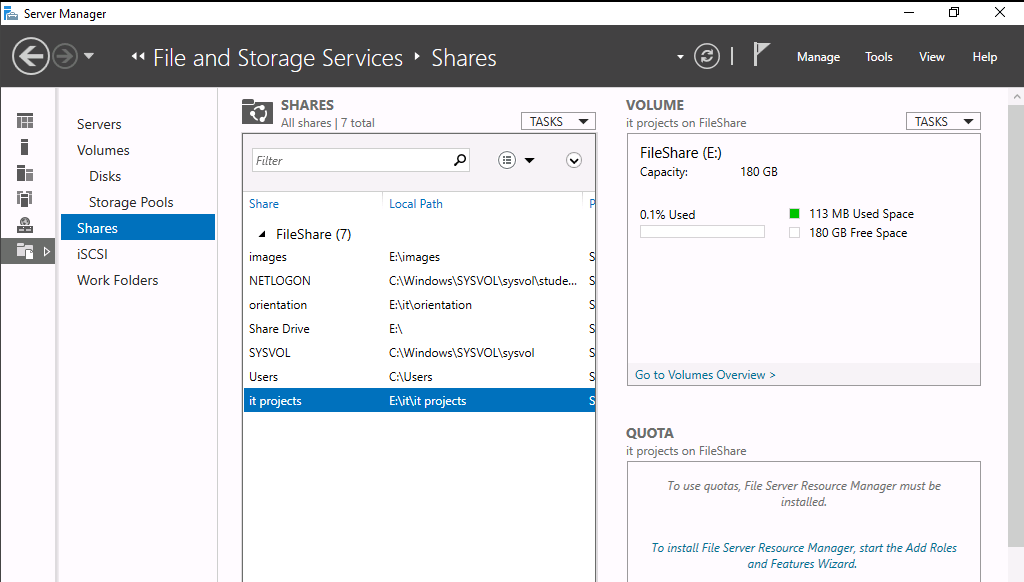


### 4.1.5 Configuring Permissions II

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

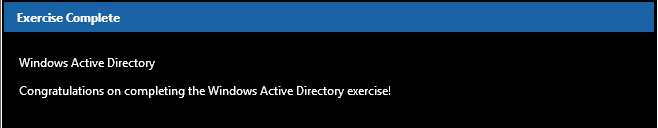




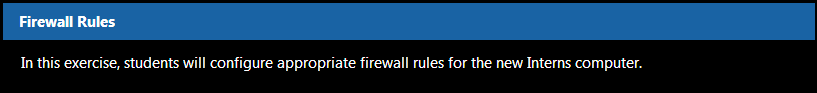


A screenshot of a social media post

Description automatically generated



## 4.2 Firewall Rules

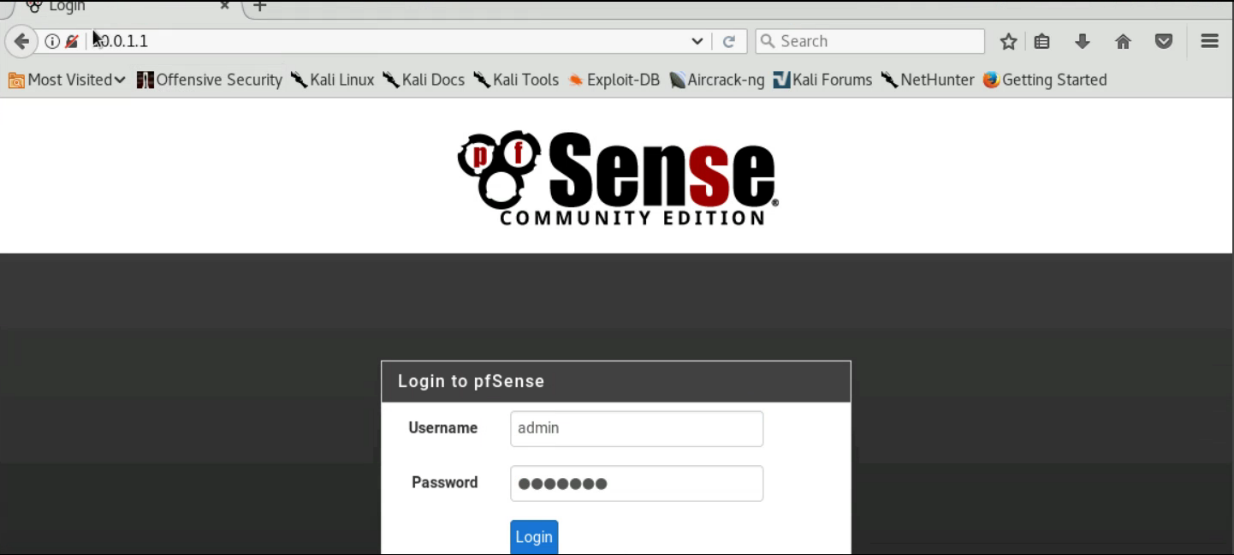


### 4.2.1 Login to Kali

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**

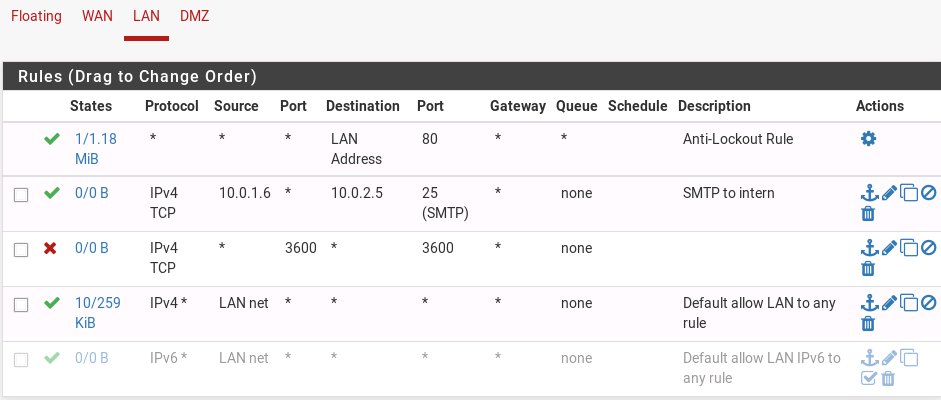


### 4.2.3 Mail Server Rule

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**".

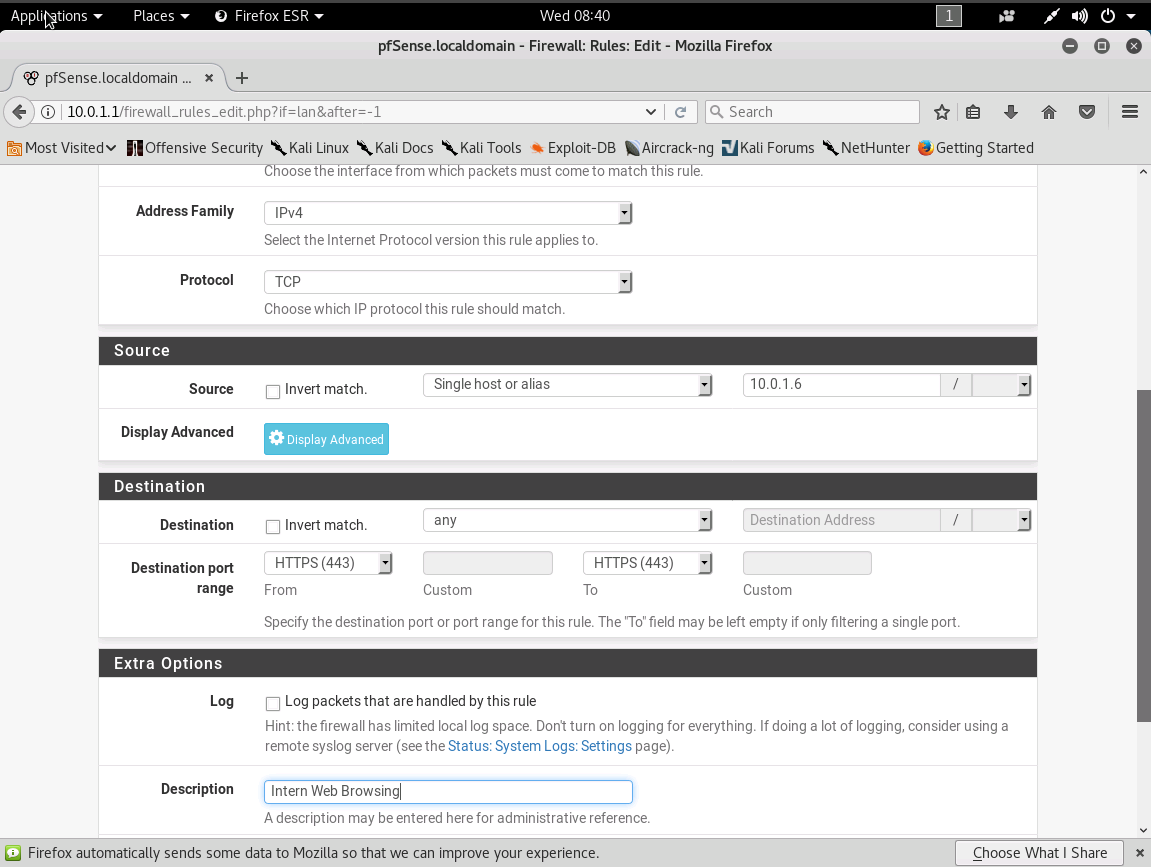
A screenshot of a cell phone

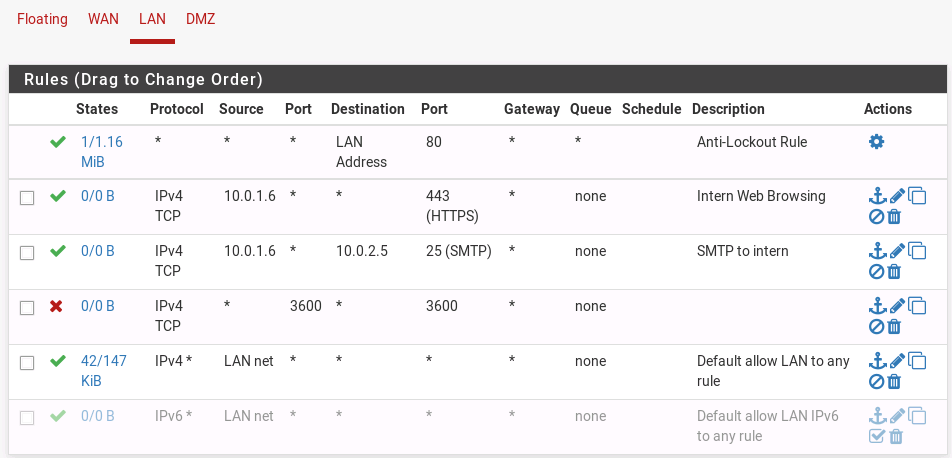
Description automatically generated



### 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**".



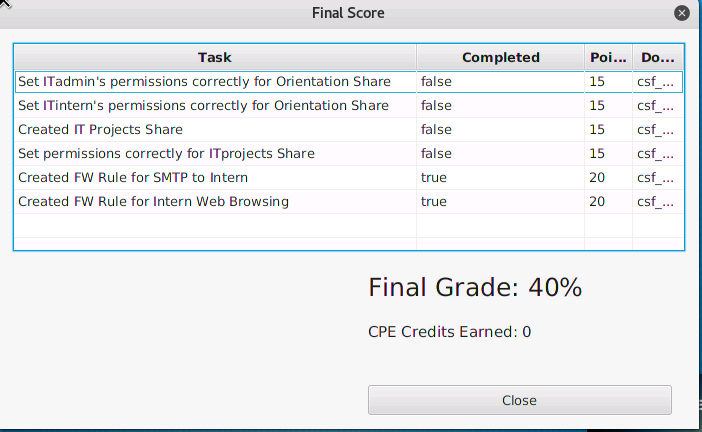


### 4.2.5 Download Configuration

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.

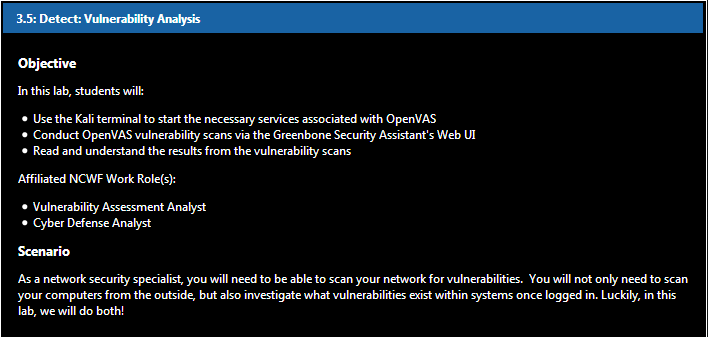
A screenshot of a cell phone

Description automatically generated

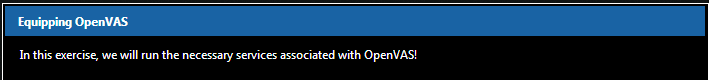


# 05 VULNERABILITY ANALYSIS

|  |  |
| --- | --- |
| 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**

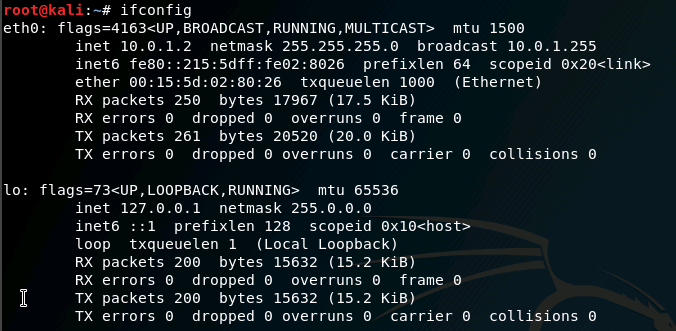
### 5.1.2 Opening a Terminal

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

In order to scan our network for vulnerabilities, we have to map it first. Type **nmap -sn 10.0.1.0/24 > Desktop/nmap.txt** to redirect the output to a new report on the Desktop.

### 5.1.5 Editing the Report

On the Desktop, double-click nmap.txt and delete everything in the file except for the live hosts on the LAN so that the file looks like this. Then save and close the new version of the report.

10.0.1.1

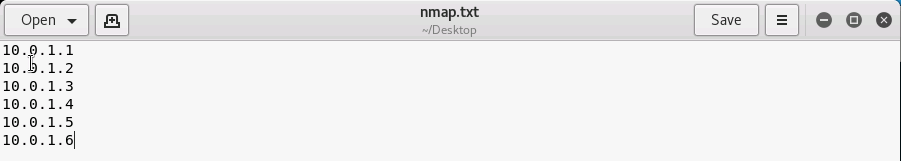
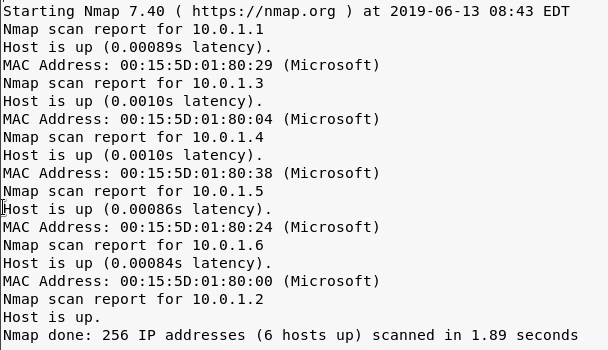
10.0.1.2

10.0.1.3

10.0.1.4

10.0.1.5

10.0.1.6

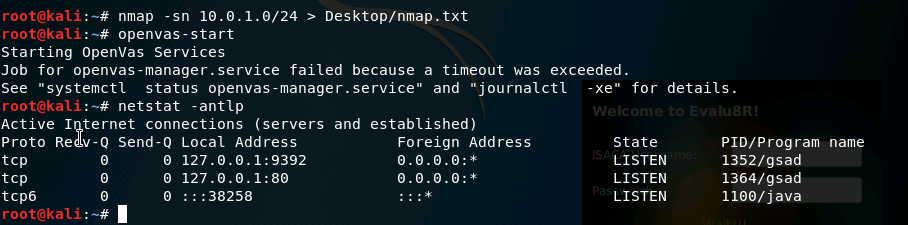


### 5.1.6 Starting OpenVAS

OpenVAS stands for **Open Vulnerability Assessment System**. It is free. Type **openvas-start** to run the services.

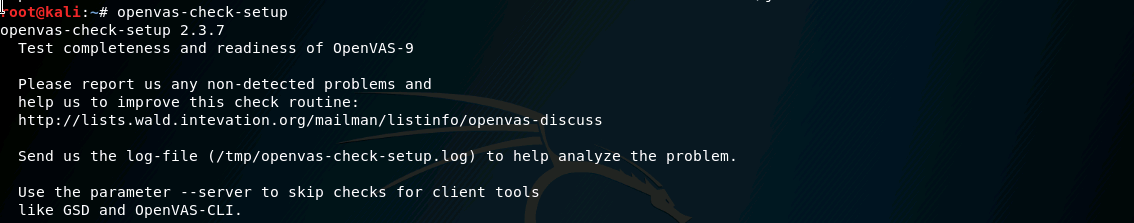
### 5.1.7 Printing Network Connections

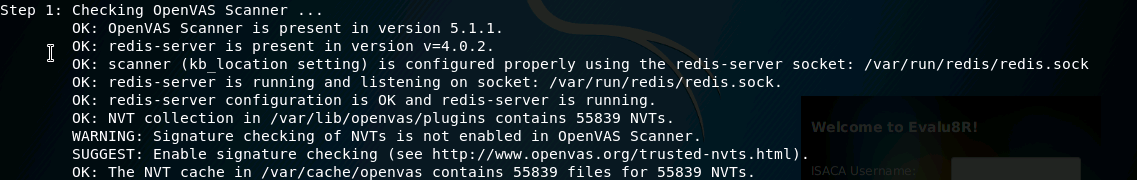
Make sure our OpenVAS services are listening. Type **netstat –antlp.** Check the **Greenbone Security Assistant Daemon (gsad)** and **OpenVAS Manager Daemon (openvasmd)** listening. Note **gsad's local IP address/port (127.0.0.1:9392).**

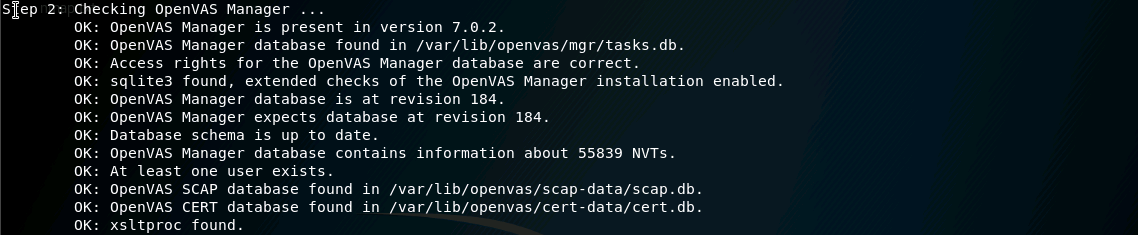


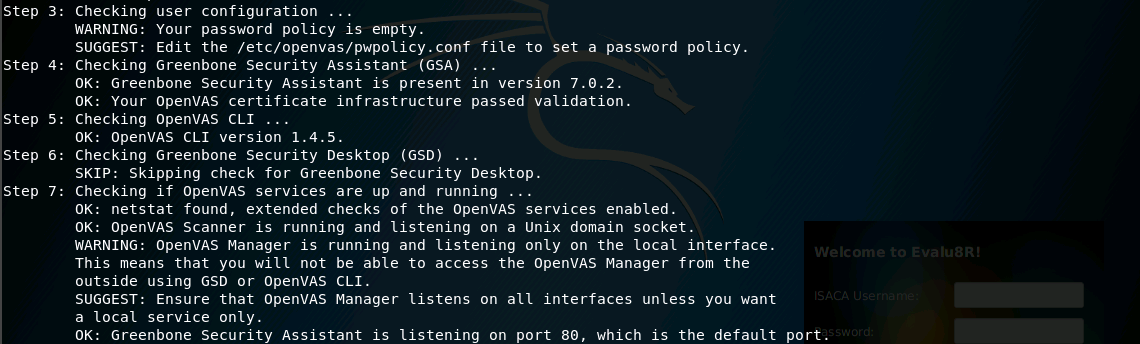
### 5.1.8 Checking Setup

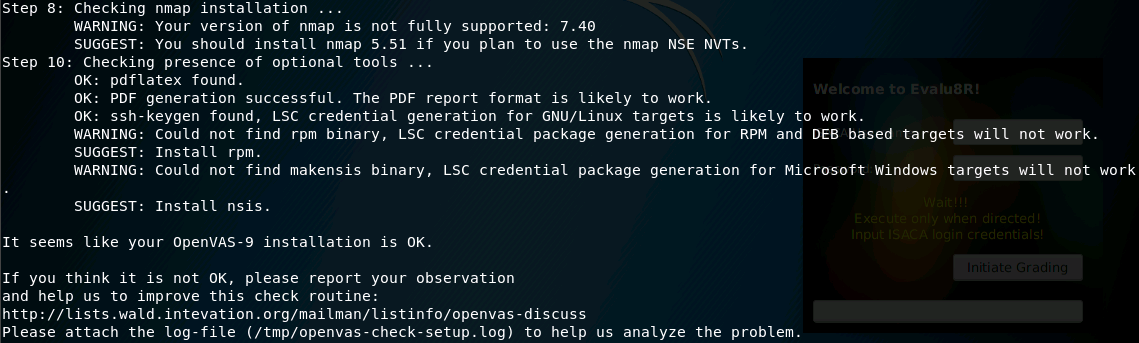
Finally, let's run the command **openvas-check-setup** to ensure that the OpenVAS installation and setup has been implemented correctly. The command's output says "It seems like your OpenVAS-9 installation is OK", so we are good to go! Type exit to close the terminal.













## 5.2 Scanning Vulnerabilities in GSA



### 5.2.1 Opening a Web Browser

Open a new web browser by clicking on the **Firefox ESR** icon on the Favorites bar.

### 5.2.2 OpenVAS Web UI

Do you remember the IP address and the port number of Greenbone Security Assistant taken from the netstat command? Type **https://127.0.0.1:9392** to open the web user interface. If that doesn't work, use **https://127.0.0.1:80**, which should redirect you to the GSA landing page. Click "**Advanced**", "**Add Exceptio**n", and "**Confirm Security Exception**". The credentials are: username: **admin** password: **admin**

A screenshot of a cell phone

Description automatically generated

### 5.2.3 Learning GSA

This is the Greenbone Security Assistant UI. Although the OpenVAS framework is free and open, it has the ability to be very powerful. Greenbone provides users with efficient and effective solutions for vulnerability scanning and management. Hover over "Configuration" and click "Targets".

### 5.2.4 Creating a Target

Click the blue star icon in the upper left-hand corner to create a new target. Name this **nmap**. For hosts, click the "**From file**" radio button and "**Browse..**." for the **nmap.txt** file on the Desktop. Click "**Create**".

A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated

### 5.2.5 Starting a Task 1

Now that we have created a new target, hover over the "**Scans**" tab and click "**Tasks**". Read the pop-up message and wait for it to disappear. Hover over the blue star icon and click "**New Task**".

### 5.2.6 Starting a Task 2

Name this scan **LAN**. Choose the previously created nmap for "**Scan Targets**". Raise the "**Min QoD**" to **80%**. Lower the "**Maximum concurrently executed NVTs per host**" and **"... scanned hosts**" both to 1. Click "Create".

A screenshot of a cell phone

Description automatically generated

### 5.2.7 Running the Scan

On the bottom of the Tasks page, make sure to hit the play button to start the scan. This scan is going to take awhile, so let's move on to the next step.

A screenshot of a cell phone

Description automatically generated

### 5.2.8 Adding Credentials 1

In our administrative notes, we have found more information on a machine placed on the LAN.

**10.0.1.4: Linux (Ubuntu)**

username: **packethunter**

password: **packethunters**

We will be using these credentials to log in to this system remotely for our second vulnerability scan. We will be able to "dig deeper" because of this use of SSH.

### 5.2.9 Adding Credentials 2

Hover over "Configuration" and click "Credentials". Click on the blue star icon to create new credentials for our next scan. Name it **Ubuntu** with a username of **packethunter** and a password of **packethunters**. Click "Create".

A screenshot of a cell phone

Description automatically generated

A screenshot of a social media post

Description automatically generated

### 5.2.10 Creating Second target

Again. hover over "Configuration" and click "Targets". Click the blue star icon. Name this **Ubuntu**. For "Manual" hosts, enter **10.0.1.4**. In the SSH row, select **Ubuntu** on port **22**. Click "Create".

A screenshot of a cell phone

Description automatically generated

A screenshot of a social media post

Description automatically generated

### 5.2.11 Starting Second Task 1

Again, hover over the "Scans" tab and click "Tasks". Hover over the blue star icon and click "New Task".

### 5.2.12 Starting Second Task 2

Name this scan Ubuntu. Choose Ubuntu for "**Scan Targets**". Raise the "**Min QoD**" to **80%**. Lower the "**Maximum concurrently executed NVTs per host**" and **"... scanned hosts**" both to 1. Click "Create".

A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated

A screenshot of a social media post

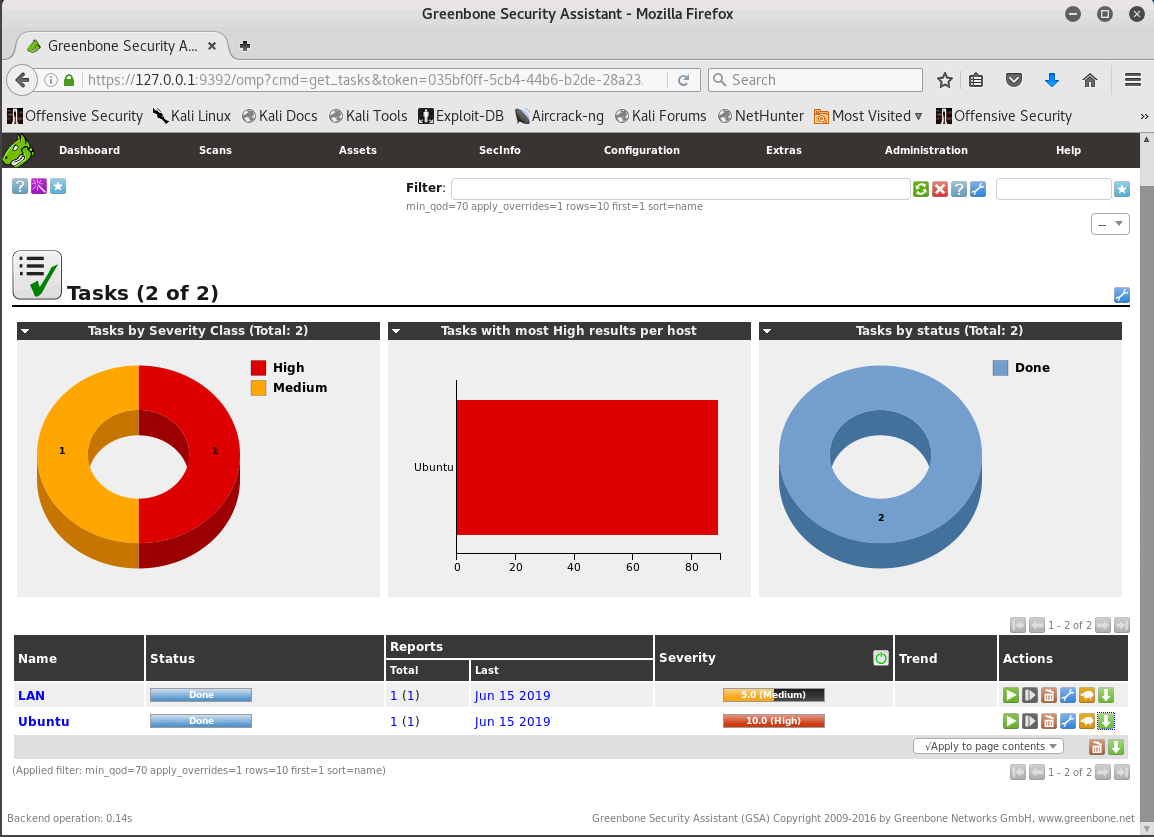
Description automatically generated

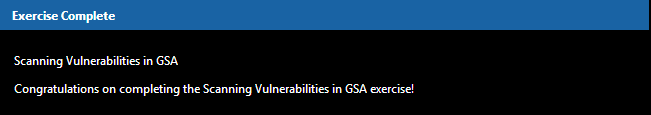
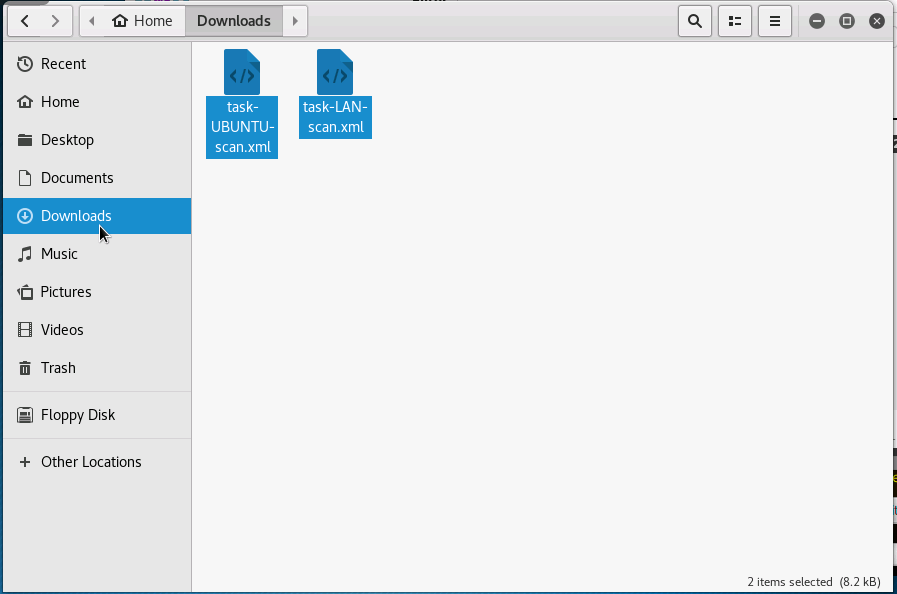
### 5.2.13 Running the Second Scan

Hit the play button to start the scan. This scan will also take awhile. If neither scan is done, feel free to go grab a drink or use the restroom.

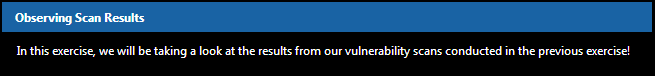
### 5.2.14 Saving Scans

For both scans, click the green download button to save the files. Keep them in the Downloads folder.





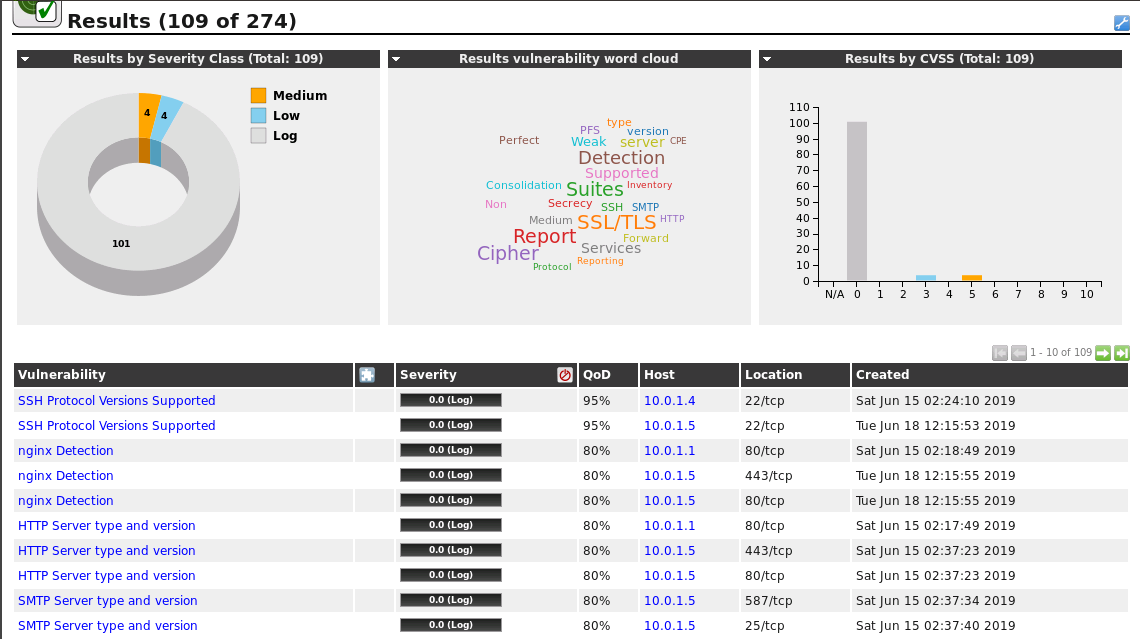
## 5.3 Observing Scan Results



### 5.3.1 Noting LAN results 1

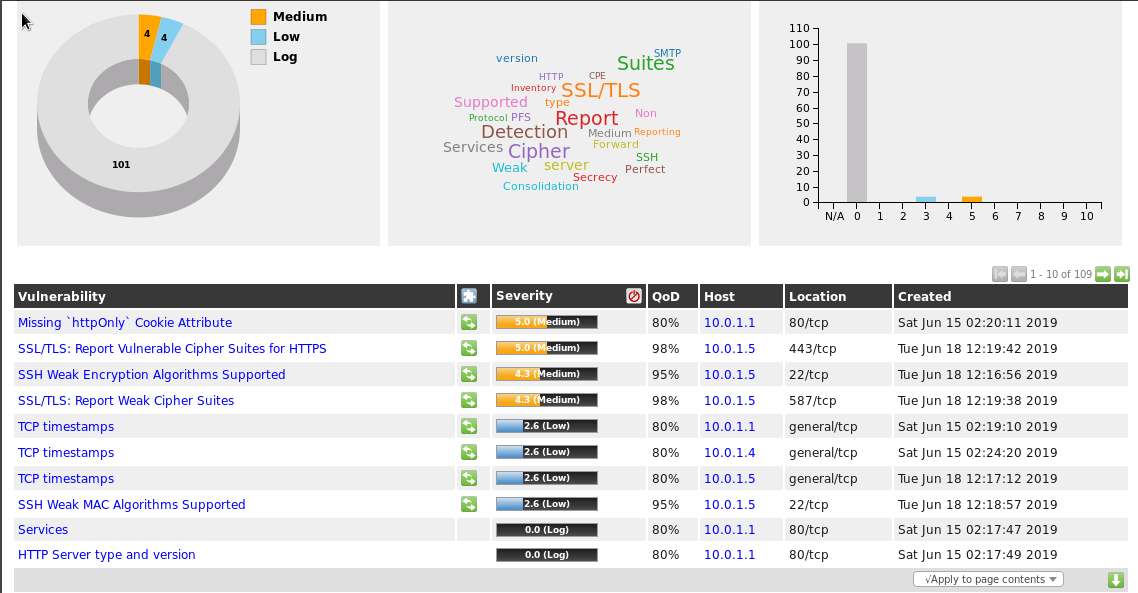
Let's take a look at the LAN vulnerability scan. Click the "**LAN**" task. Click on the number next to "**Results:**"





### 5.3.2 Noting LAN results 2

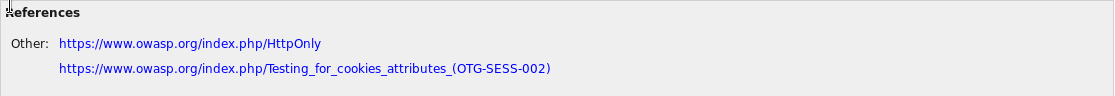
On this page, we can categorize the vulnerabilities by **alphabetical order, solution types, severity, quality of detection, hosts, port and protocol,** and **time**. Click on "**Severit**y" twice to sort from high to low.



### 5.3.3 Noting LAN results 3

Note that there are no high severity ranked vulnerabilities from **10.0.1.4**. Feel free to check these vulnerabilities out by clicking on them!

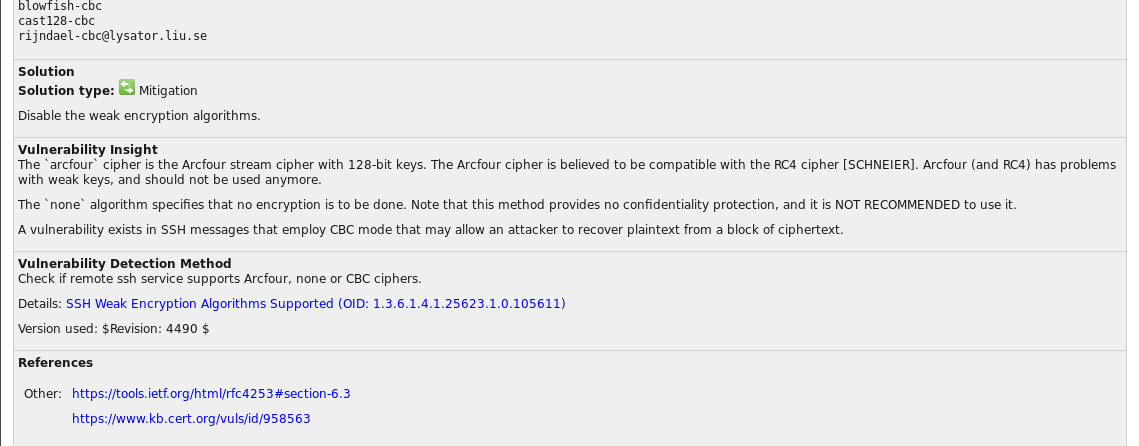


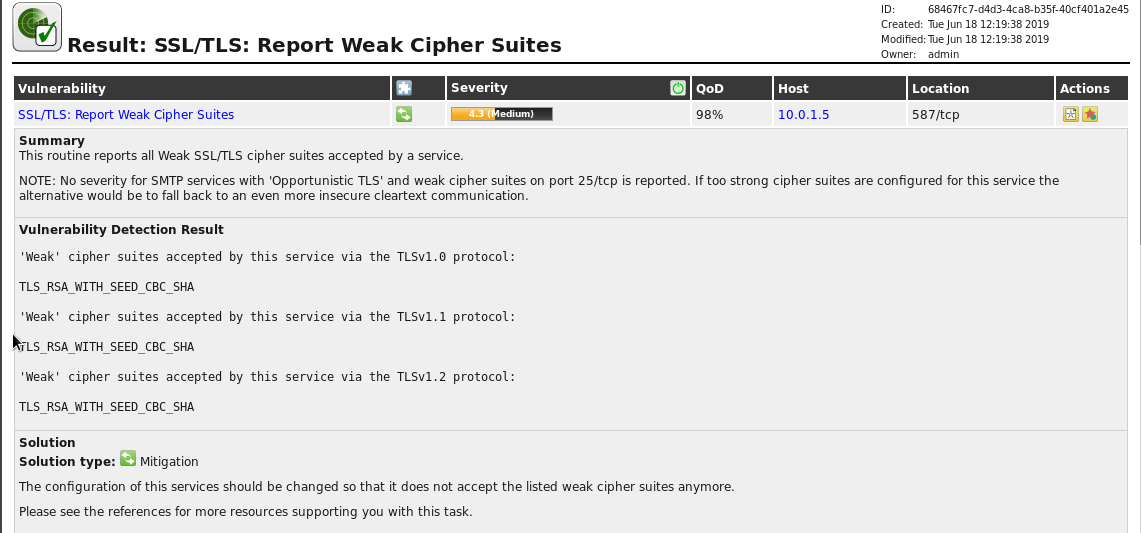


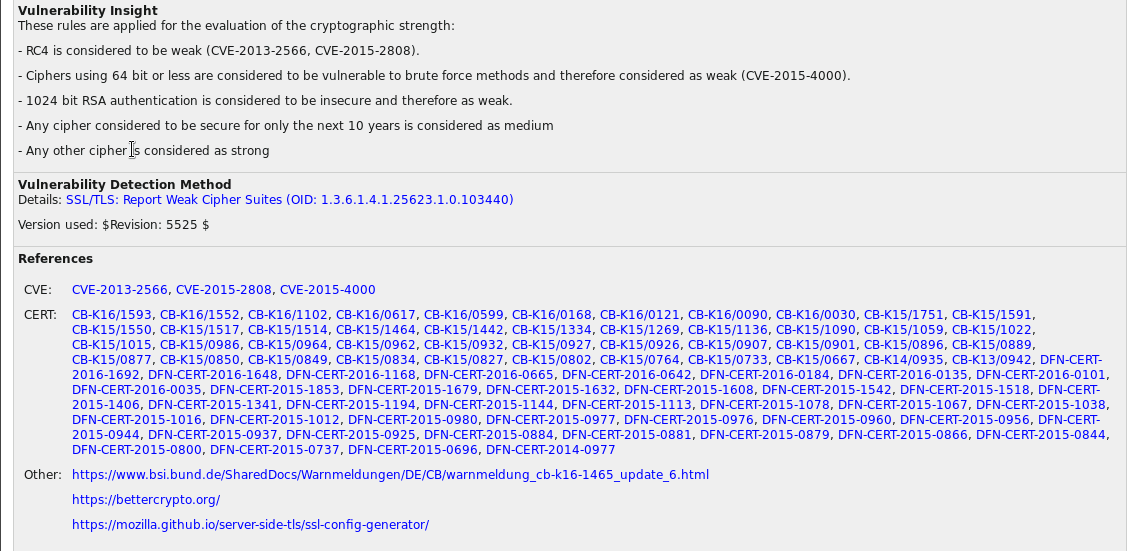












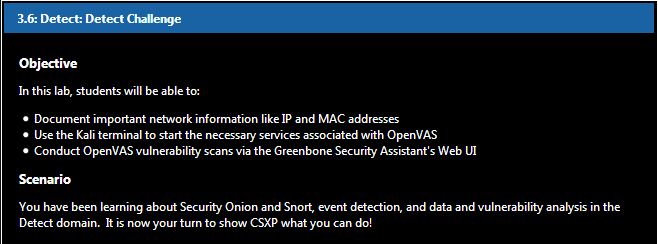
### 5.3.4 Noting UBUNTU results 1

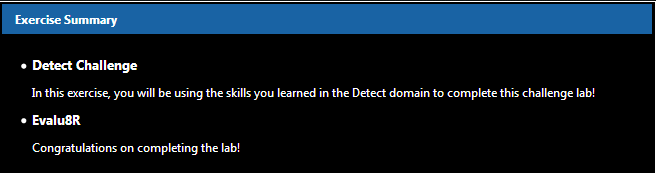
### 5.3.5 Noting UBUNTU results 2

### 5.3.6 Noting UBUNTU results 3

# 06 DETECT CHALLENGE

|  |  |
| --- | --- |
| TASK | KEY PERFORMANCE INDICATORS |
| Recorded IP address | **T0299**: Identify network mapping and operating system (OS) fingerprinting activities.  **T0850**: Perform or support technical network analysis and mapping.  **K0300**: Knowledge of network mapping and recreating network topologies.  **S0081:** Skill in using network analysis tools to identify vulnerabilities. (e.g., fuzzing, nmap, etc.). |
| Recorded MAC address | **S0081**: Skill in using network analysis tools to identify vulnerabilities. (e.g., fuzzing, nmap, etc.).  **K0300:** Knowledge of network mapping and recreating network topologies.  **T0850:** Perform or support technical network analysis and mapping.  **T0299:** Identify network mapping and operating system (OS) fingerprinting activities. |
| Scanned local Kali box | **S0137: Skill in conducting application vulnerability assessments.**  **A0015: Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.**  **T0606: Compile, integrate, and/or interpret all-source data for intelligence or vulnerability value with respect to specific targets.**  **T0616: Conduct network scouting and vulnerability analyses of systems within a network.**  **K0013: Knowledge of cyber defense and vulnerability assessment tools and their capabilities.** |

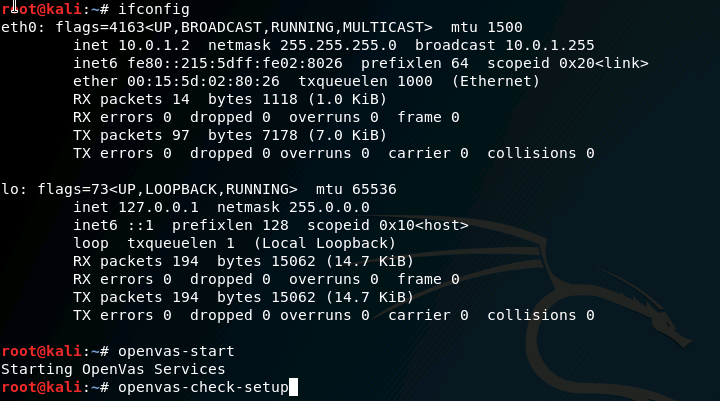


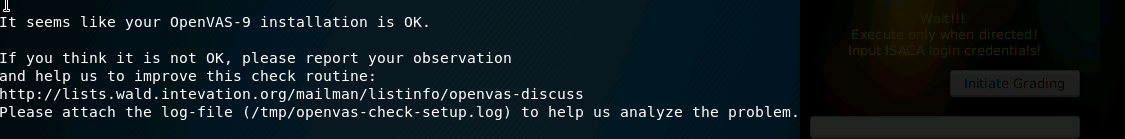


## 6.1 Detect Challenge

### 6.1.1 Starting Services

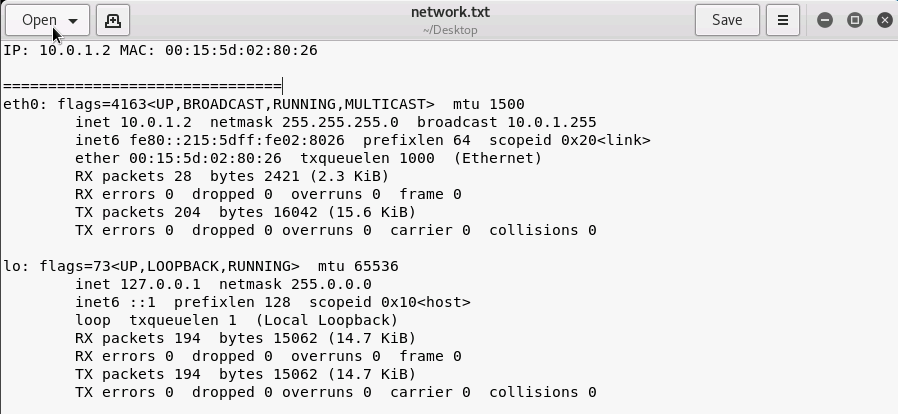
Log in to the Kali VM with the following credentials: username: **root** password: **isaca**. Start the challenge lab by running the OpenVAS essential services.





### 6.1.2 Creating a File

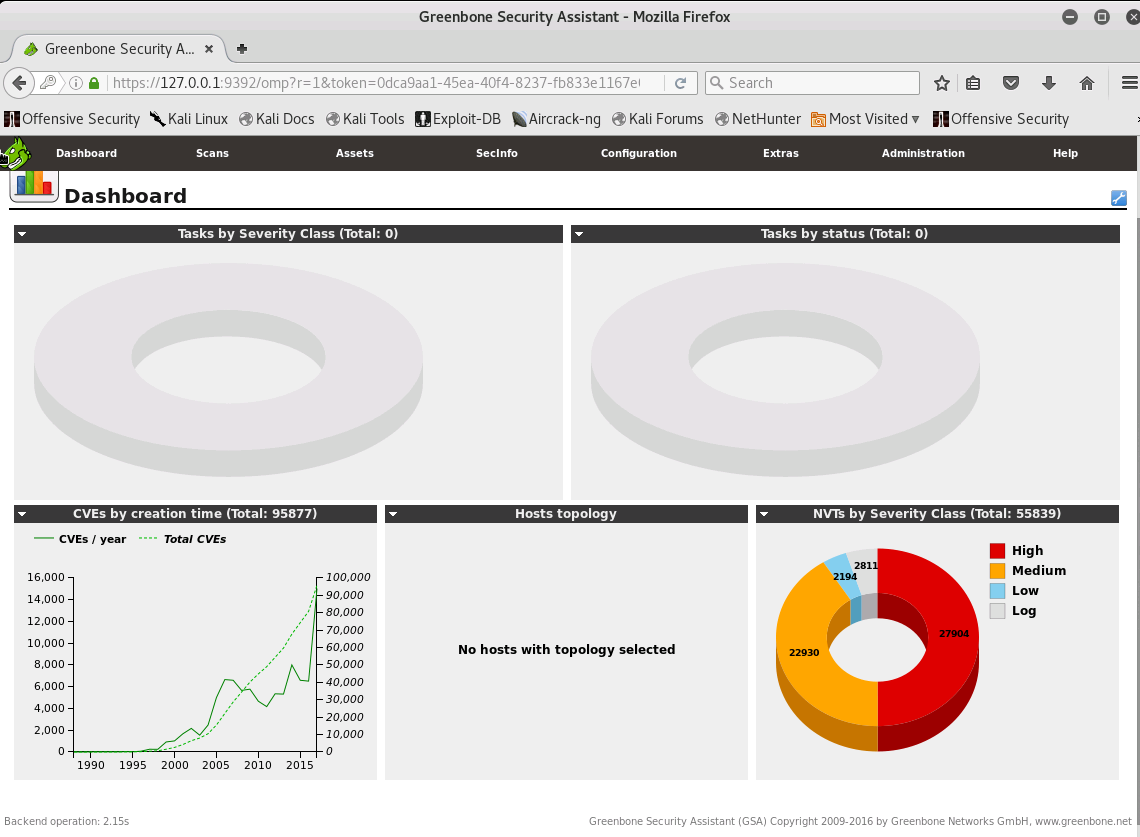
Open Leafpad and document your IP address and MAC address. Save the file as network.txt to your Desktop.



### 6.1.3 Opening the Web UI

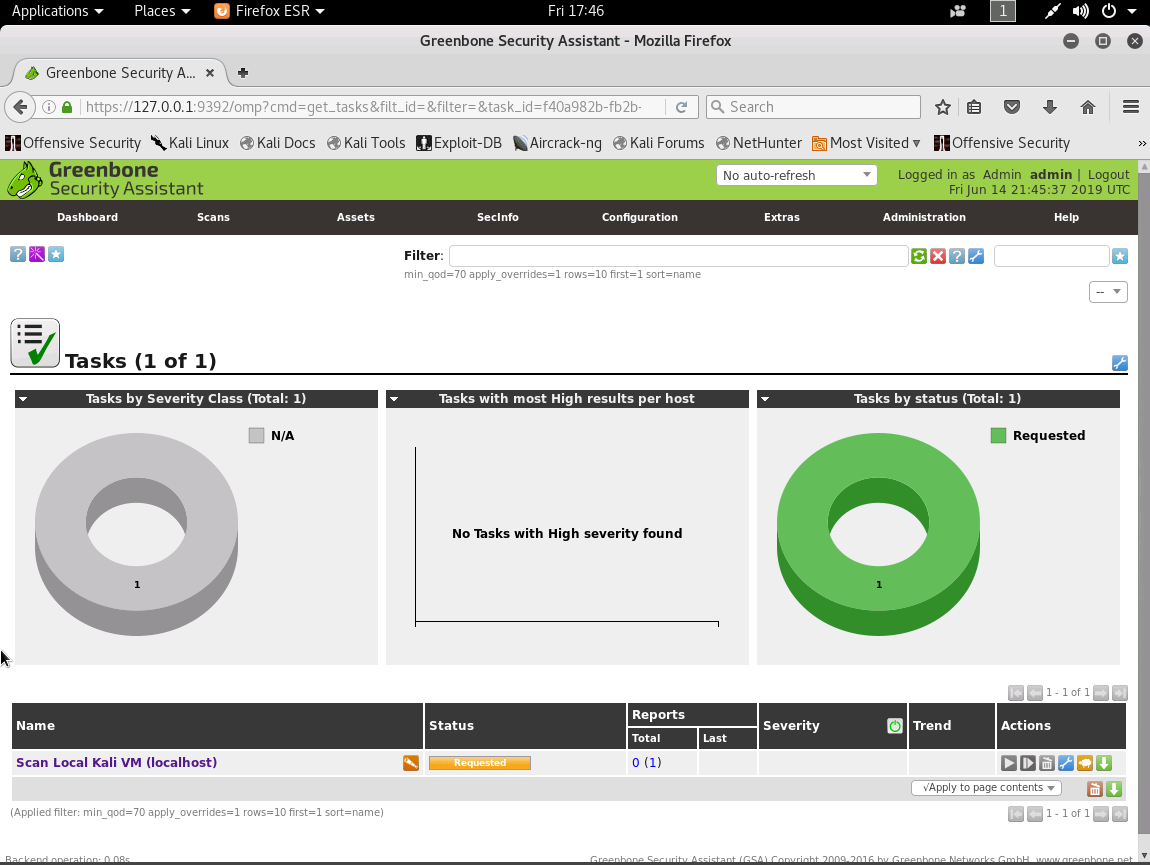
Navigate to the **Greenbone Security Assistant** at **https://127.0.0.1:9392** with the following credentials:

username: **admin** password: **admin**



### 6.1.4 Conducting a Scan

Scan the local Kali VM (localhost) for vulnerabilities. Export the scan to an XML document. Name the **scan.xml** and save it to the Desktop. Do not forget to lower the "**Maximum concurrently executed NVTs per hos**t" and "**... scanned hosts**" both to 1.



A screenshot of a cell phone

Description automatically generated

# 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