FAKULTI TEKNOLOGI
KEJURUTERAAN KELAUTAN
DAN INFORMATIK

2020/2021

CYBER SECURITY

Lab 6: Scanning Vulnerabilities

VERSION 1

`

Revision History

Revision Date	Previous Revision Date	Summary of Changes	Changes Marked
30/03/2021		First Issue	Fakhrul Adli Mohd Zaki Dr Farizah Yunus
21/5/2021		Update previous version of “Scanning Vulnerabilities”	

`

CONTENTS

`

INSTRUCTIONS

Manual makmal ini adalah untuk kegunaan pelajar-pelajar Fakulti Teknologi Kejuruteraan Kelautan dan Informatik (FTKKI), Universiti Malaysia Terengganu (UMT) sahaja. Tidak dibenarkan mencetak dan mengedar manual ini tanpa kebenaran rasmi daripada penulis.

Sila ikuti langkah demi langkah sebagaimana yang dinyatakan di dalam manual.

Arahan laporan makmal:

a) Pelajar perlu menyediakan laporan makmal untuk aktiviti makmal.
b) Kandungan laporan makmal mesti terdiri daripada beberapa tangkapan skrin untuk semua tetapan makmal keselamatan maya yang berjaya dengan beberapa penjelasan.
c) Jawab semua soalan refleksi untuk setiap sesi makmal.
d) Pelajar dapat memberikan senarai rujukan untuk rujukan tambahan.
e) Laporan makmal mesti dihantar dalam masa yang diberikan menggunakan pautan yang disediakan di platform eLearning.

This laboratory manual is for use by the students of the Faculty of Ocean Engineering Technology and Informatics, Universiti Malaysia Terengganu (UMT) only. It is not permissible to print and distribute this manual without the official authorisation of the author.

Please follow step by step as described in the manual.

Lab report instructions:

a) Students need to prepare lab report for lab activities.
b) The contents of the lab report must consist of several screenshots for all successful setting of the virtual security lab with some explanation.
c) Answer all the reflection questions for every lab sessions.
d) Student can provide the list of references for extra references.
e) The lab report must be submitted within the time given using the provided link in the eLearning platform.

`

TASK 1: RUNNING GREEN BONE SECURITY MANAGER (GSM)

OBJECTIVE

To download and run the commercial trial version of OpenVAS known as Green Bone Security Manager (GSM) virtual machine.

TASK DESCRIPTION

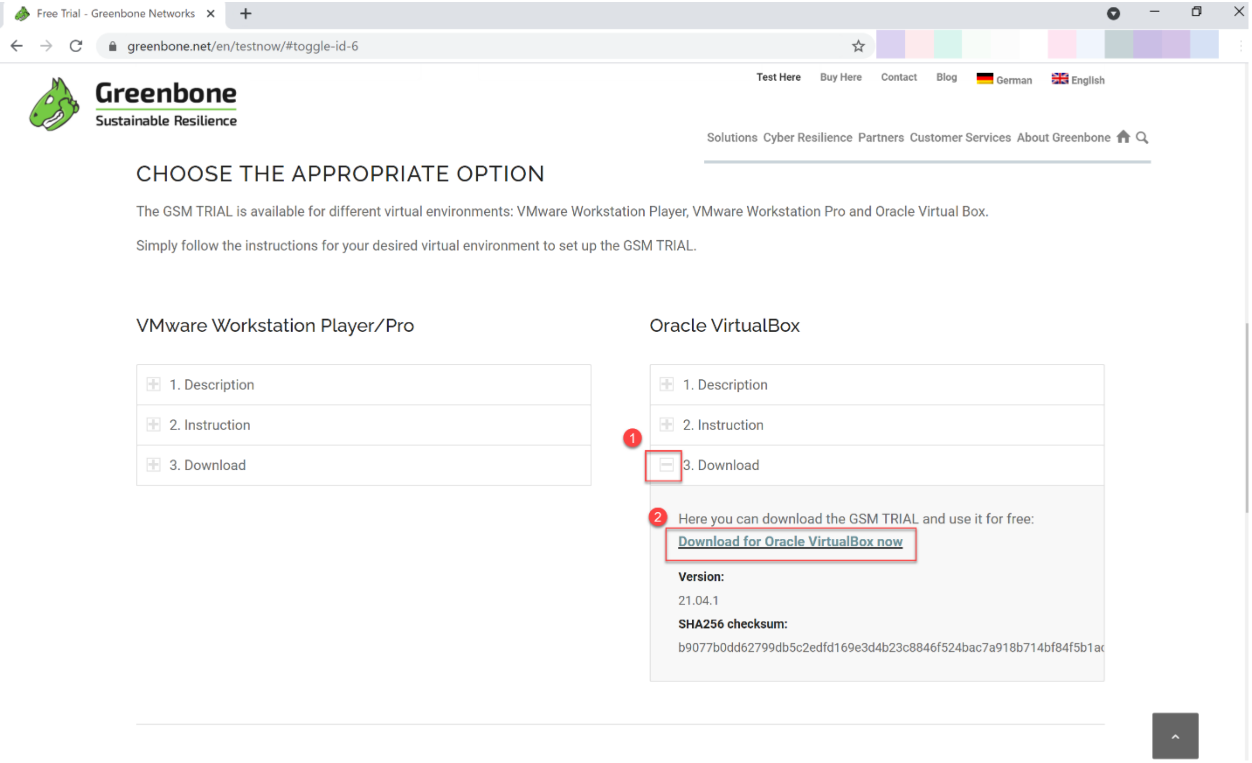
For this task, the student needs to download GSM virtual machine from the given link and run it on the Virtual Box. GSM later will be used to scan the vulnerabilities of the Metasploitable virtual machine.

ESTIMATED TIME

60 Minutes

STEPS:

1. Open a browser, then go to https://www.greenbone.net/en/testnow/#toggle-id-6
2. Download the GSM virtual machine file (.ova). Remember to keep the location of the file.



CHOOSE THE APPROPRIATE OPTION

The GSM TRIAL is available for different virtual environments: VMware Workstation Player, VMware Workstation Pro and Oracle Virtual Box.

Simply follow the instructions for your desired virtual environment to set up the GSM TRIAL.

VMware Workstation Player/Pro

- ⊞ 1. Description
- ⊞ 2. Instruction
- ⊞ 3. Download

Oracle VirtualBox

- ⊞ 1. Description
- ⊞ 2. Instruction
- ⊟ 3. Download

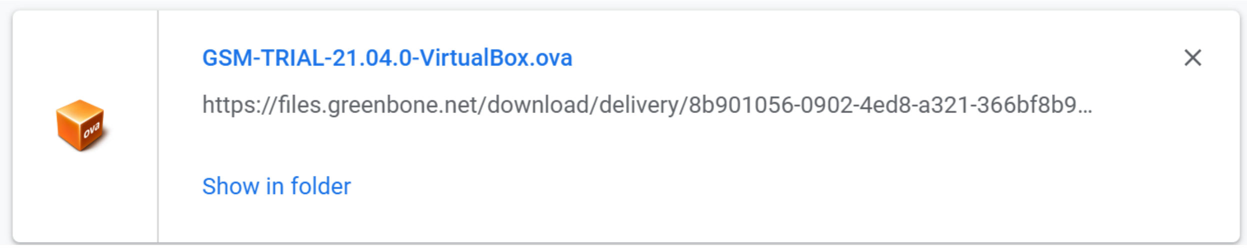
Here you can download the GSM TRIAL and use it for free:
Download for Oracle VirtualBox now

Version:
21.04.1

SHA256 checksum:
b9077b0dd62799db5c2edfd169e3d4b23c8846f524bac7a918b714bf84f5b1a

`

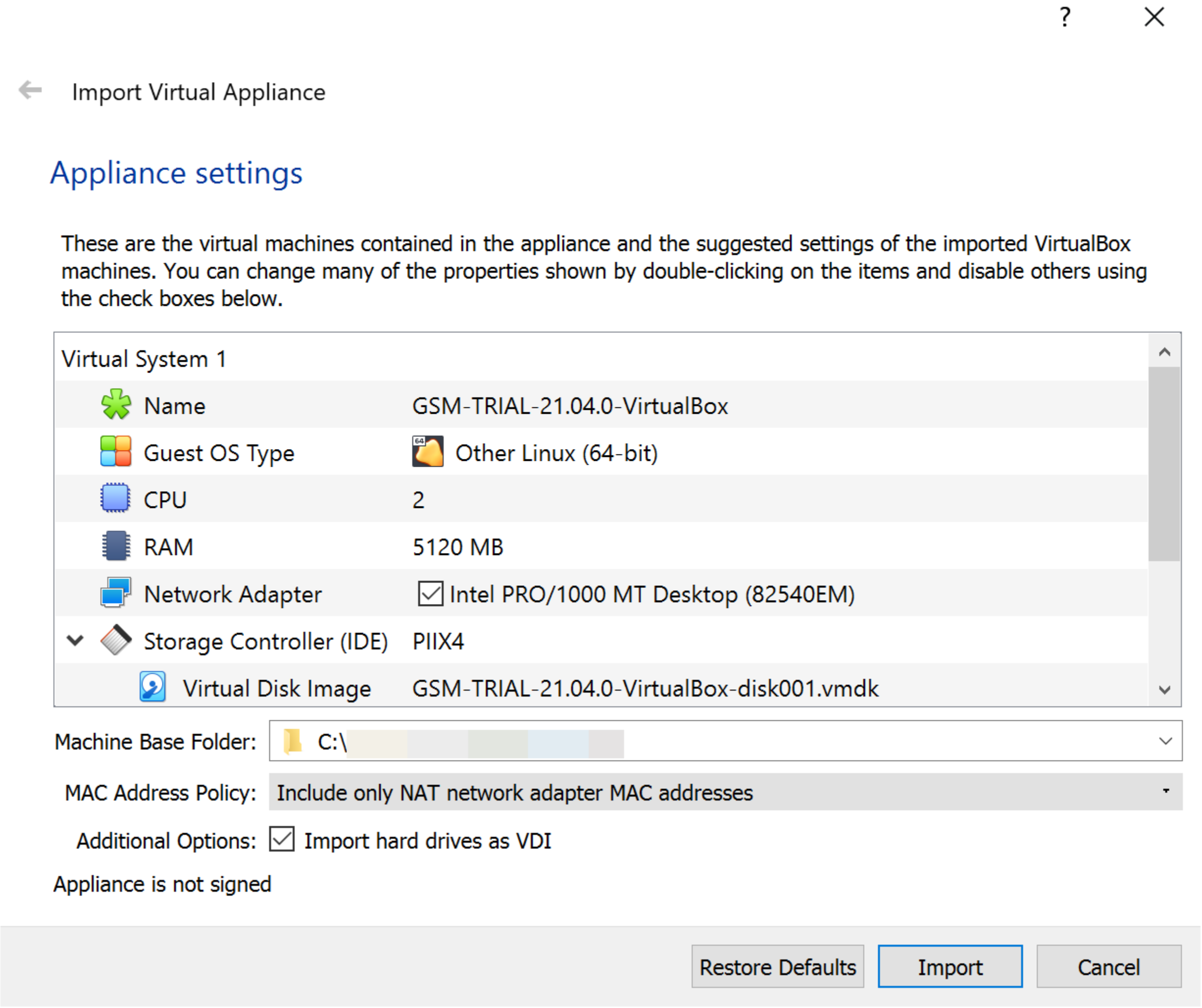
3. After the download complete, double-click on the icon of the file.



GSM-TRIAL-21.04.0-VirtualBox.ova

https://files.greenbone.net/download/delivery/8b901056-0902-4ed8-a321-366bf8b9...

4. You will see the appliance settings for the GSM virtual machine. Keep the configuration as it is and click **Import**.



Import Virtual Appliance

Appliance settings

These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.

Virtual System 1	
Name	GSM-TRIAL-21.04.0-VirtualBox
Guest OS Type	Other Linux (64-bit)
CPU	2
RAM	5120 MB
Network Adapter	☑ Intel PRO/1000 MT Desktop (82540EM)
Storage Controller (IDE)	PIIX4
Virtual Disk Image	GSM-TRIAL-21.04.0-VirtualBox-disk001.vmdk

Machine Base Folder: C:\ [redacted]

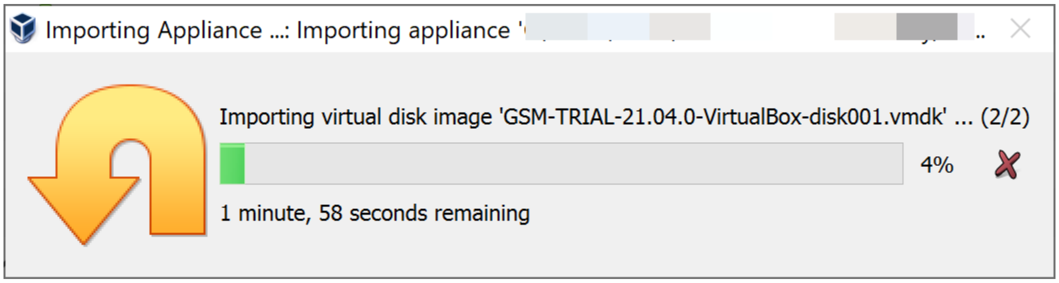
MAC Address Policy: Include only NAT network adapter MAC addresses

Additional Options: ☑ Import hard drives as VDI

Appliance is not signed

`

5. Wait until the importing appliance process finish.



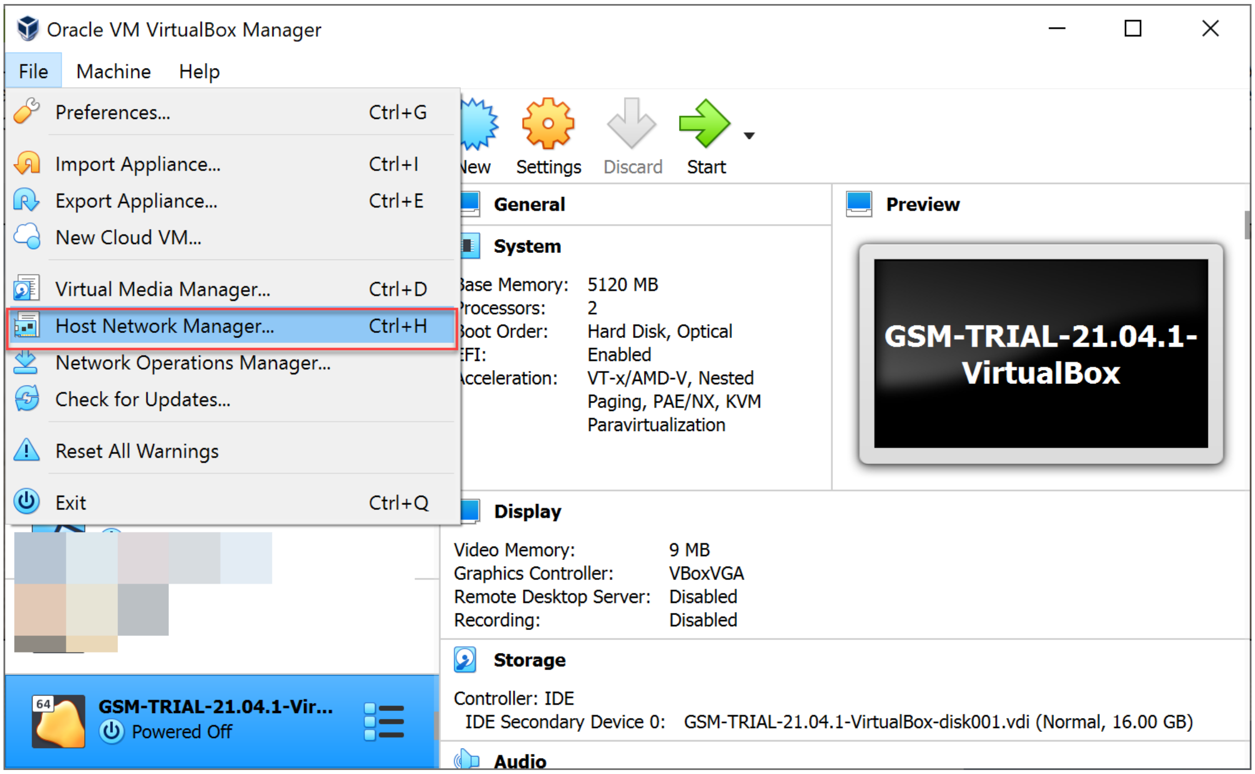
Importing Appliance ...: Importing appliance '

Importing virtual disk image 'GSM-TRIAL-21.04.0-VirtualBox-disk001.vmdk' ... (2/2)

4%

1 minute, 58 seconds remaining

6. After the GSM virtual machine successfully imported to Virtual Box, now we are going to set up the network for it. First of all, go to **File > Host Network Manager.**



Oracle VM VirtualBox Manager
File
Machine
Help
Preferences... Ctrl+G
Import Appliance... Ctrl+I
Export Appliance... Ctrl+E
New Cloud VM...
Virtual Media Manager... Ctrl+D
Host Network Manager... Ctrl+H
Network Operations Manager...
Check for Updates...
Reset All Warnings
Exit Ctrl+Q
New
Settings
Discard
Start
Preview
GSM-TRIAL-21.04.1-VirtualBox
64

GSM-TRIAL-21.04.1-Vir...
Powered Off

General

System

Base Memory: 5120 MB
Processors: 2
Boot Order: Hard Disk, Optical
EFI: Enabled
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization

Display

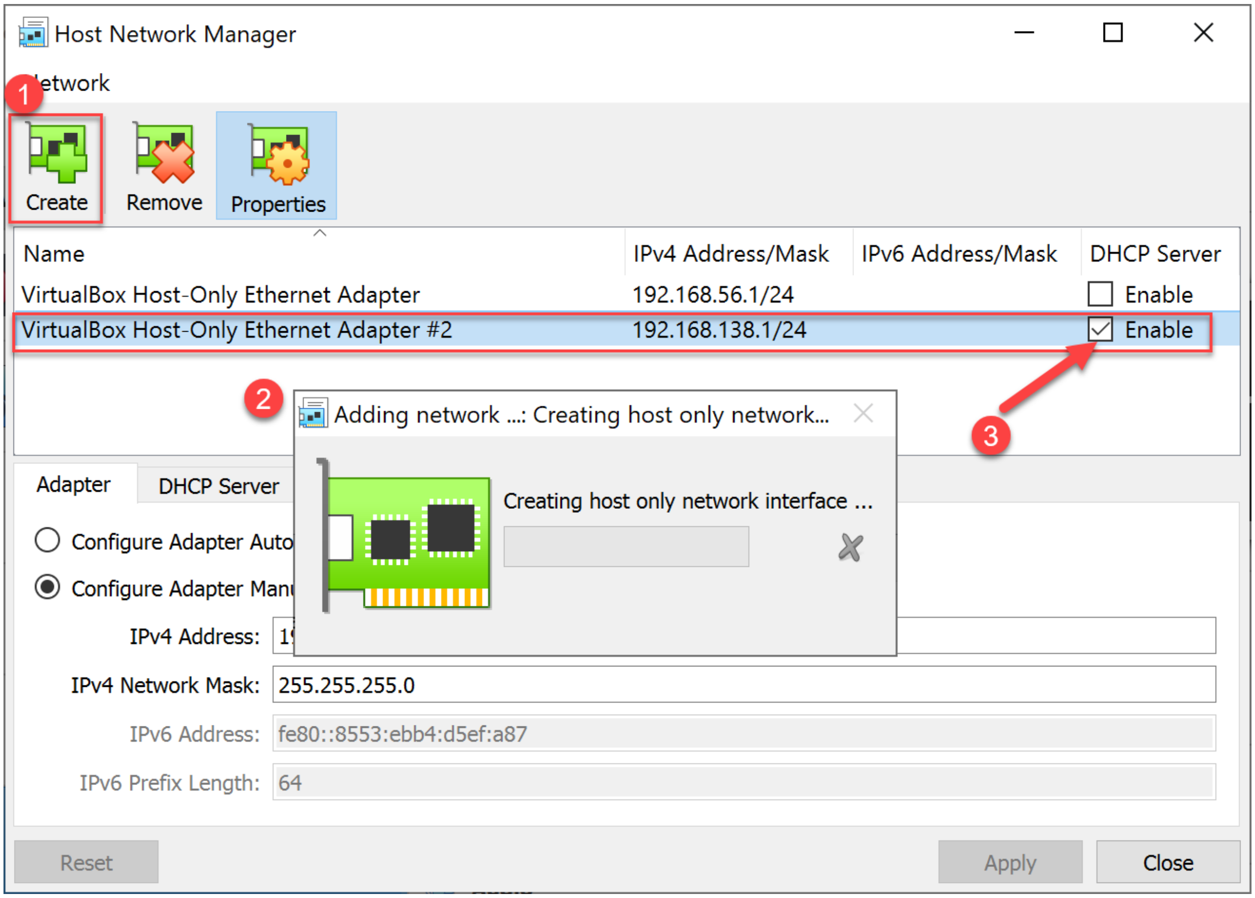
Video Memory: 9 MB
Graphics Controller: VBoxVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Device 0: GSM-TRIAL-21.04.1-VirtualBox-disk001.vdi (Normal, 16.00 GB)

Audio

7. We will use an internal network with DHCP for our GSM virtual machine. Follow the following steps to create a new network interface with DHCP server enabled. In this manual, the name of the interface is **VirtualBox Host-Only Ethernet Adapter #2**. However, in your case, it might be slightly different. Wait until the process finishes, then click **Close**.



Name	IPv4 Address/Mask	IPv6 Address/Mask	DHCP Server
VirtualBox Host-Only Ethernet Adapter	192.168.56.1/24		□ Enable
VirtualBox Host-Only Ethernet Adapter #2	192.168.138.1/24		☑ Enable

Adding network ...: Creating host only network...

Creating host only network interface ...

○ Configure Adapter Auto

● Configure Adapter Manu

IPv4 Address: 1

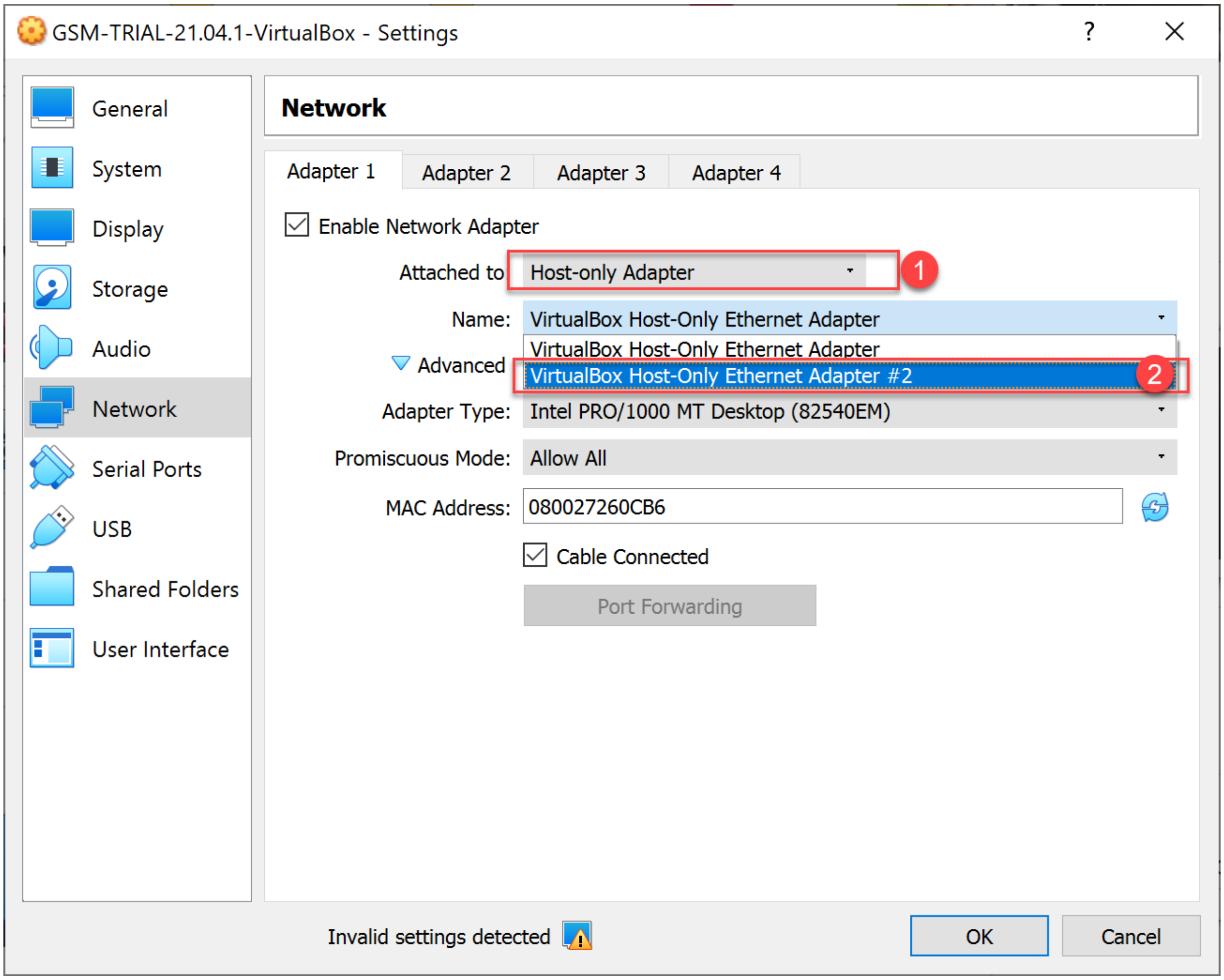
IPv4 Network Mask: 255.255.255.0

IPv6 Address: fe80::8553:ebb4:d5ef:a87

IPv6 Prefix Length: 64

`

8. Next, go back to the Virtual Box main screen. Select the **GSM-TRIAL-21.04.1** virtual machine, then go to its settings. This time, we are going to associate the network with the previously created interface. Follow the steps as shown in the screenshot below. Click **OK** after completed.



GSM-TRIAL-21.04.1-VirtualBox - Settings

Network

☑ Enable Network Adapter

Attached to: Host-only Adapter

Name: VirtualBox Host-Only Ethernet Adapter

VirtualBox Host-Only Ethernet Adapter

VirtualBox Host-Only Ethernet Adapter #2

▽ Advanced

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

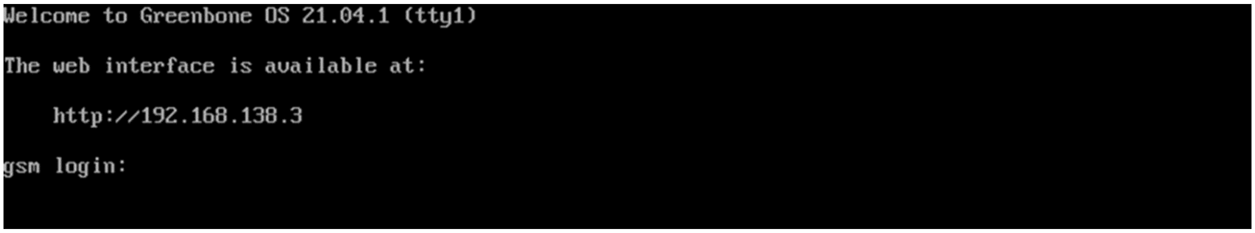
Promiscuous Mode: Allow All

MAC Address: 080027260CB6

☑ Cable Connected

Invalid settings detected ⚠

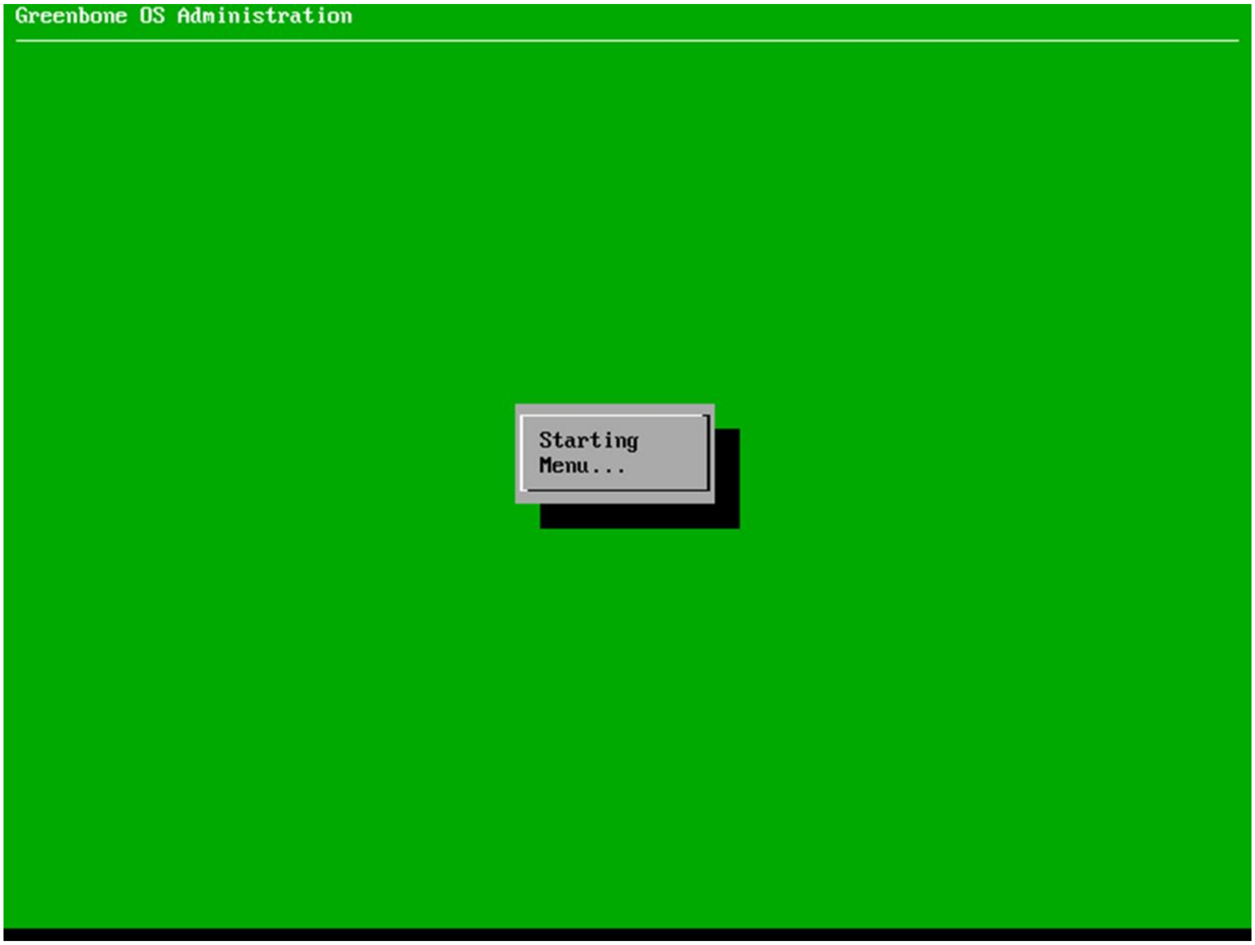
9. Start the GSM virtual machine and you will see a welcome screen similar to the following. However, the IP Address might be different because it is randomly assigned by the DHCP server in the Virtual Box that we have set up before. Log in to the console using **admin** as the username and password.



```
Welcome to Greenbone OS 21.04.1 (tty1)

The web interface is available at:

    http://192.168.138.3

gsm login:
```

`

10. This is the first screen of the GSM setup.

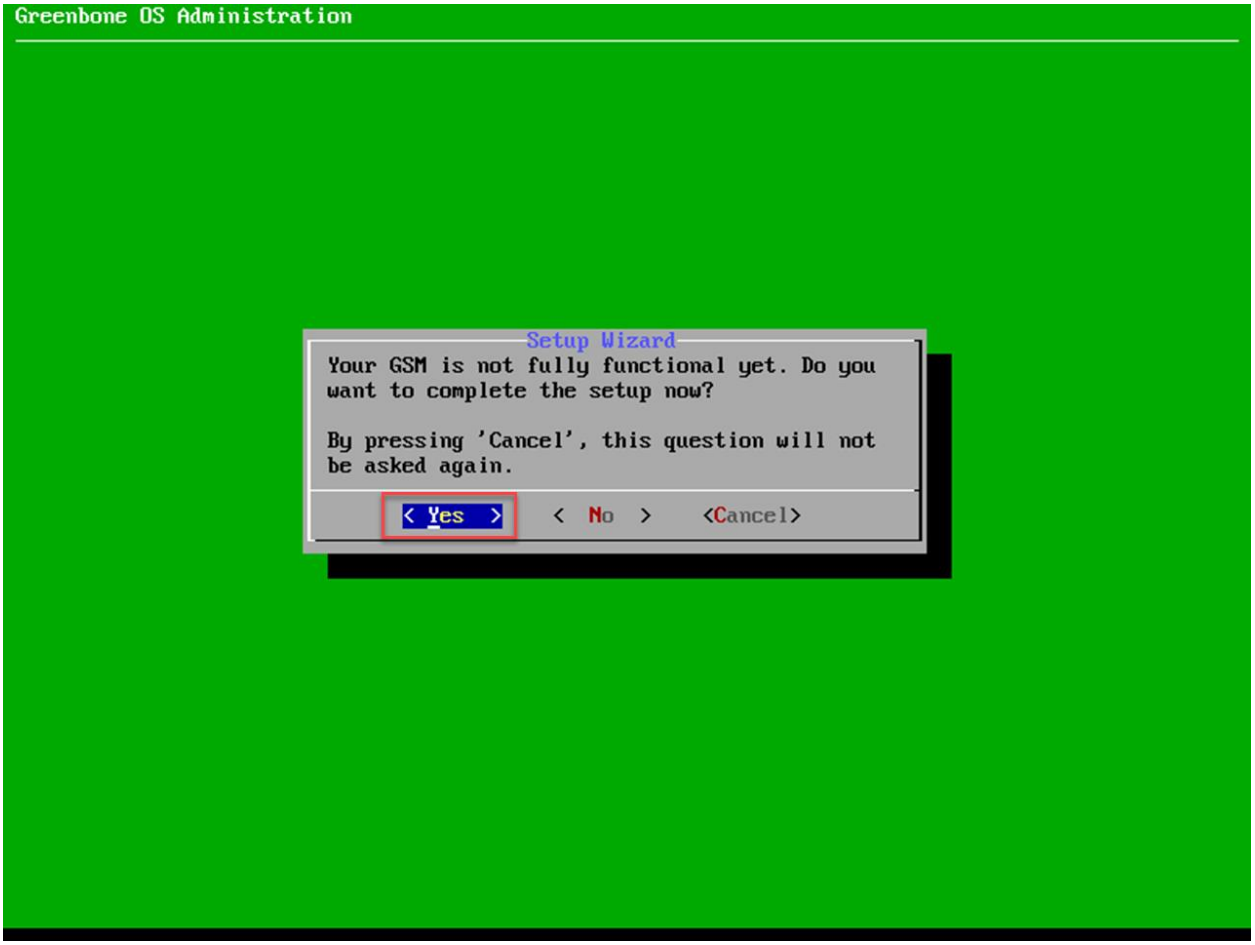


Greenbone OS Administration

Starting
Menu...

`

11. Select **Yes** then hit **Enter** to continue the setup.

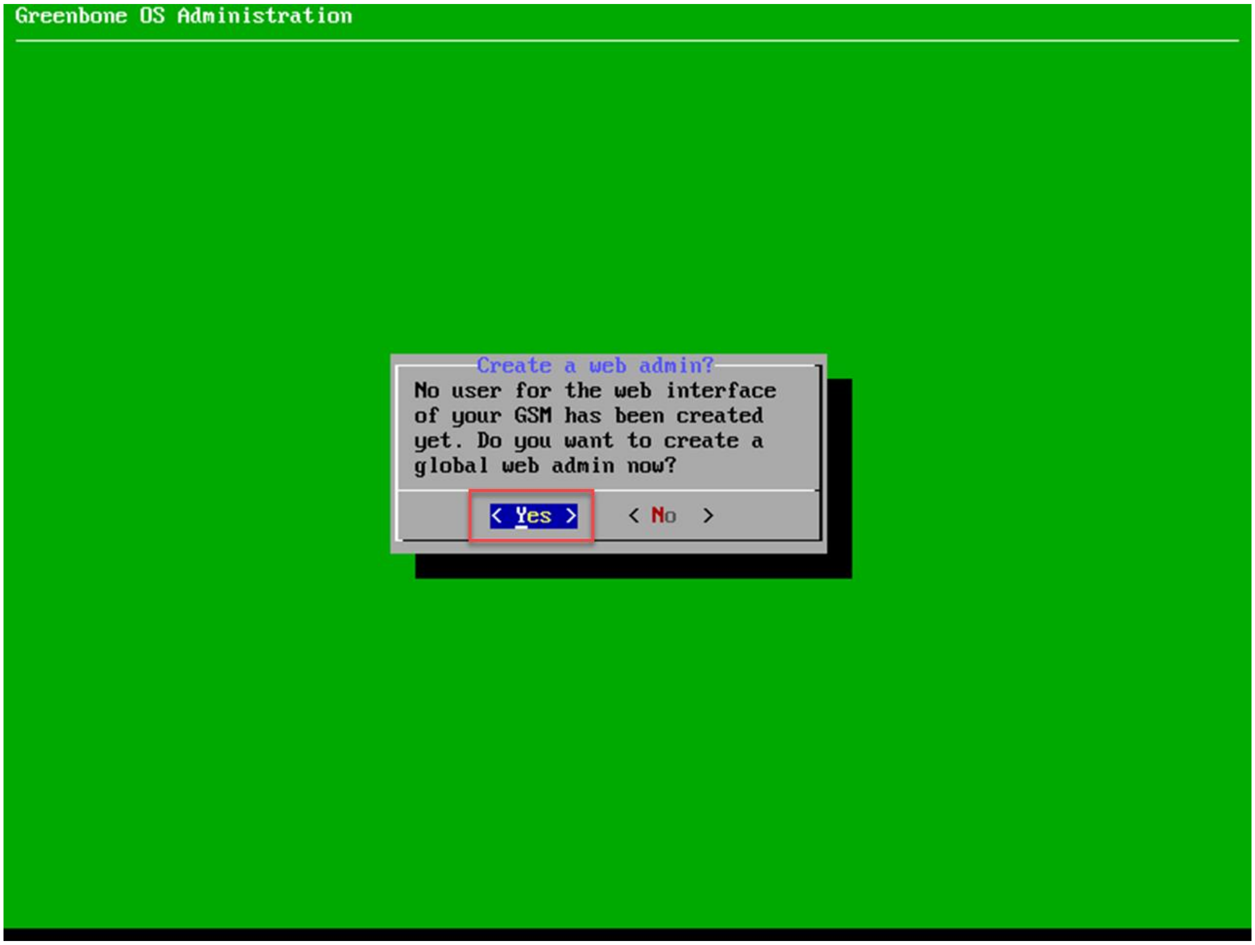


Your GSM is not fully functional yet. Do you want to complete the setup now?

By pressing 'Cancel', this question will not be asked again.

`

12. First, we are going to create a web admin. This account will be used for login from the web interface.



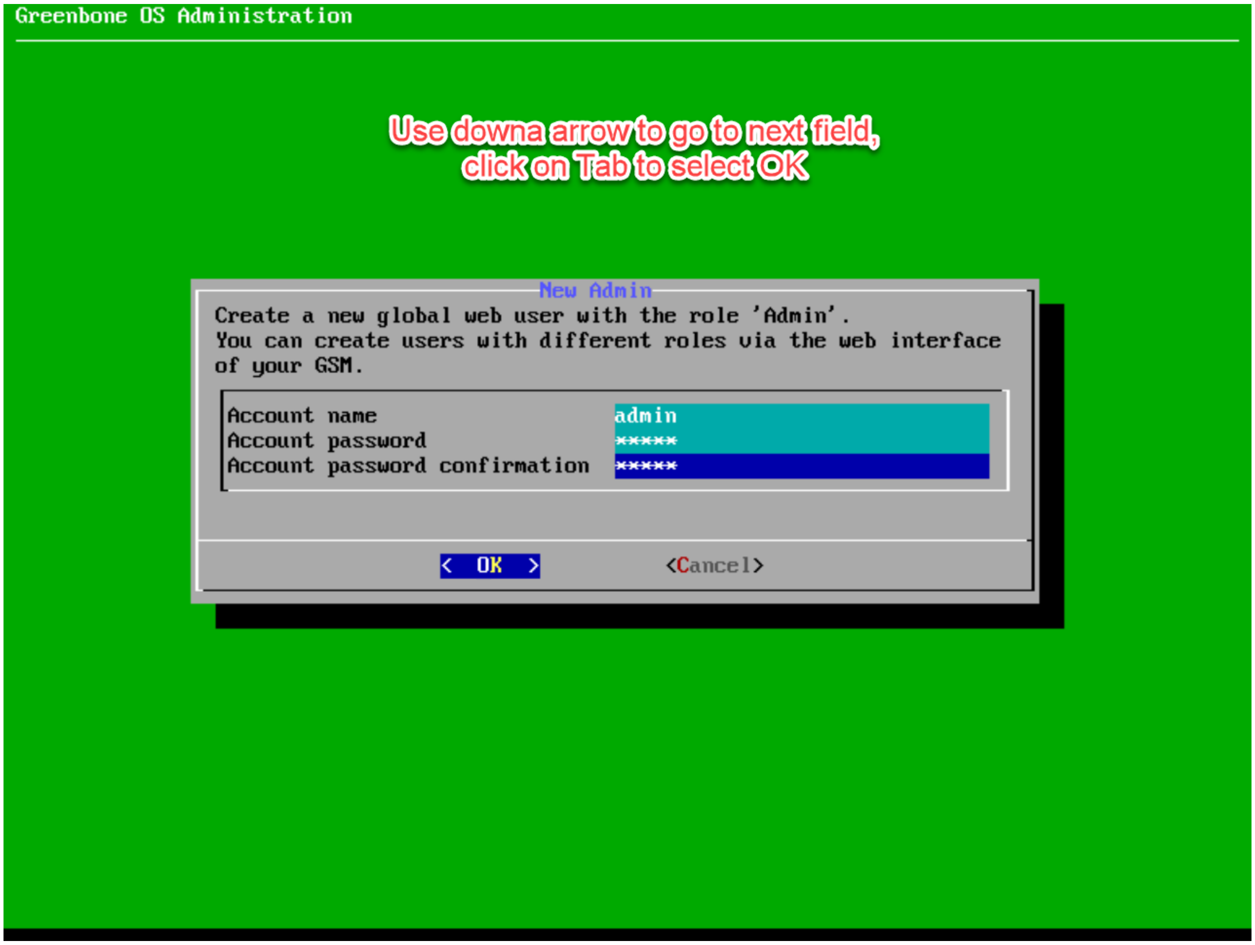
Greenbone OS Administration

Create a web admin?

No user for the web interface of your GSM has been created yet. Do you want to create a global web admin now?

`

13. Just for educational purposes, use **admin** as the account name and password. Select **OK**, and hit **Enter** after completed.



Greenbone OS Administration

Use downa arrow to go to next field, click on Tab to select OK

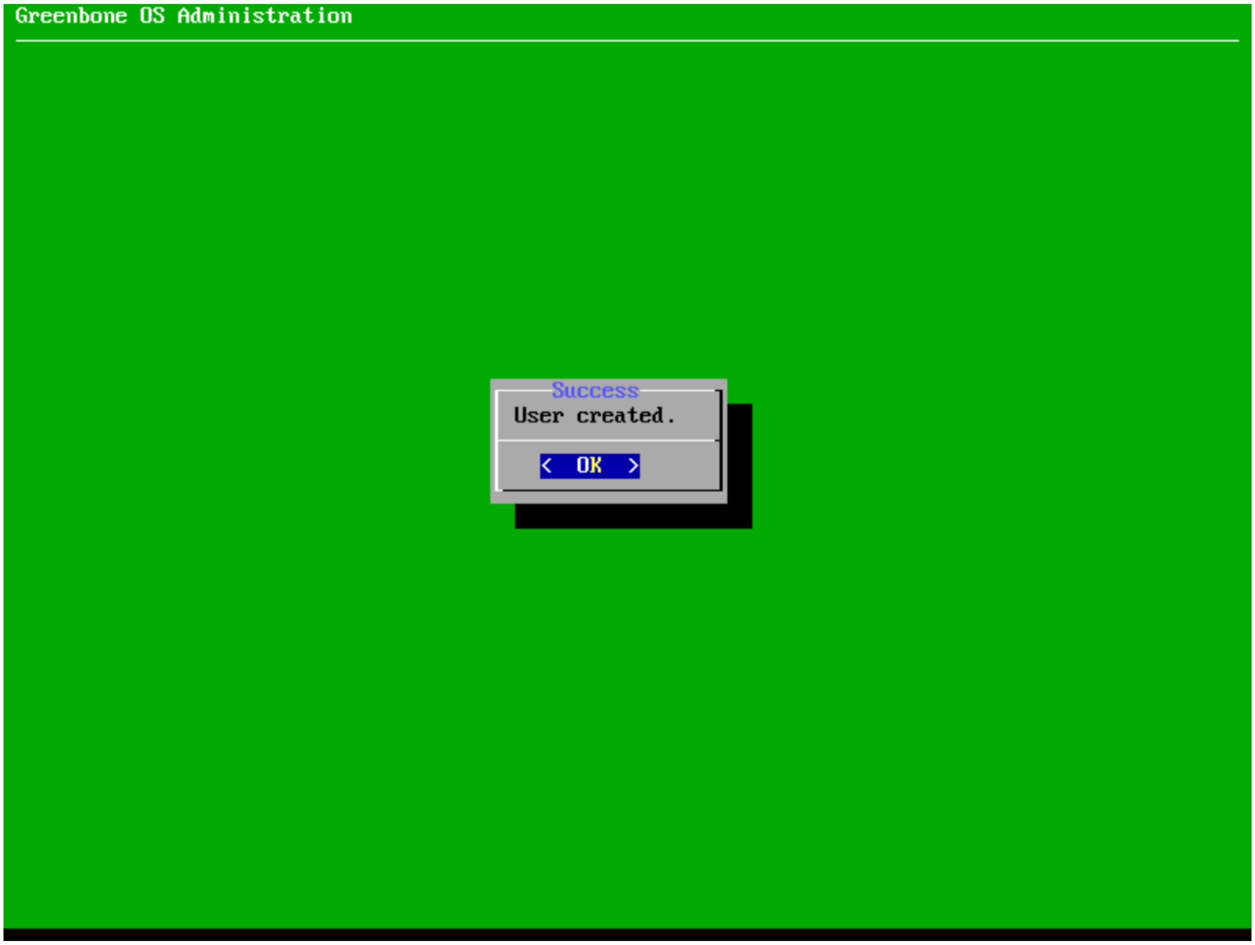
New Admin

Create a new global web user with the role 'Admin'.
You can create users with different roles via the web interface of your GSM.

```
Account name                     admin
Account password                 *****
Account password confirmation    *****
```

`

14. If successful, the window prompt below will be shown. Click **OK**.



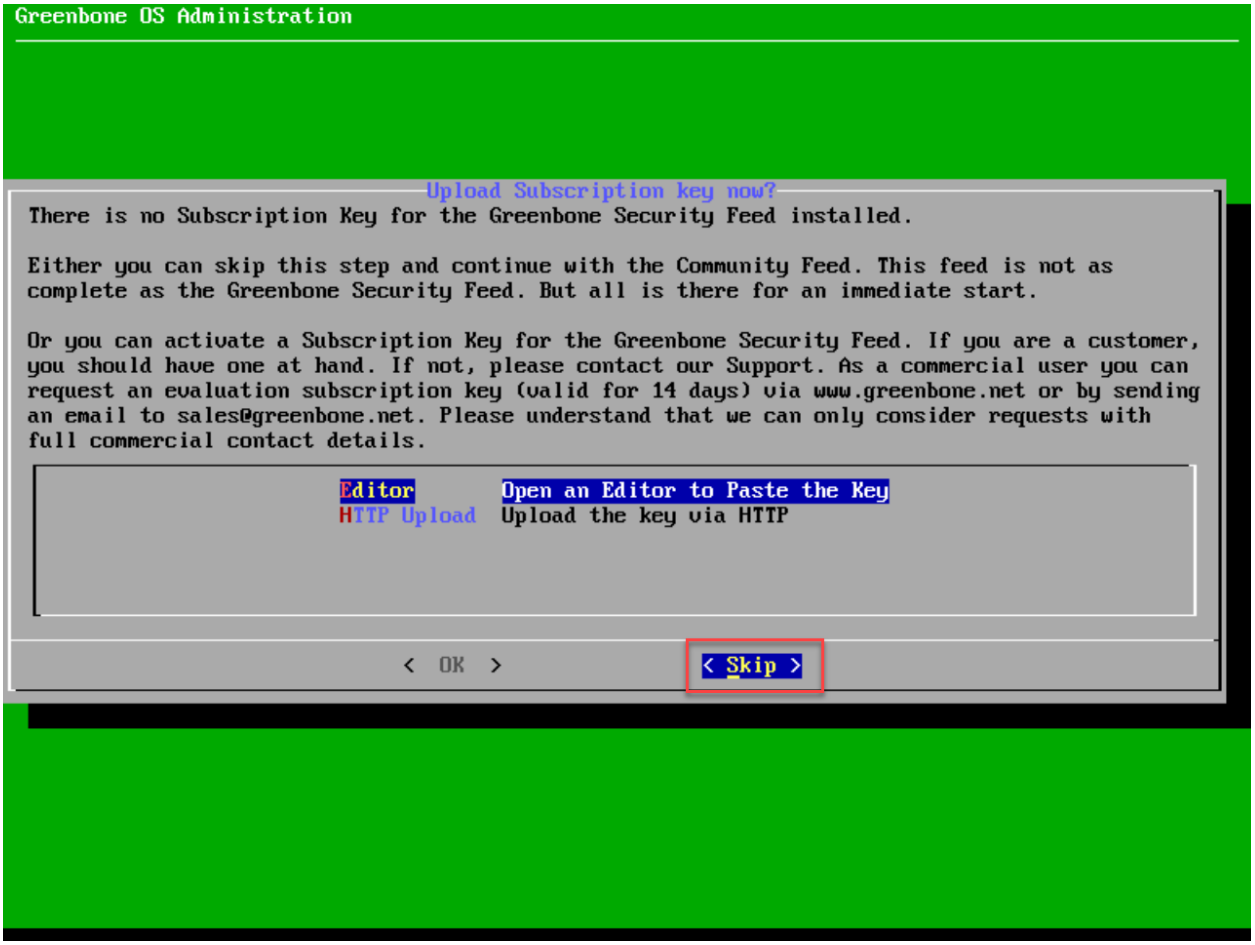
Greenbone OS Administration

Success

User created.

`

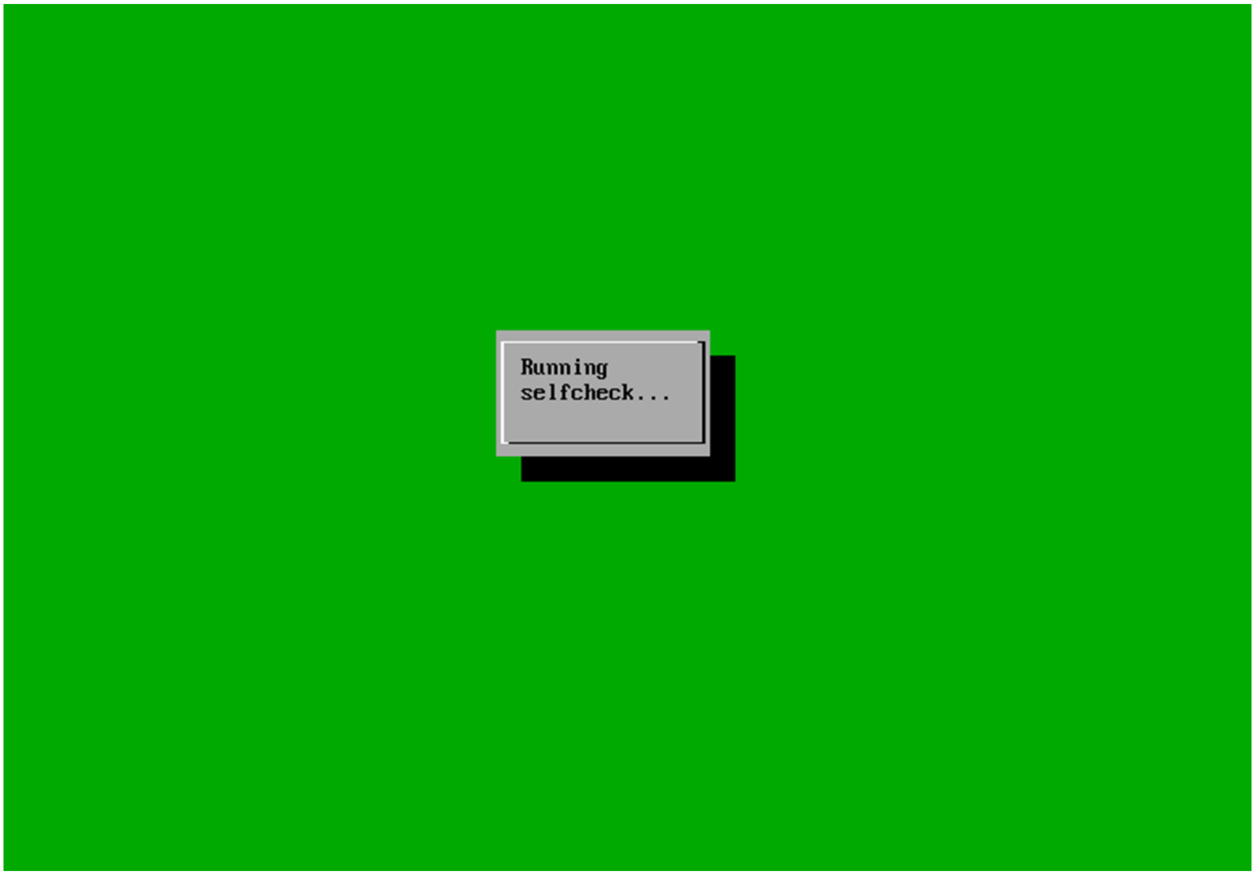
15. At this moment, we do not need to enter the subscription key, select **Skip** and hit **Enter**.



```
Greenbone OS Administration

Upload Subscription key now?
There is no Subscription Key for the Greenbone Security Feed installed.

Either you can skip this step and continue with the Community Feed. This feed is not as
complete as the Greenbone Security Feed. But all is there for an immediate start.

Or you can activate a Subscription Key for the Greenbone Security Feed. If you are a customer,
you should have one at hand. If not, please contact our Support. As a commercial user you can
request an evaluation subscription key (valid for 14 days) via www.greenbone.net or by sending
an email to sales@greenbone.net. Please understand that we can only consider requests with
full commercial contact details.

          Editor        Open an Editor to Paste the Key
          HTTP Upload   Upload the key via HTTP

              <  OK  >              < Skip >
```

`

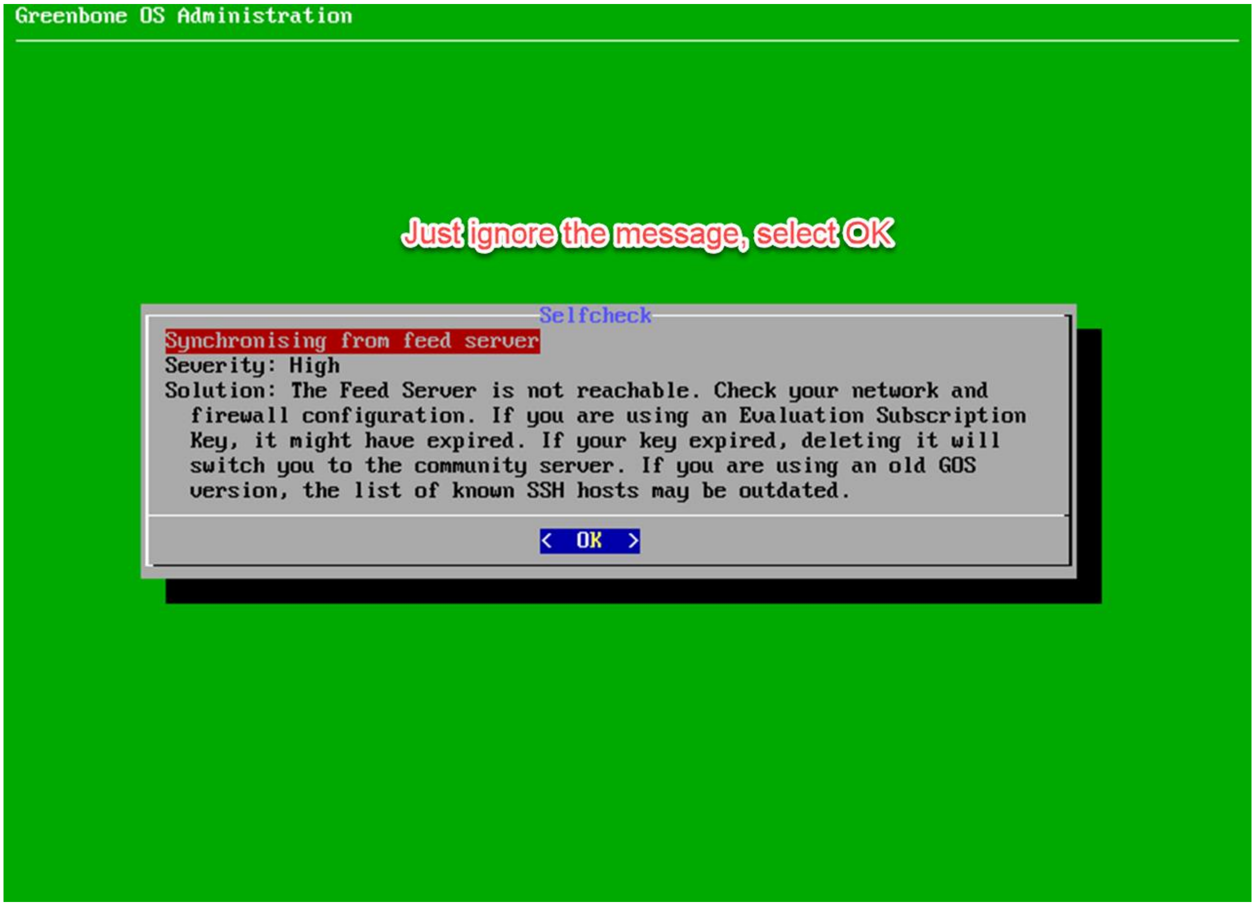
16. Now, the installer will run the self-check.



Running
selfcheck...

`

17. You might see a different screen than the one shown below. Just ignore the message by selecting **OK**.

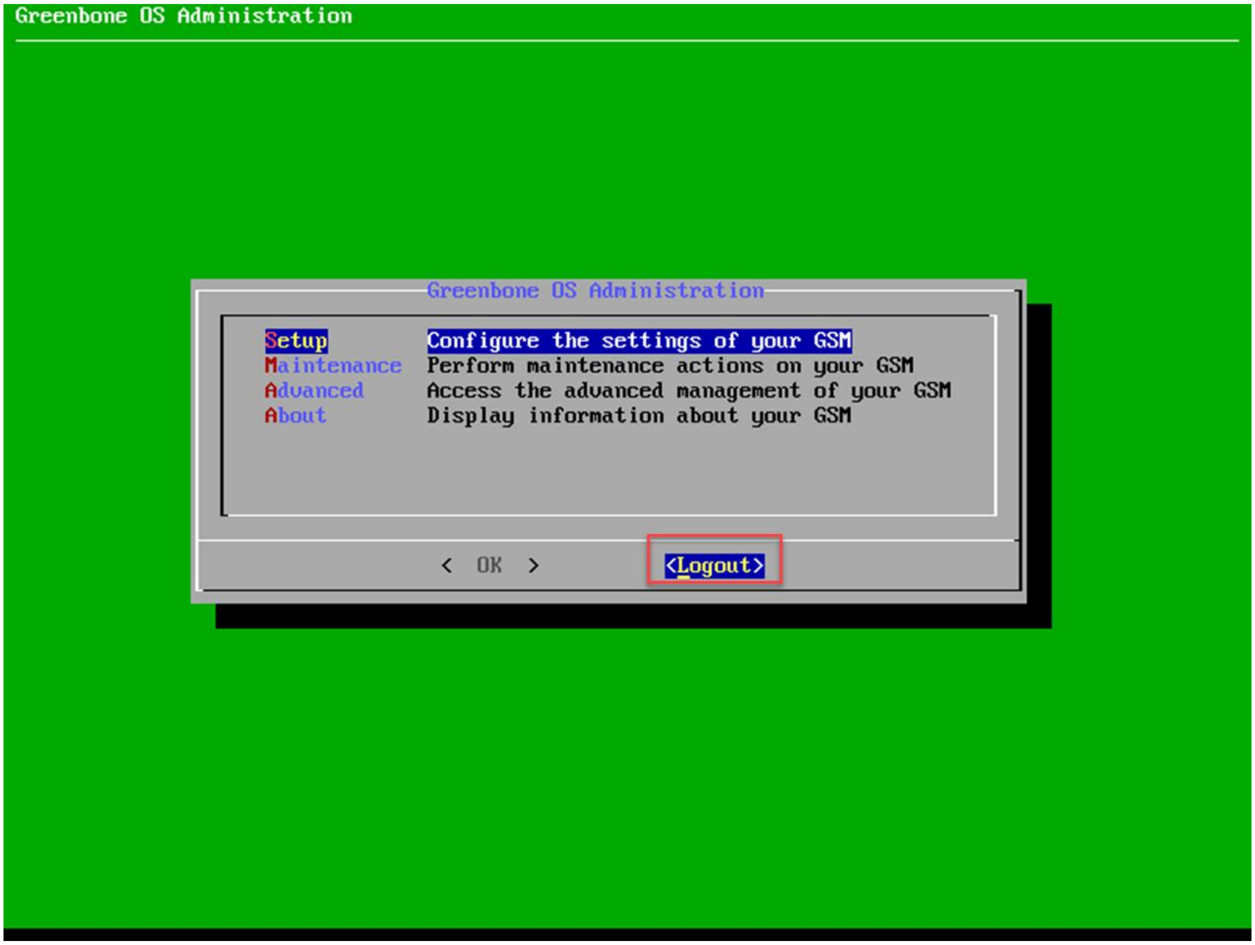


Just ignore the message, select OK

```
Selfcheck
Synchronising from feed server
Severity: High
Solution: The Feed Server is not reachable. Check your network and
  firewall configuration. If you are using an Evaluation Subscription
  Key, it might have expired. If your key expired, deleting it will
  switch you to the community server. If you are using an old GOS
  version, the list of known SSH hosts may be outdated.
```

`

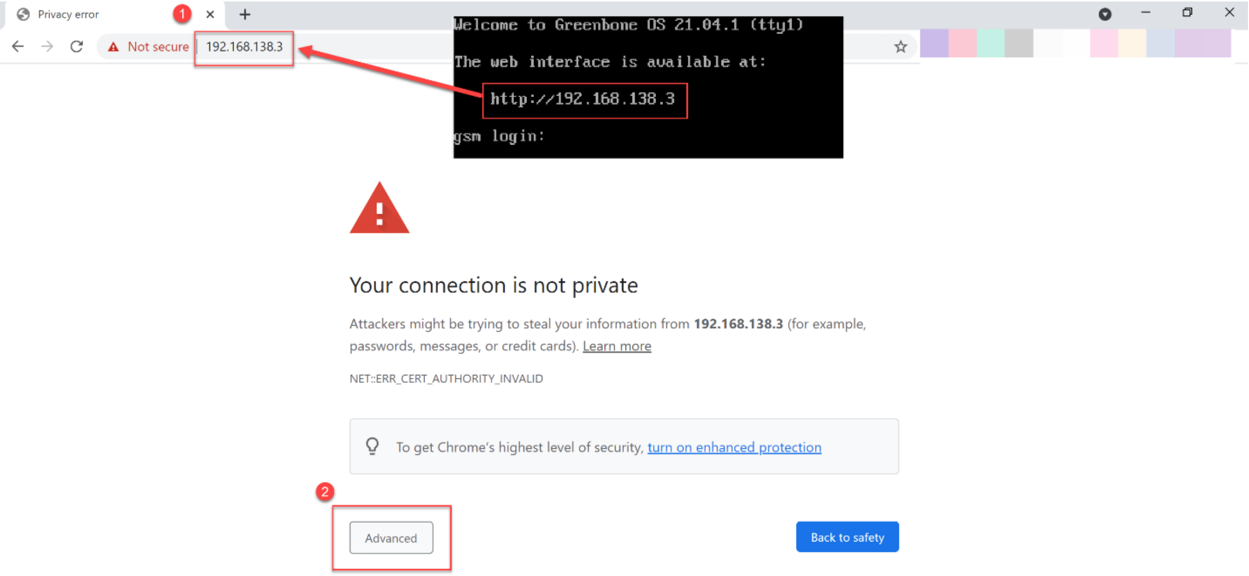
18. Everything looks good now and nothing more for the setup. Choose **Logout** and hit **Enter**.



```
Greenbone OS Administration

              Greenbone OS Administration
   Setup         Configure the settings of your GSM
   Maintenance   Perform maintenance actions on your GSM
   Advanced      Access the advanced management of your GSM
   About         Display information about your GSM

            <  OK  >          <Logout>
```

`

19. Now, let's access the web interface with the credentials we supplied during the setup before. Open a web browser, then type the IP address shown in the GSM virtual machine console. Click **Advanced** to skip the warning. This warning appears because we are not using a valid certificate. This is just for testing purposes and not to worry about it.



```
Welcome to Greenbone OS 21.04.1 (tty1)

The web interface is available at:

    http://192.168.138.3

gsm login:
```

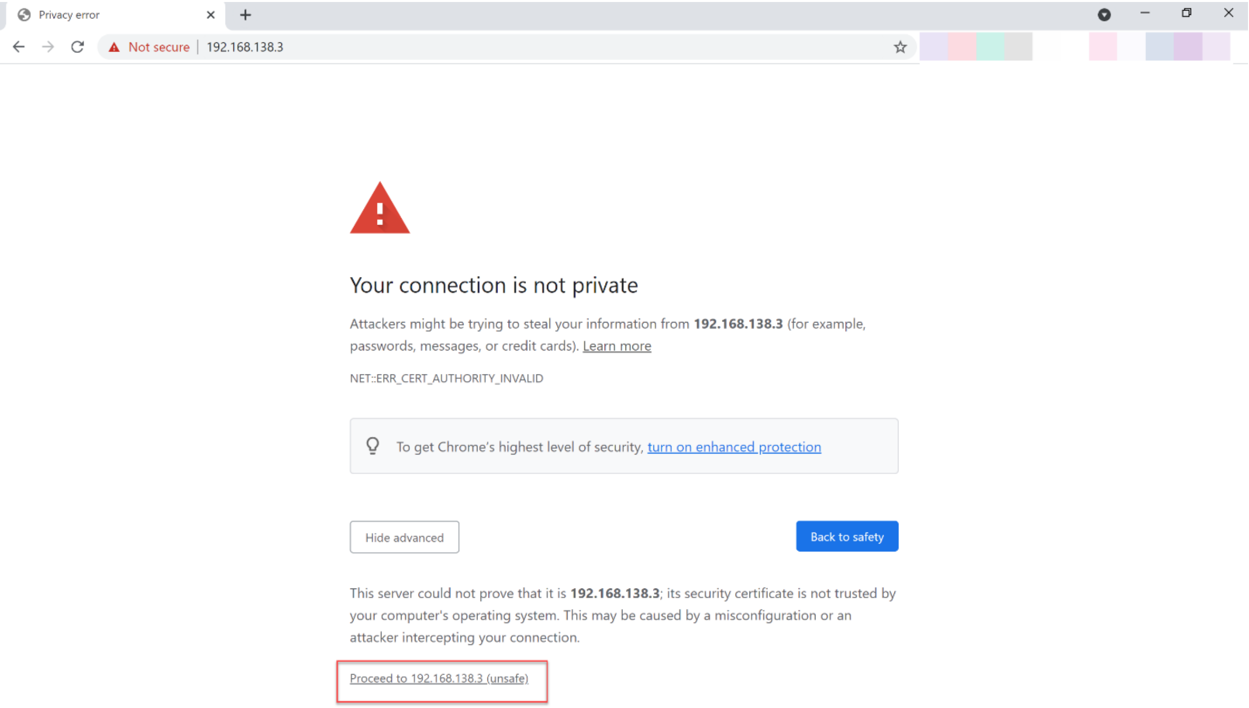
Your connection is not private

Attackers might be trying to steal your information from **192.168.138.3** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

To get Chrome's highest level of security, turn on enhanced protection

20. Click **Proceed to [IP Address]**.



Your connection is not private

Attackers might be trying to steal your information from **192.168.138.3** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

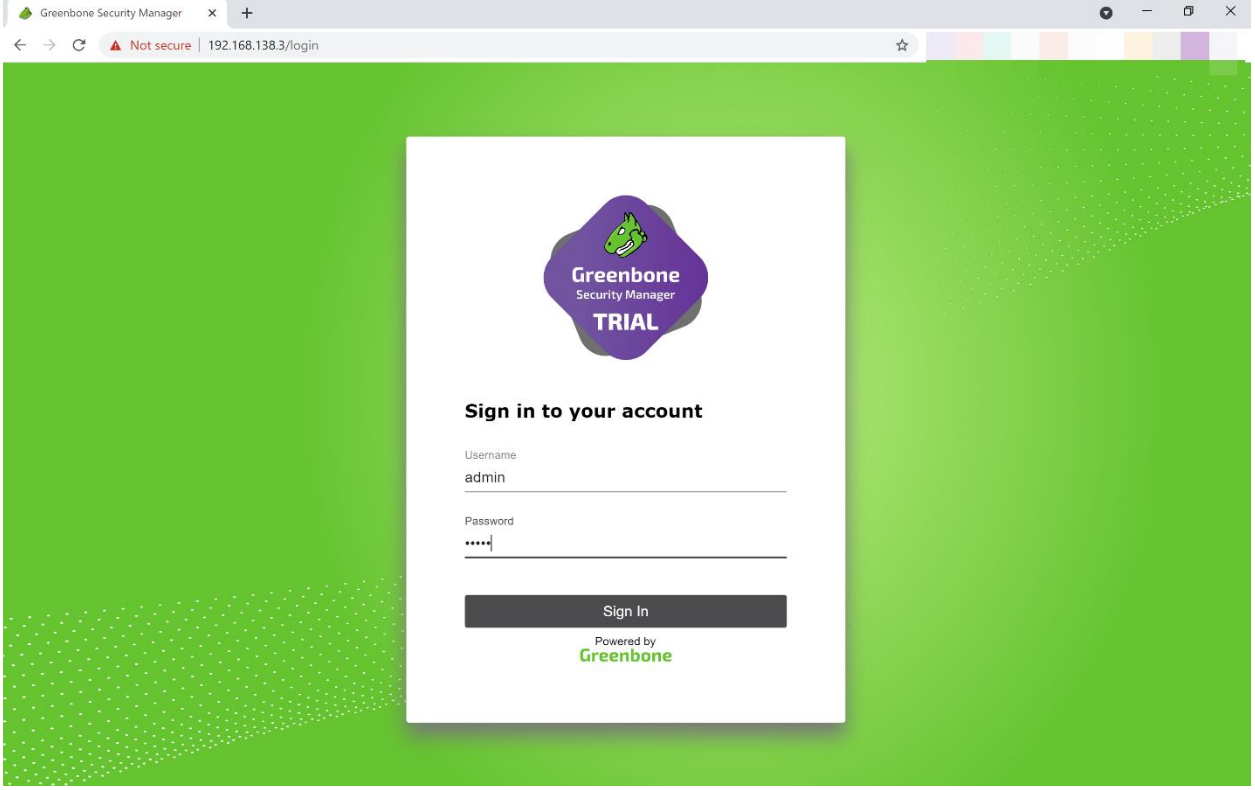
To get Chrome's highest level of security, turn on enhanced protection

This server could not prove that it is **192.168.138.3**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 192.168.138.3 (unsafe)

`

21. You will see the homepage of the GSM. Use **admin** as the username and password (we created these during the setup previously).



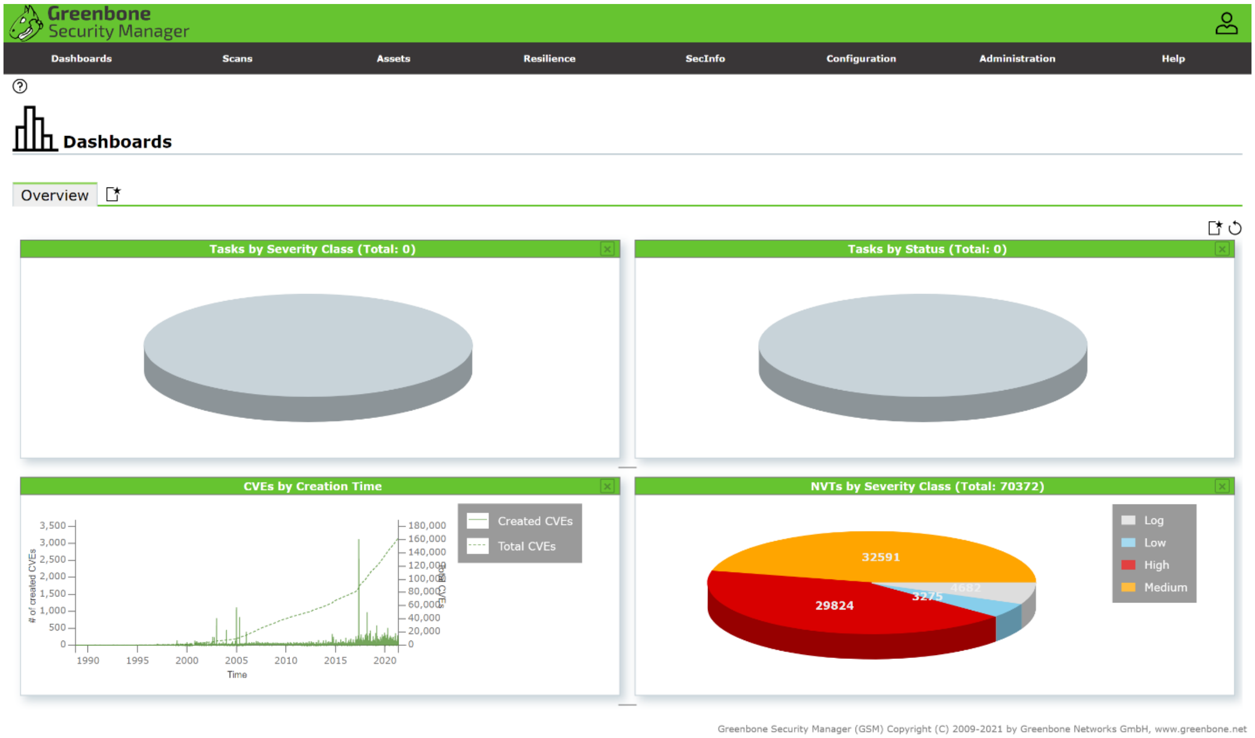
Sign in to your account

Username
admin

Password
•••••

`

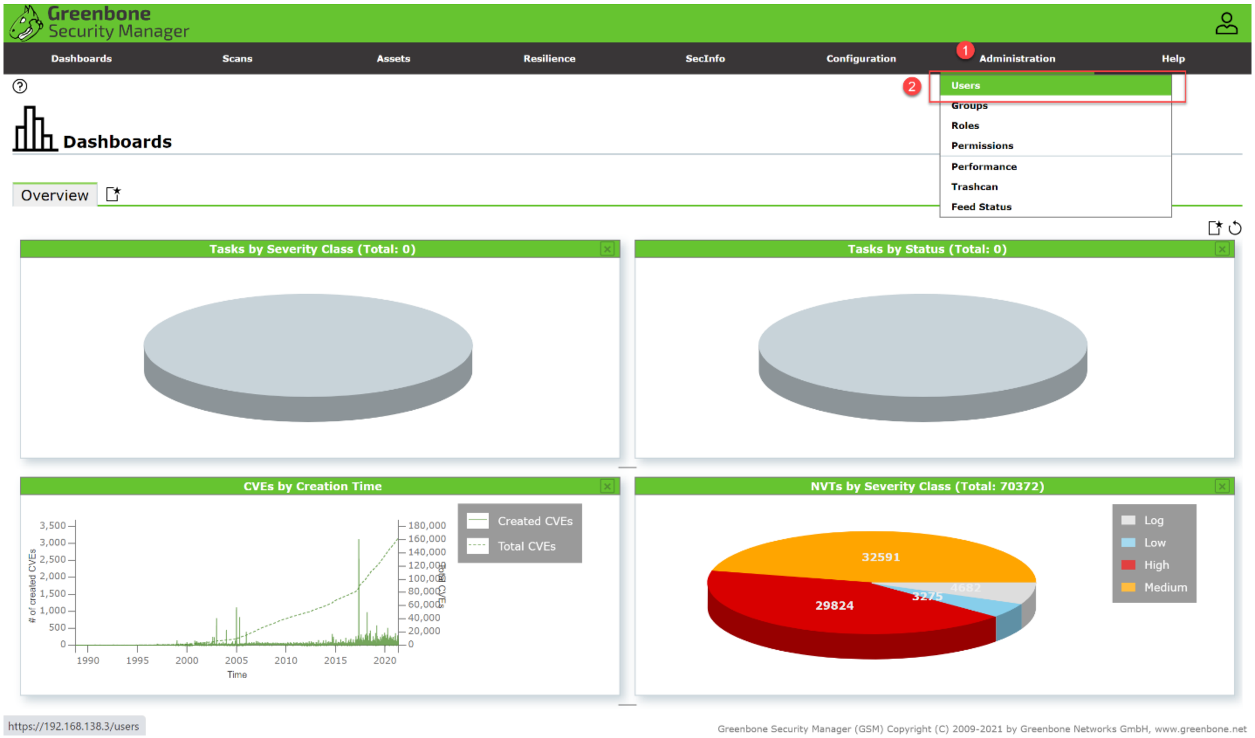
22. This is the dashboard that shows some important information. You can see bottom right a pie chart of Network Vulnerability Tests (NVTs) along with the severity such as Log, Low, High and Medium.



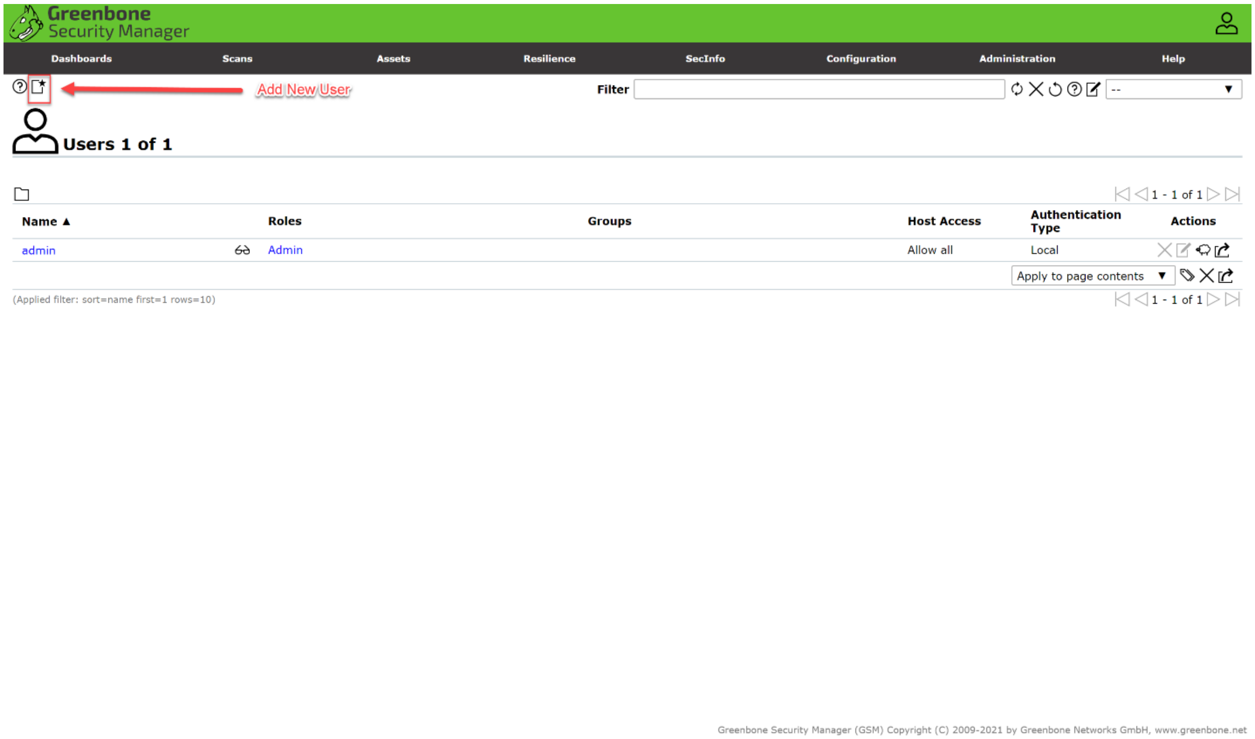
Greenbone Security Manager (GSM) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

`

23. Next, let us create a new user. In a real scenario, usually, we will work in a team. So that, we need to create a user and assign them with proper privileges. Choose **Administration** from the menu, then choose **Users**.



24. On the following page, click on the icon to add a new user.



Name ▲	Roles	Groups	Host Access	Authentication Type	Actions
admin	Admin		Allow all	Local	

Apply to page contents ▼

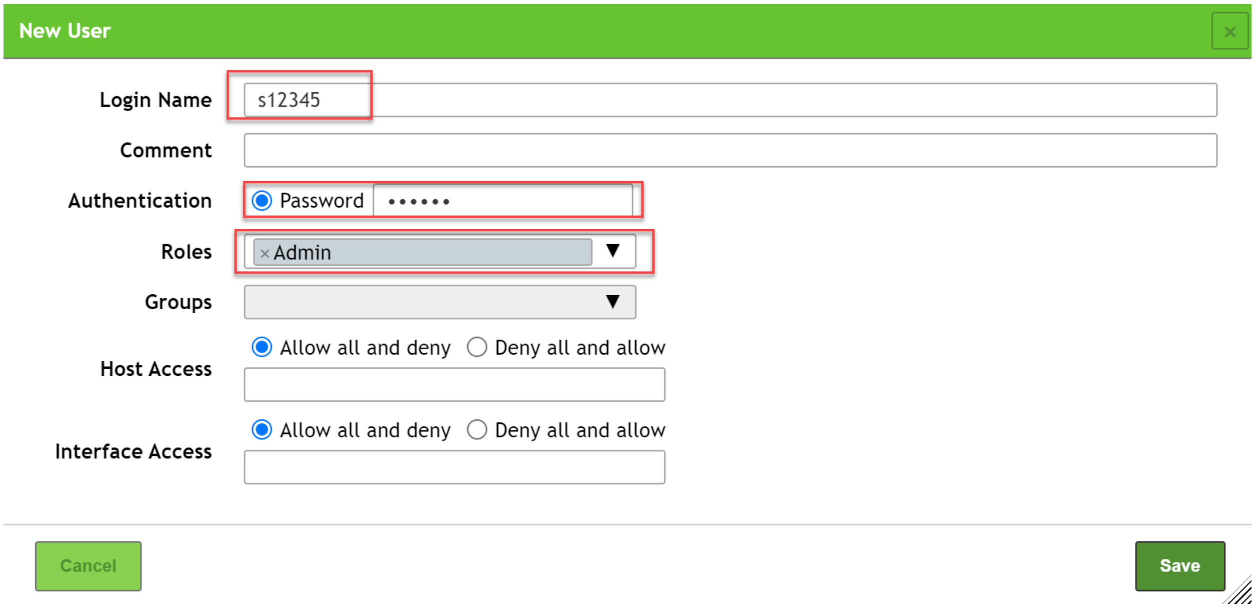
(Applied filter: sort=name first=1 rows=10)

1 - 1 of 1

Greenbone Security Manager (GSM) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

`

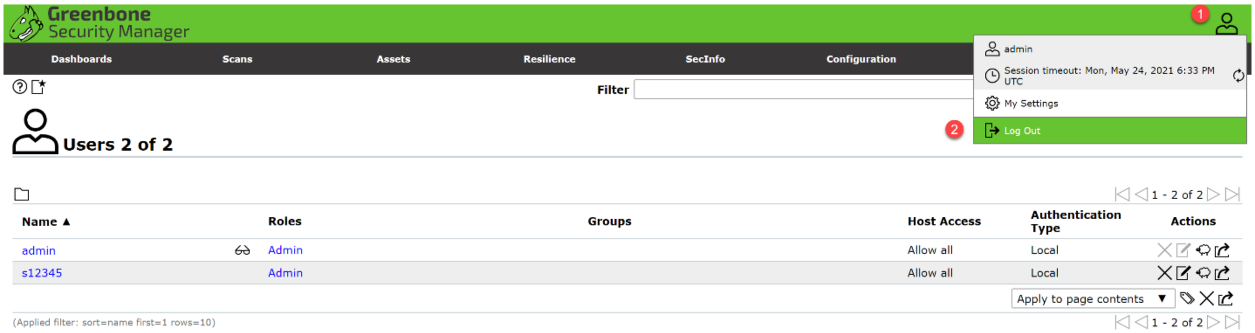
25. Fill in the form by replacing the Login name and password with your matric number. Take a screenshot of this activity and put it into your lab report.



New User

Login Name	s12345
Comment	
Authentication	● Password ••••••
Roles	× Admin ▼
Groups	▼
Host Access	● Allow all and deny ○ Deny all and allow
Interface Access	● Allow all and deny ○ Deny all and allow

26. If everything good, then you will see the new user in the list. Log out from the system after completed.



Users 2 of 2

1 - 2 of 2

Name ▲	Roles	Groups	Host Access	Authentication Type	Actions
admin	Admin		Allow all	Local	
s12345	Admin		Allow all	Local	

Apply to page contents ▼

(Applied filter: sort=name first=1 rows=10)

1 - 2 of 2

Greenbone Security Manager (GSM) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

`

TASK 2: SETTING UP THE NETWORK FOR METASPLOITABLE

OBJECTIVE

To set up the network for Metasploitable virtual machine.

TASK DESCRIPTION

For this task, the student needs to set up the Host-only Adapter for the Metasploitable virtual machine. This setup will allow the GSM to scan the latter for its vulnerabilities.

ESTIMATED TIME

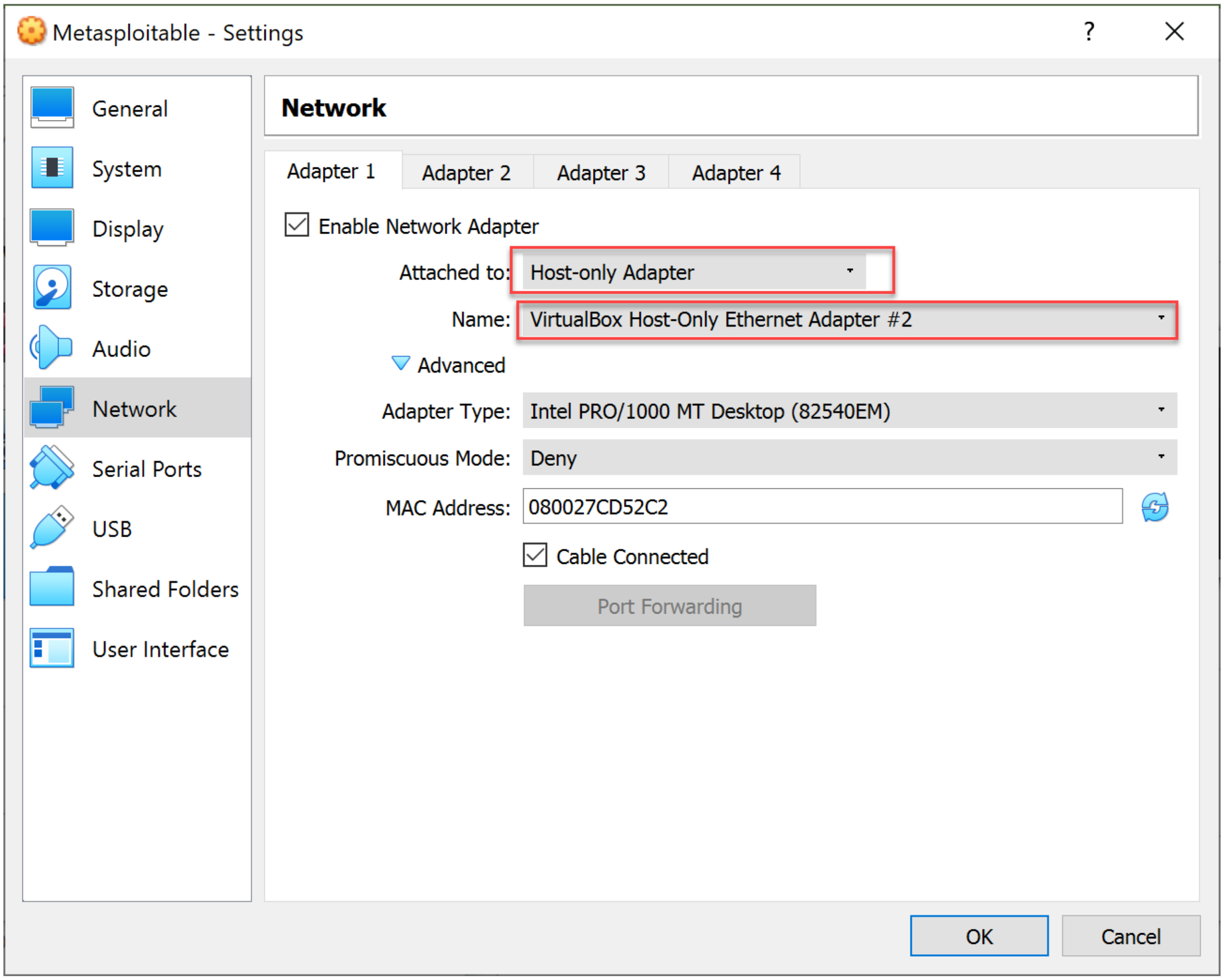
15 Minutes

STEPS:

1. Select the Metasploitable virtual machine from the menu of Virtual Box. Then, go to its settings.

`

2. Choose Network from the menu on the left. Select **Host-only Adapter** and from the Name: dropdown, choose the same interface that has been chosen for GSM virtual machine before (refer to Step 8 in Task 1). Click **OK** after the finish.



Network

☑ Enable Network Adapter

Attached to: Host-only Adapter

Name: VirtualBox Host-Only Ethernet Adapter #2

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

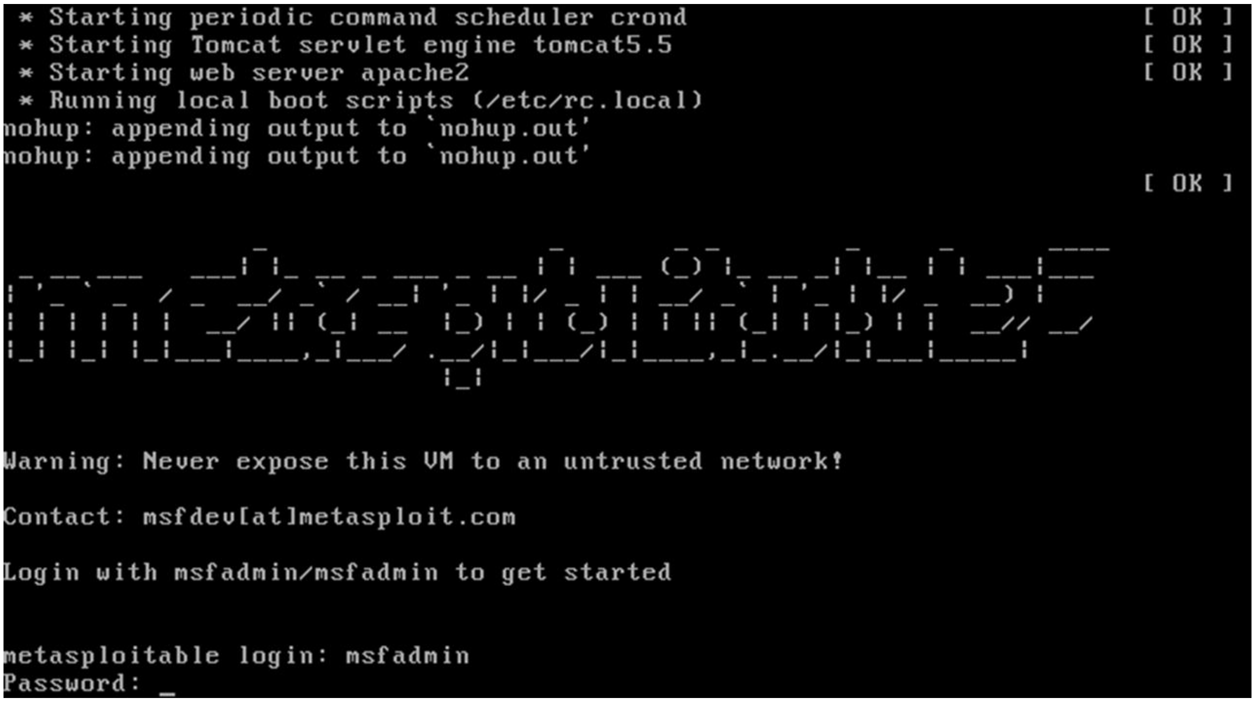
Promiscuous Mode: Deny

MAC Address: 080027CD52C2

☑ Cable Connected

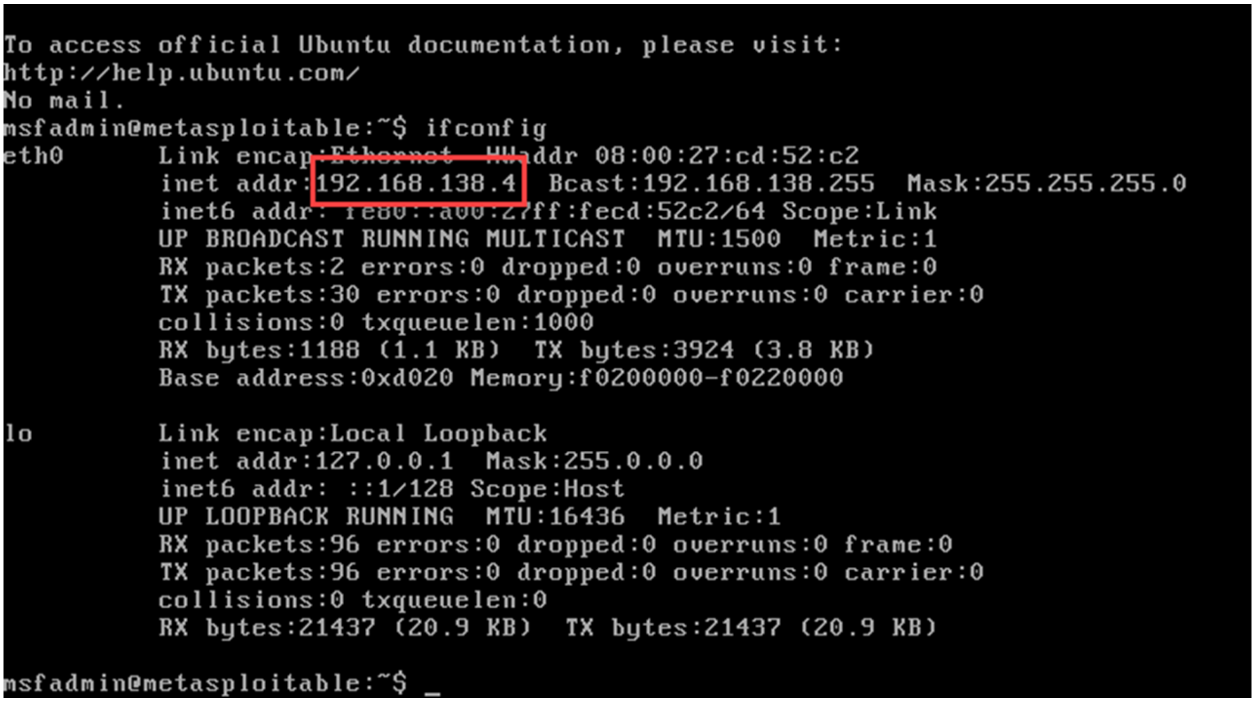
`

3. Start the Metasploitable virtual machine and log in with **msfadmin** as the username and password.



```
 * Starting periodic command scheduler crond                          [ OK ]
 * Starting Tomcat servlet engine tomcat5.5                           [ OK ]
 * Starting web server apache2                                        [ OK ]
 * Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'
                                                                      [ OK ]

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password: _
```

4. Now, let's check the IP Address of the Metasploitable virtual machine assigned by the DHCP server. Type **ifconfig** command on the console and hit **Enter**. Again, for your case, this might be different from the one on the screenshot. Take note of the IP Address as we are going to set it as a target at the GSM web interface.



```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:cd:52:c2
          inet addr:192.168.138.4  Bcast:192.168.138.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fecd:52c2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:30 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1188 (1.1 KB)  TX bytes:3924 (3.8 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:96 errors:0 dropped:0 overruns:0 frame:0
          TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21437 (20.9 KB)  TX bytes:21437 (20.9 KB)

msfadmin@metasploitable:~$ _
```

`

TASK 3: SCANNING THE VULNERABILITIES IN METASPLOITABLE

OBJECTIVE

To scan the vulnerabilities in Metaspolitable using Greenbone Security Manager (GSM).

TASK DESCRIPTION

For this task, the student needs to run the GSM scanner to assess the vulnerabilities of the Metasploitable Virtual Machine.

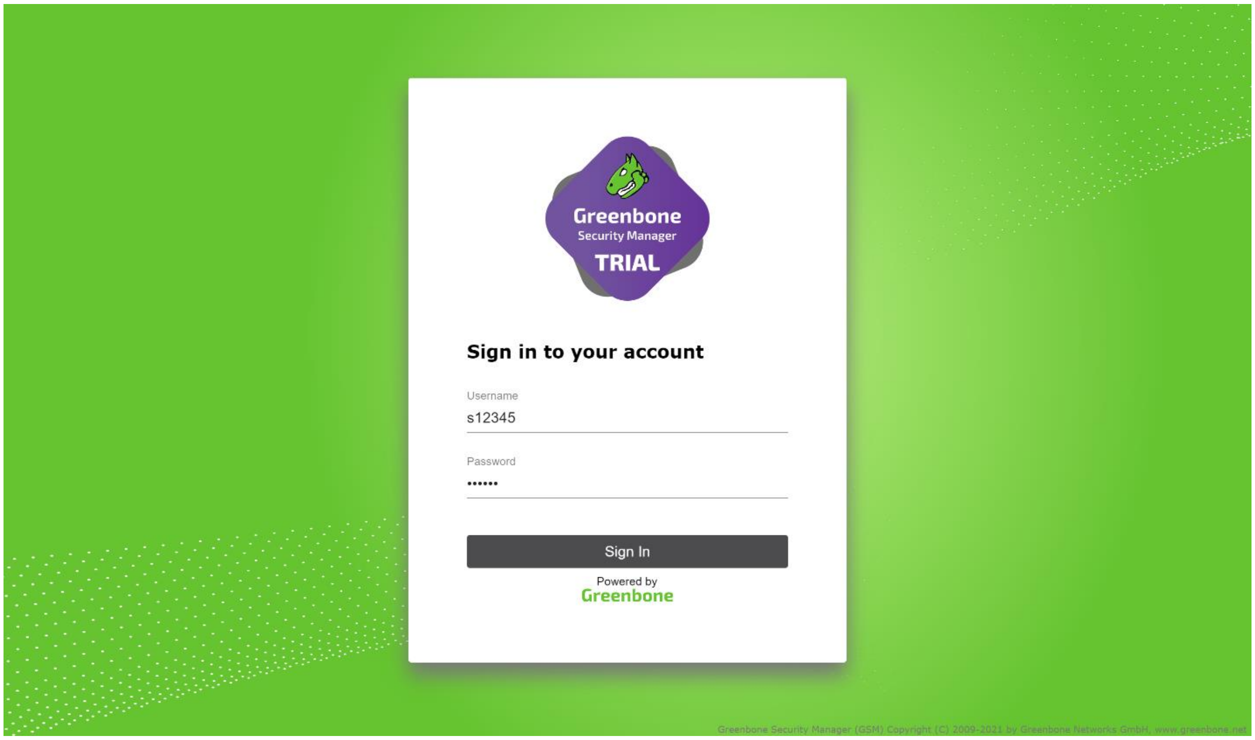
ESTIMATED TIME

105 Minutes

STEPS:

1. After completing the network set up in the previous task, now we ready to start the vulnerability scanning process.

2. First of all, go back to the link in Task 1. But now, we are going to log in with the new user credential (your matric number).



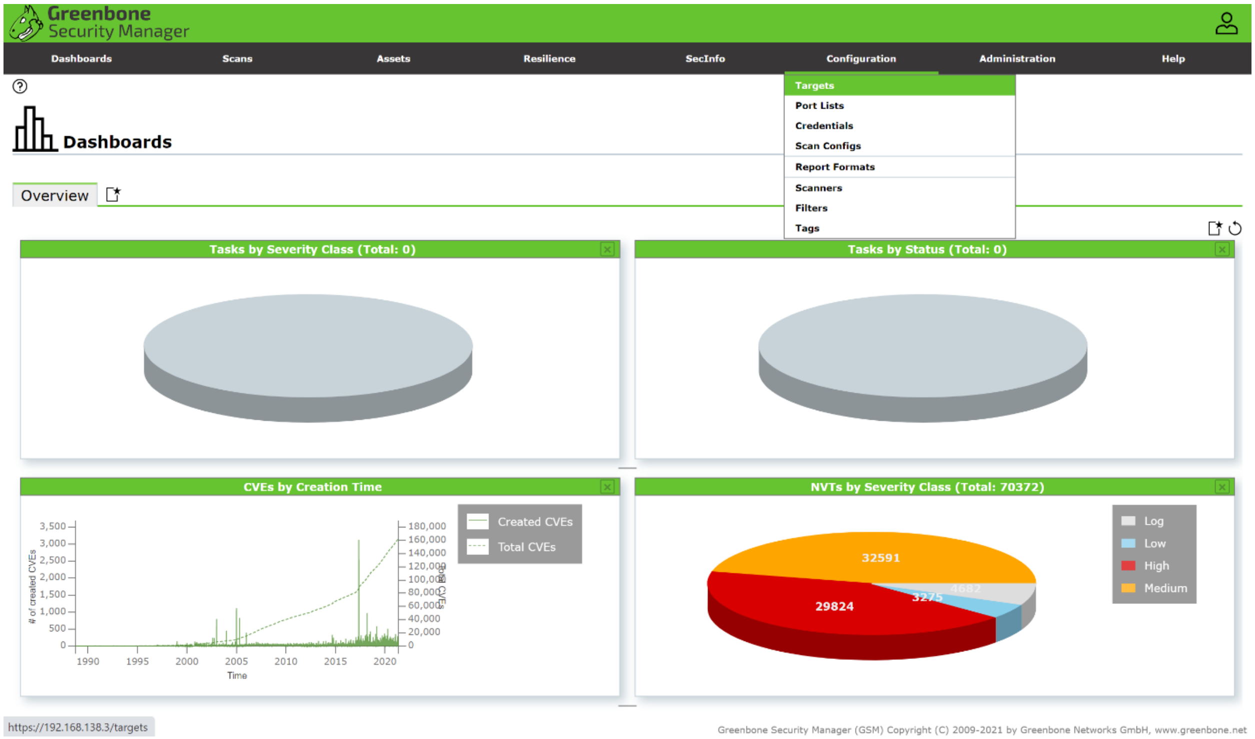
Username
s12345

Password
••••••

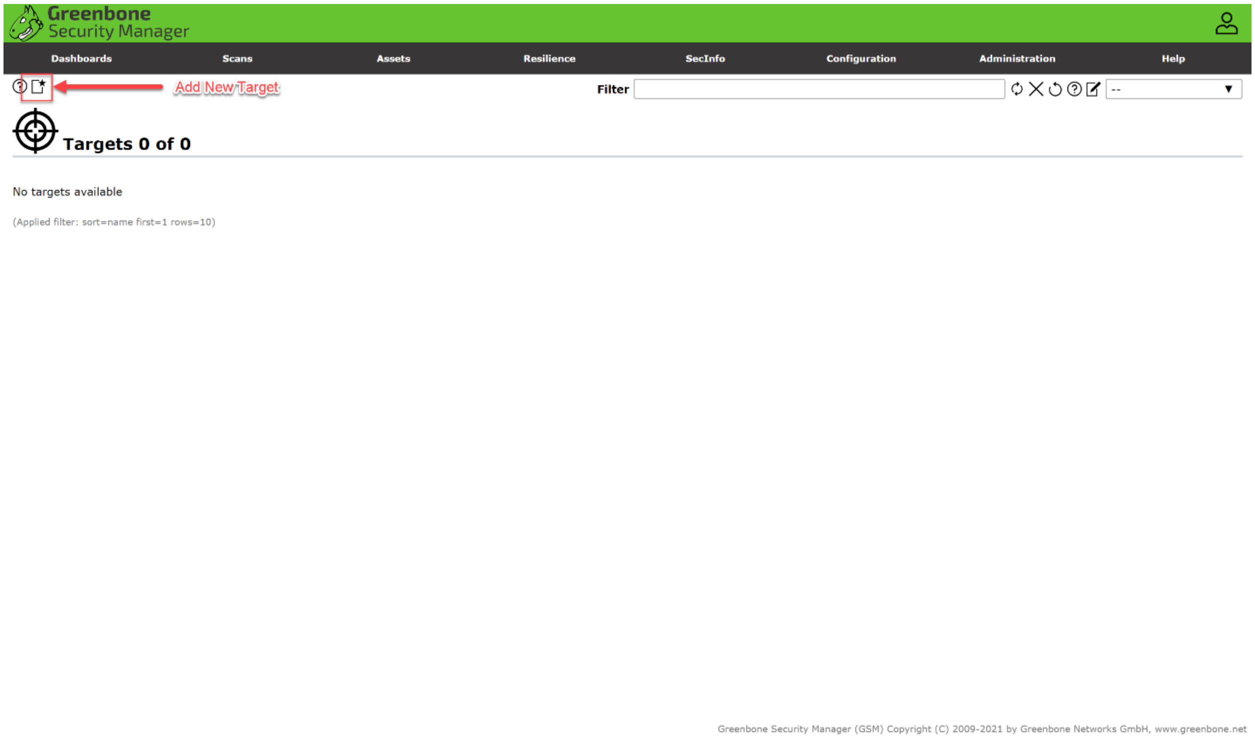
Greenbone Security Manager (GSM) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

`

3. Next, go to **Configuration>Targets**.

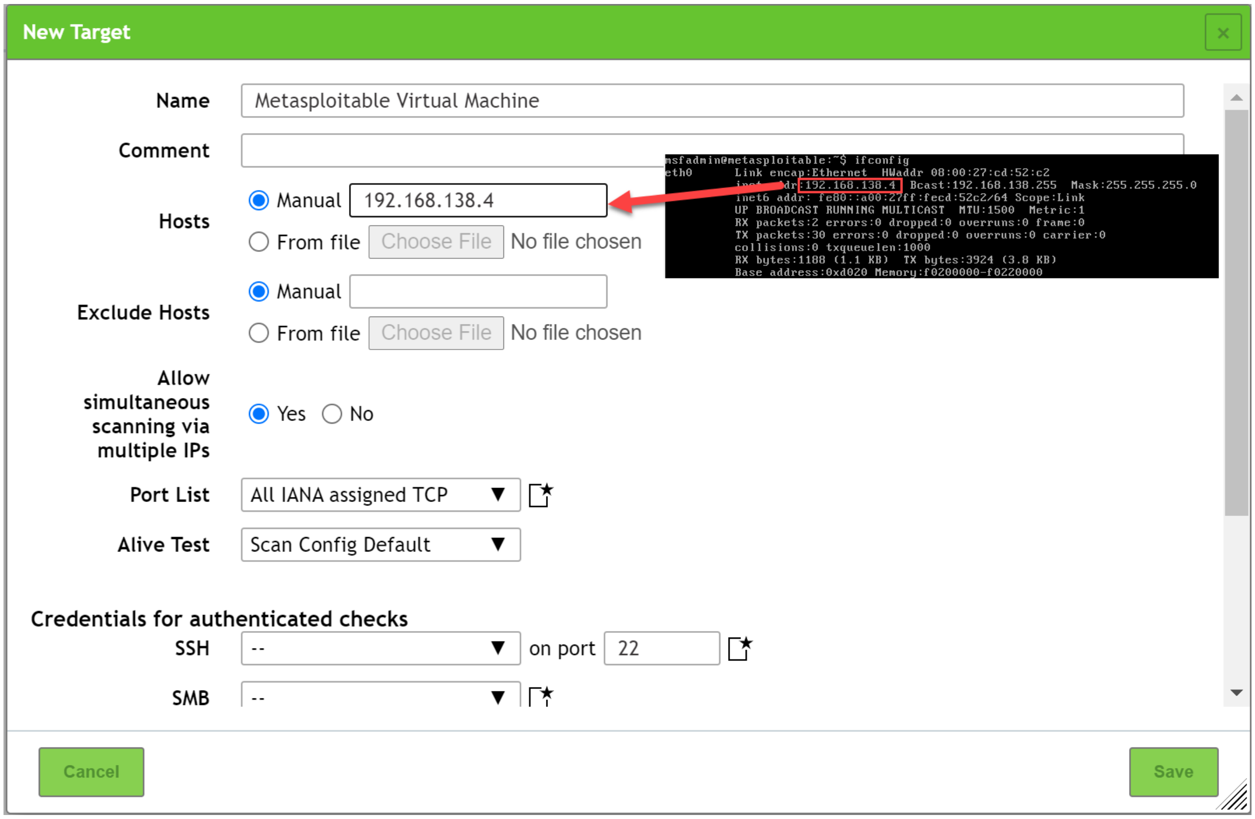


4. We are going to set the target. Our target is the Metasploitable virtual machine. Click on the icon to add a new target.



`

5. Name the target as **Metasploitable Virtual Machine** and put the IP Address as obtained in Task 2 Step 4. Make sure you enter it correctly.



Name: Metasploitable Virtual Machine

Comment:

Hosts: ● Manual 192.168.138.4
○ From file Choose File No file chosen

Exclude Hosts: ● Manual
○ From file Choose File No file chosen

Allow simultaneous scanning via multiple IPs: ● Yes ○ No

Port List: All IANA assigned TCP ▼

Alive Test: Scan Config Default ▼

Credentials for authenticated checks

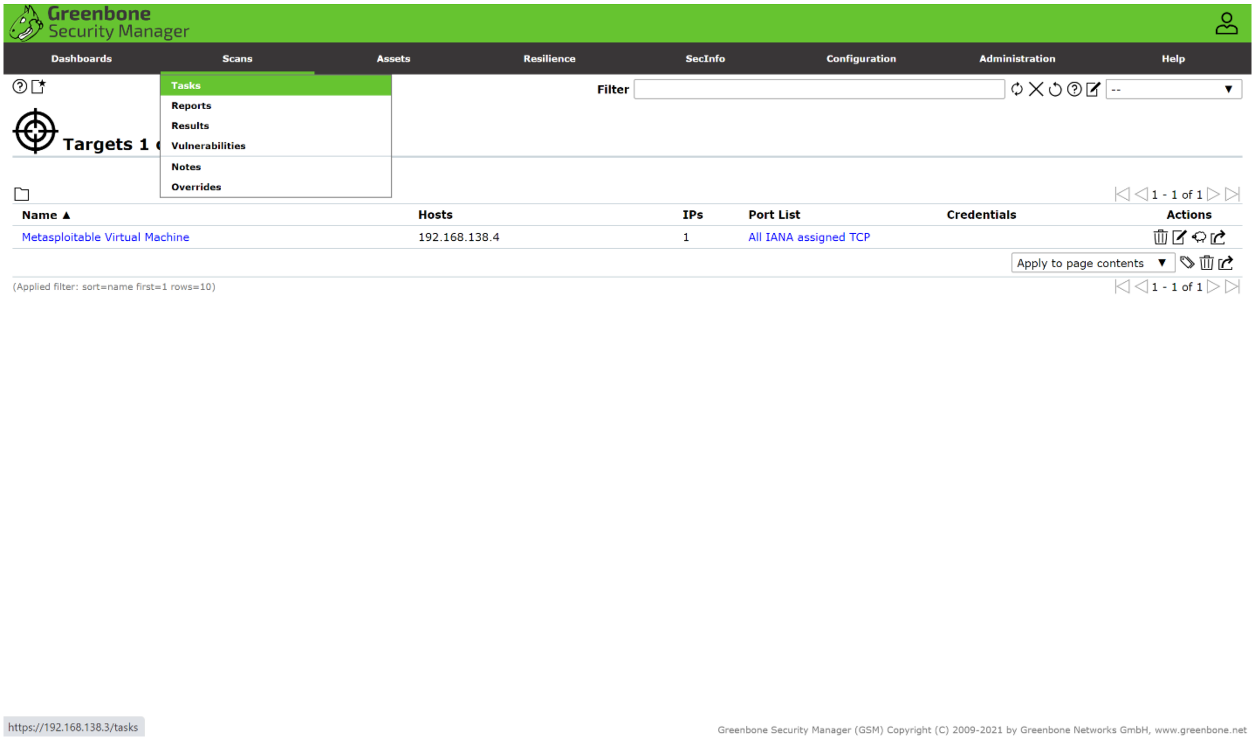
SSH: -- ▼ on port 22

SMB: -- ▼

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:cd:52:c2
          inet addr:192.168.138.4  Bcast:192.168.138.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fecd:52c2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:30 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1188 (1.1 KB)  TX bytes:3924 (3.8 KB)
          Base address:0xd020 Memory:f0200000-f0220000
```

`

6. After setting the target, we need to create the scanning task. Go to **Scans>Tasks**.



Targets 1 of 1

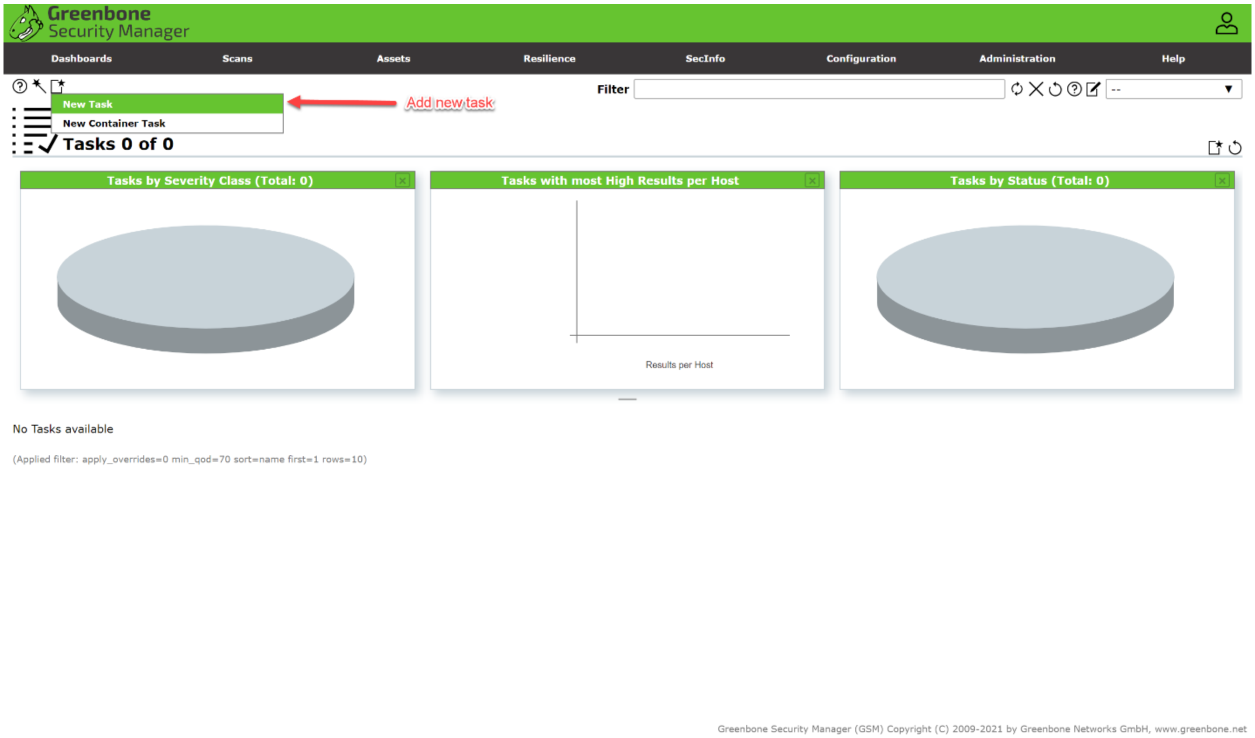
Name ▲	Hosts	IPs	Port List	Credentials	Actions
Metasploitable Virtual Machine	192.168.138.4	1	All IANA assigned TCP		

(Applied filter: sort=name first=1 rows=10)

https://192.168.138.3/tasks

Greenbone Security Manager (GSM) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

7. Click on the icon to add a new task.



Tasks 0 of 0

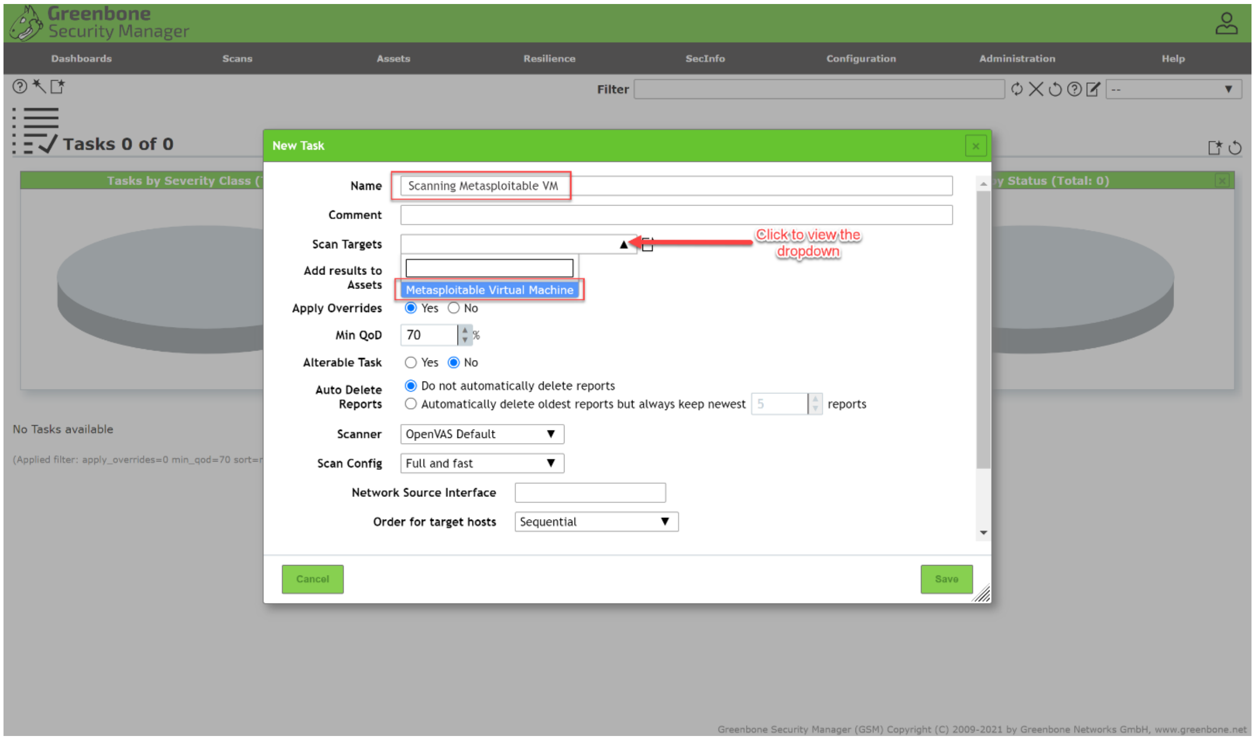
No Tasks available

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

Greenbone Security Manager (GSM) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

`

8. Name the task as **Scanning Metasploitable VM**. Set the **Scan Targets** as **Metasploitable Virtual Machine** from the dropdown list.



New Task

Name: Scanning Metasploitable VM

Comment:

Scan Targets: Metasploitable Virtual Machine

Add results to Assets

Apply Overrides: ● Yes ○ No

Min QoD: 70 %

Alterable Task: ○ Yes ● No

Auto Delete Reports: ● Do not automatically delete reports
○ Automatically delete oldest reports but always keep newest 5 reports

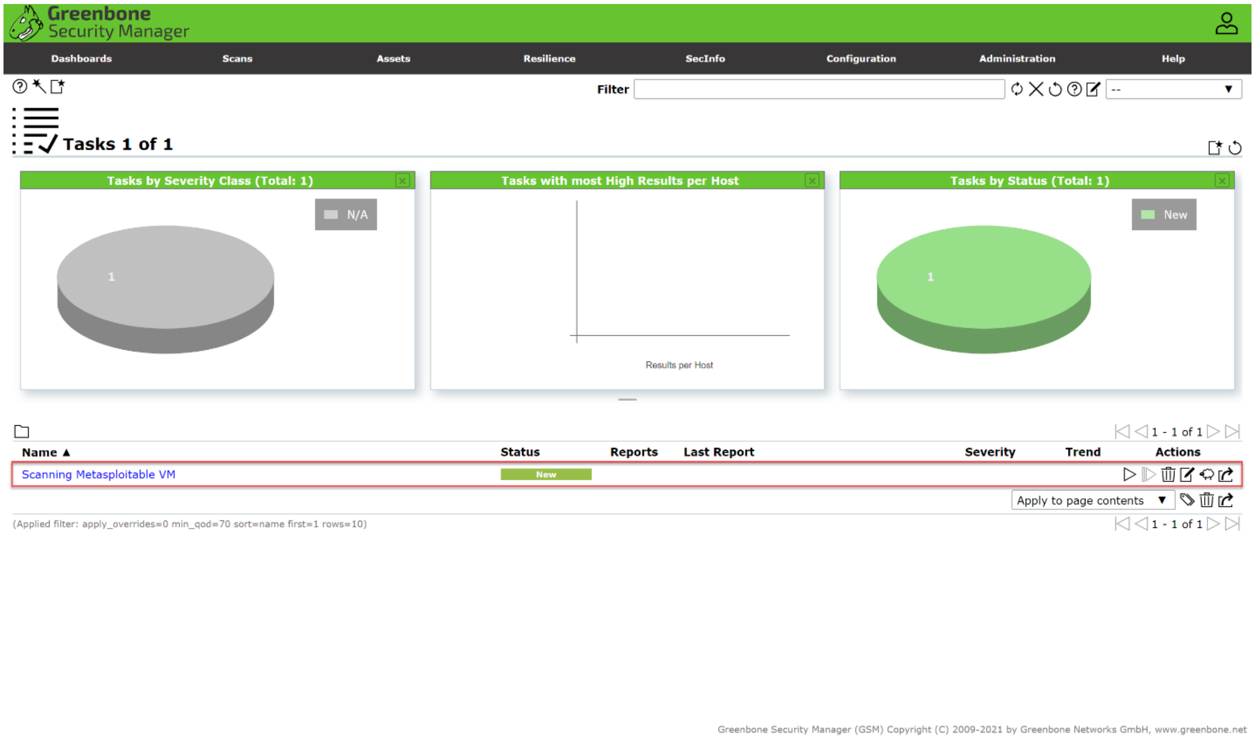
Scanner: OpenVAS Default

Scan Config: Full and fast

Network Source Interface:

Order for target hosts: Sequential

9. Now we can see that the newly created task is now on the list.

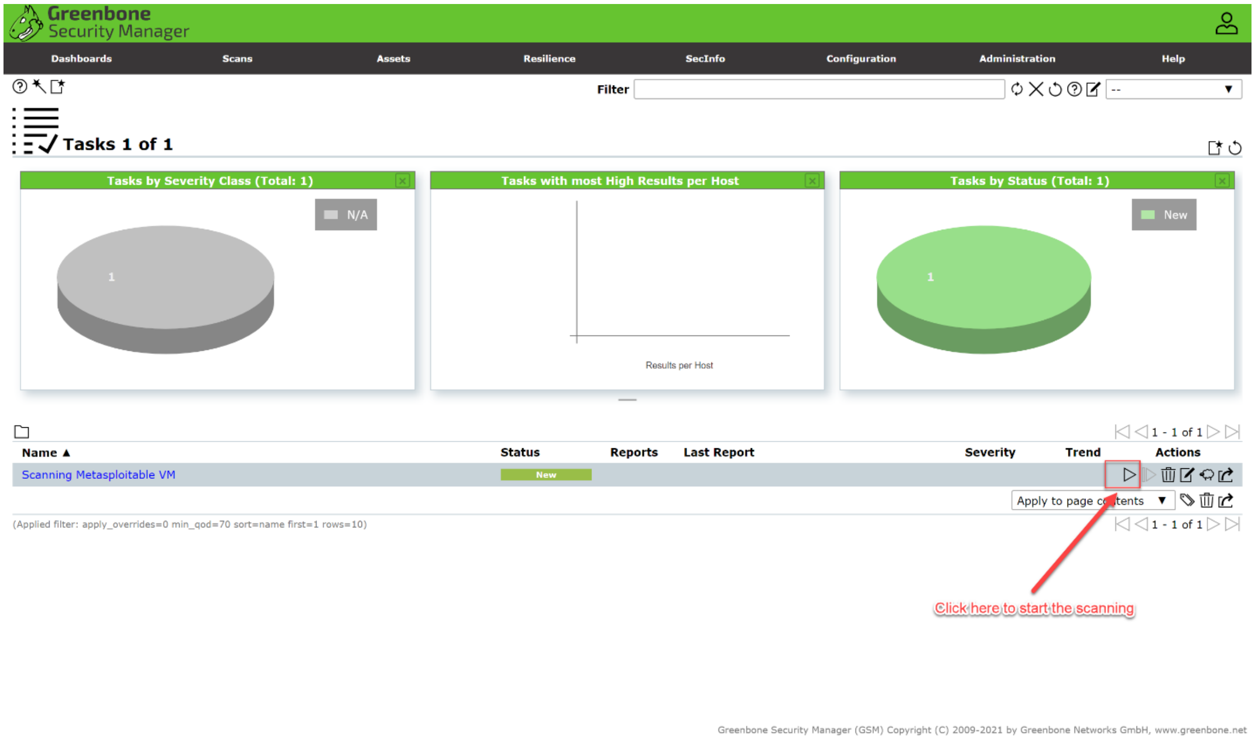

Greenbone
Security Manager
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help
Filter
--
Tasks 1 of 1
Tasks by Severity Class (Total: 1)
N/A
1
Tasks with most High Results per Host
Results per Host
Tasks by Status (Total: 1)
New
1
1 - 1 of 1
Apply to page contents
1 - 1 of 1
Greenbone Security Manager (GSM) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Scanning Metasploitable VM	New					

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

`

10. To begin the scanning, click on the icon.



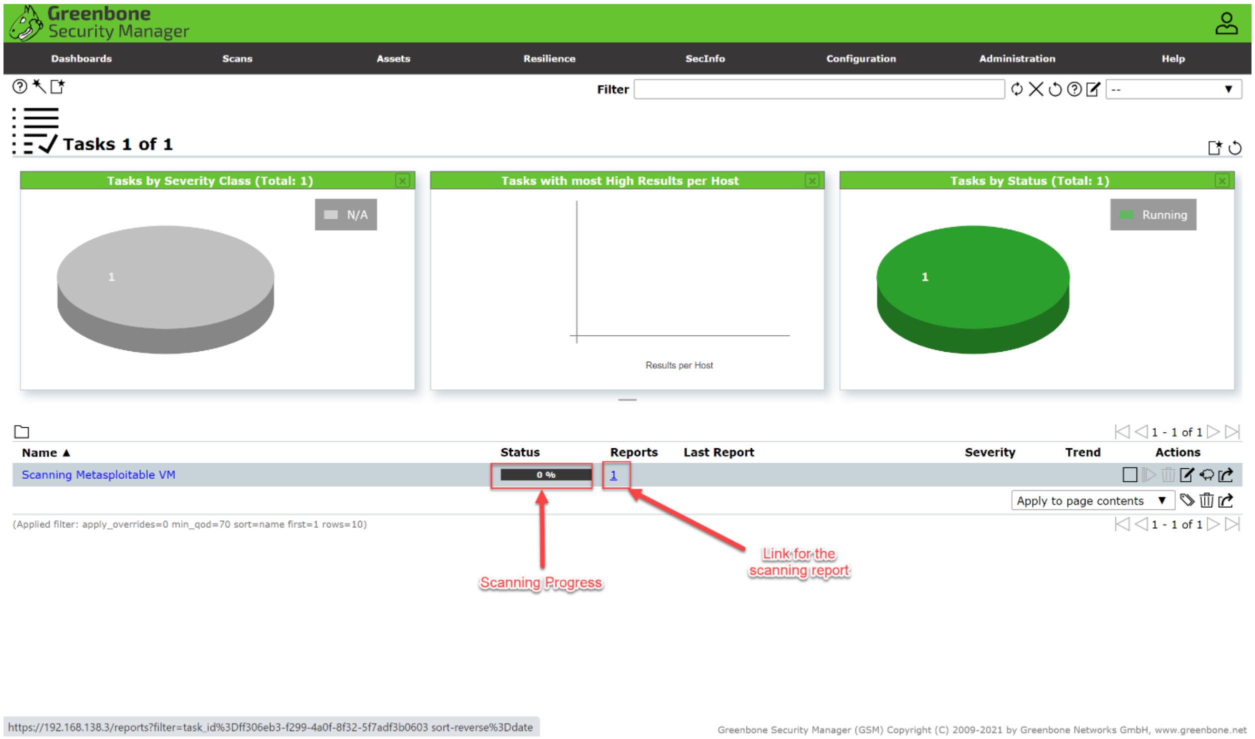
Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Scanning Metasploitable VM	New					

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

Click here to start the scanning

Greenbone Security Manager (GSM) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

11. You can see the progress and reports of the scanning on the screen. The scanning process could take more than half an hour to complete. While waiting, you may answer the reflection questions first.



Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Scanning Metasploitable VM	0 %	1				

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

Scanning Progress

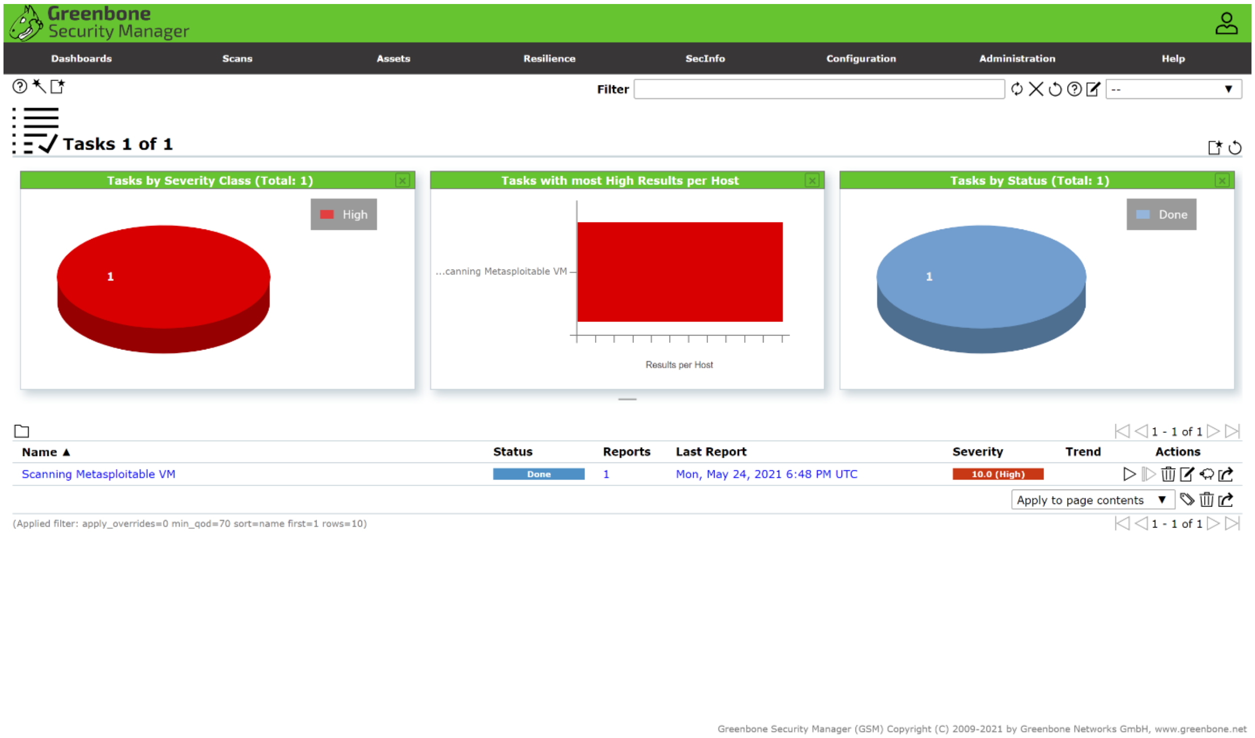
Link for the scanning report

https://192.168.138.3/reports?filter=task_id%3Dff306eb3-f299-4a0f-8f32-5f7adf3b0603 sort-reverse%3Ddate

Greenbone Security Manager (GSM) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

`

12. Below is the screenshot of a completed scan. You can see the status is now changed to **Done**. Please take a screenshot of this and put it into your lab report.



Tasks 1 of 1

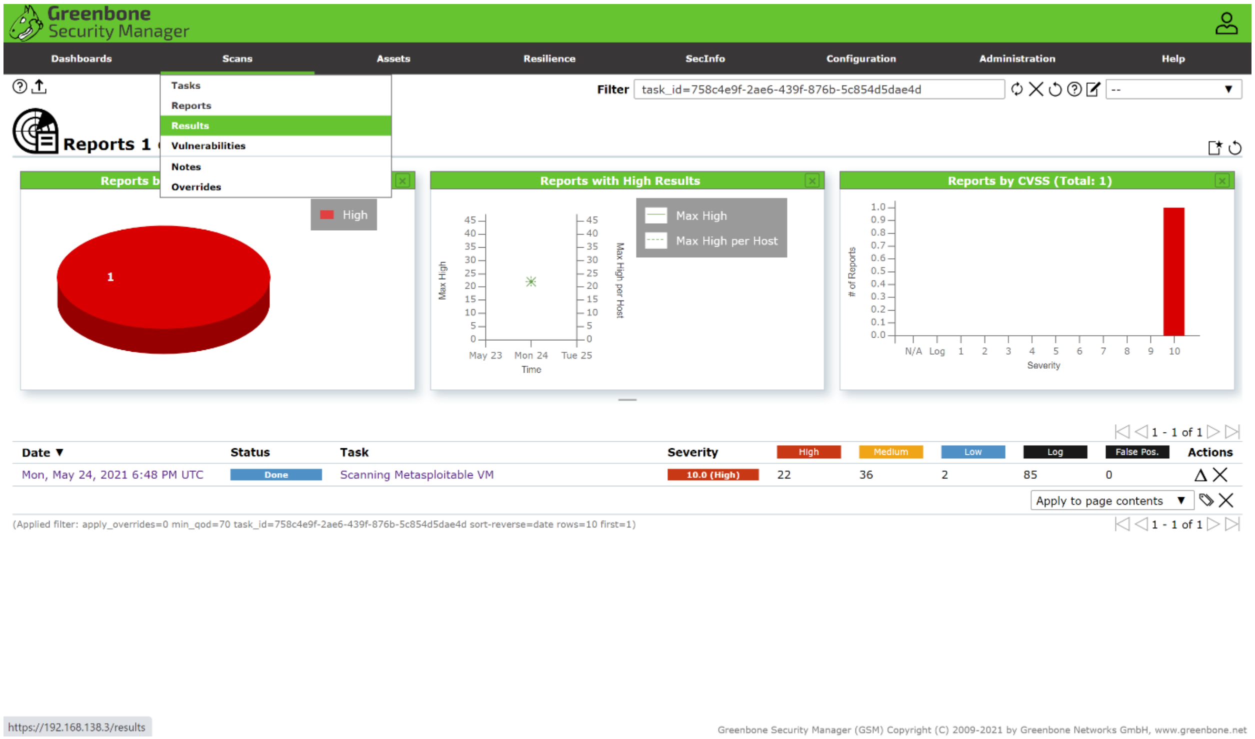
Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Scanning Metasploitable VM	Done	1	Mon, May 24, 2021 6:48 PM UTC	10.0 (High)		

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

Greenbone Security Manager (GSM) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

`

13. You can click on the date and time link of the **Last Report** on the previous screen to see the summary. Next, let's see the complete results by choosing **Scans>Results** from the menu.



Filter task_id=758c4e9f-2ae6-439f-876b-5c854d5dae4d

1 - 1 of 1

Date ▼	Status	Task	Severity	High	Medium	Low	Log	False Pos.	Actions
Mon, May 24, 2021 6:48 PM UTC	Done	Scanning Metasploitable VM	10.0 (High)	22	36	2	85	0	Δ ✕

Apply to page contents ▼

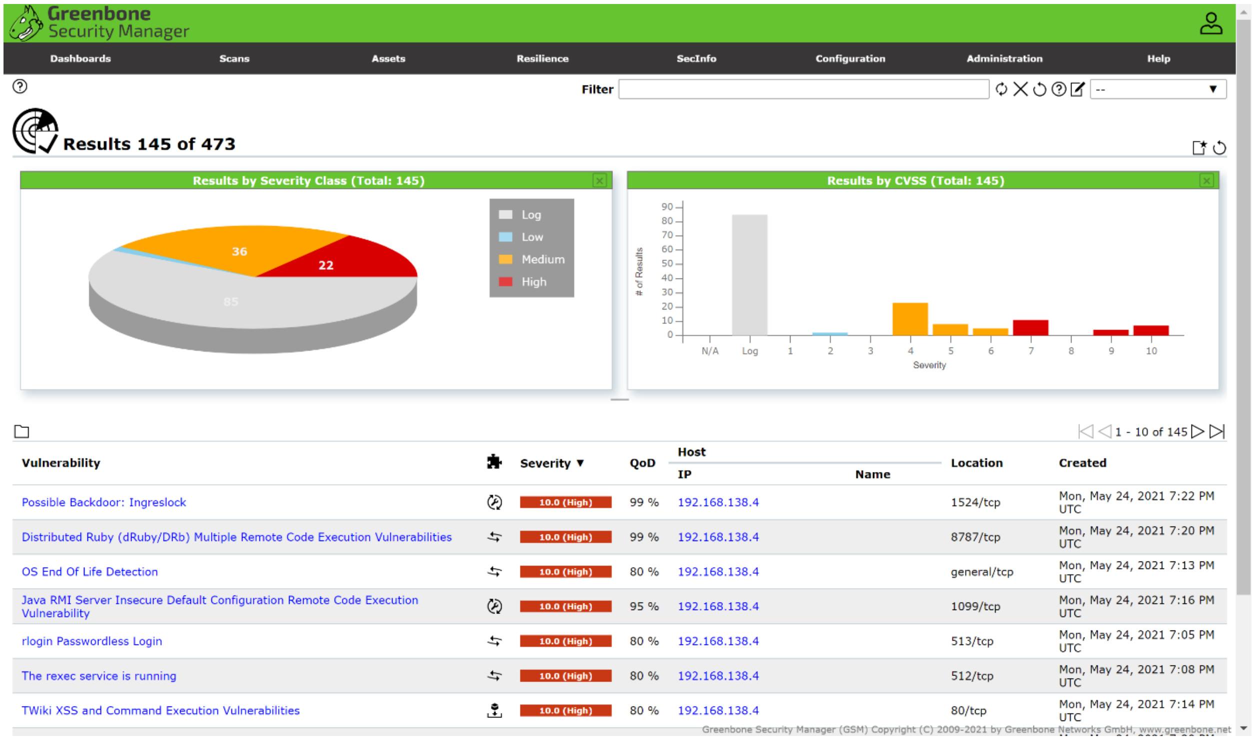
(Applied filter: apply_overrides=0 min_qod=70 task_id=758c4e9f-2ae6-439f-876b-5c854d5dae4d sort-reverse=date rows=10 first=1)

1 - 1 of 1

https://192.168.138.3/results

Greenbone Security Manager (GSM) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

14. At the following screen, you will see a list of vulnerabilities found at the Metasploitable virtual machine.



1 - 10 of 145

Vulnerability		Severity ▼	QoD	Host		Location	Created
				IP	Name		
Possible Backdoor: Ingreslock		10.0 (High)	99 %	192.168.138.4		1524/tcp	Mon, May 24, 2021 7:22 PM UTC
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities		10.0 (High)	99 %	192.168.138.4		8787/tcp	Mon, May 24, 2021 7:20 PM UTC
OS End Of Life Detection		10.0 (High)	80 %	192.168.138.4		general/tcp	Mon, May 24, 2021 7:13 PM UTC
Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability		10.0 (High)	95 %	192.168.138.4		1099/tcp	Mon, May 24, 2021 7:16 PM UTC
rlogin Passwordless Login		10.0 (High)	80 %	192.168.138.4		513/tcp	Mon, May 24, 2021 7:05 PM UTC
The rexec service is running		10.0 (High)	80 %	192.168.138.4		512/tcp	Mon, May 24, 2021 7:08 PM UTC
TWiki XSS and Command Execution Vulnerabilities		10.0 (High)	80 %	192.168.138.4		80/tcp	Mon, May 24, 2021 7:14 PM UTC

Greenbone Security Manager (GSM) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

`

15. You can find the details of each vulnerability by clicking on the link of the name.

16. Based on your findings, answer the following questions:

    a. Referring to the result of the scanning, complete the table of the severity class below:

Severity	**Total**
High	
Medium	
Low	
Log	
Grand Total	145

    b. What are vulnerabilities that have the highest severities? List them.

    c. What is the vulnerability for port 513/tcp?

    d. List three (3) vulnerabilities with medium severity.

    e. Based on the given information by GSM, how do we solve the "VNC Brute Force" vulnerability?

REFLECTION QUESTIONS

1. In your own words, explain about Common Vulnerability Scanning System (CVSS) and Common Vulnerability Enumeration (CVE).
2. Explain the difference(s) between CVSS and CVE.
3. How many severity levels are there in the CVSS version 3.0?
4. Draw a table of CVSS3.0 severity levels and their base score range.
5. Observe the information provided at vuldb.com and answer the questions below:
    a. List three (3) most recent vulnerabilities and their severities.
    b. List three (3) latest available exploits.
    c. List three (3) vulnerabilities in current CVSS Top 5.