Lab 03 Requirements

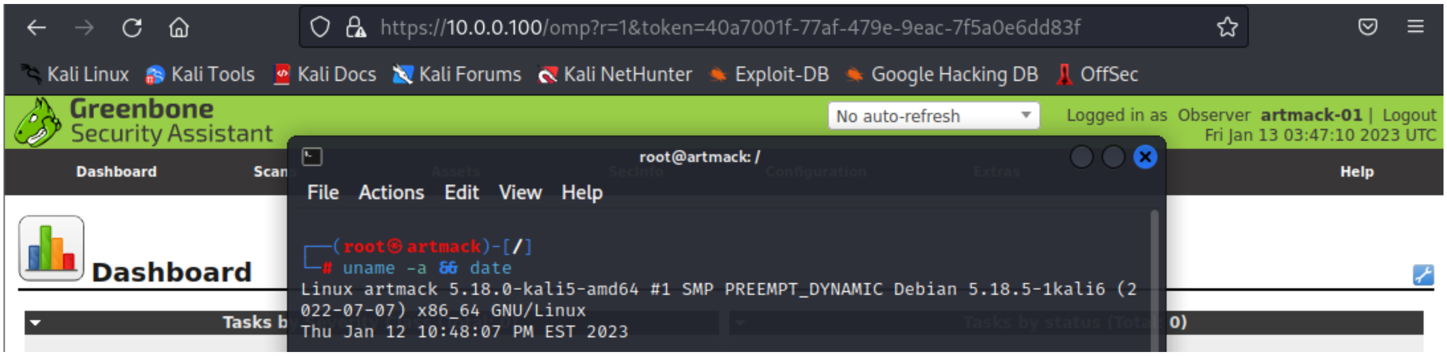
- Internet connectivity & VMware Workstation version 15.5.7 or above
- Download **OpenVAS9.7z** from resources link under content on FOL
- Download **S2008R2.7z** from resources link under content on FOL
- VM Snapshots from previous labs

Part 01: Initial Configuration of OpenVAS

- Use 7-zip to unzip **OpenVAS9.7z** on your host machine
- Verify that the 2 network adapters are configured so that the first is on NAT, and the second is on your INFO6065 LAN Segment. Ensure that the LAN segment is set correctly before powering OpenVAS up
- Power on the OpenVAS9 VM (if asked, select **I Moved it**)
- Logon with the username student and password student, then change your password to INFO6065 with the passwd command
- Use the **sudo -su** command to switch to the root user
- Change the hostname to your ov-FOLusername (example: ov-artmack)

Greenbone Security Assistant

- On Kali, open a browser and navigate to https://10.0.0.100
- Accept the risks and login as admin / admin
- Under Administration → Users, edit the admin user and change the password to INFO6065
- You use the star symbol to make new entities in OpenVAS
- Create a user called FOLusername-01 with INFO6065 as the password
- For **Roles** select **Observer** and leave defaults for the rest



Logged in as Observer **artmack-01** | Logout
Fri Jan 13 03:47:10 2023 UTC

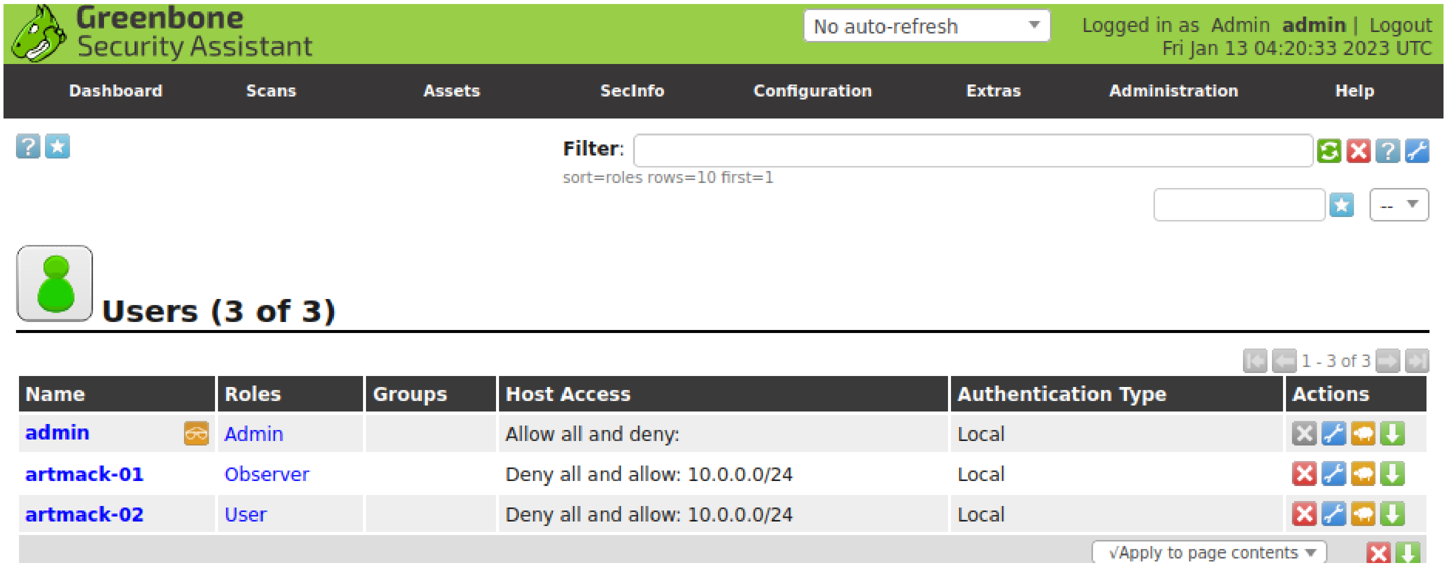
```
┌──(root㉿artmack)-[/]
└─# uname -a && date
Linux artmack 5.18.0-kali5-amd64 #1 SMP PREEMPT_DYNAMIC Debian 5.18.5-1kali6 (2
022-07-07) x86_64 GNU/Linux
Thu Jan 12 10:48:07 PM EST 2023
```

Slide 01:

- Login as FOLusername-01 then take a screenshot showing the logged in user as an **Observer**
- Include the output of **uname –a && date** from the terminal as shown in the example above

User Management

- From Kali, log back into OpenVAS as the **admin**
- Under Administration → Users, create a new user called FOLusername-02 with a password of INFO6065 and leave them as in the role of **User**
- Login as this new user then navigate back to the Administration → Users tab
  - If you set things up correctly, you won't even be able to see the tab
- Logout and log back in as **admin**, then navigate back to the Administration → Users tab
  - Choose to edit FOLusername-02
  - Investigate the **Roles** options for users
  - Are you able to control the hosts a user can or can't access?
  - Set FOLusername-01 and FOLusername-02 to be able to access only hosts on the subnet we are using for our LAN segment. (CIDR)



Users (3 of 3)

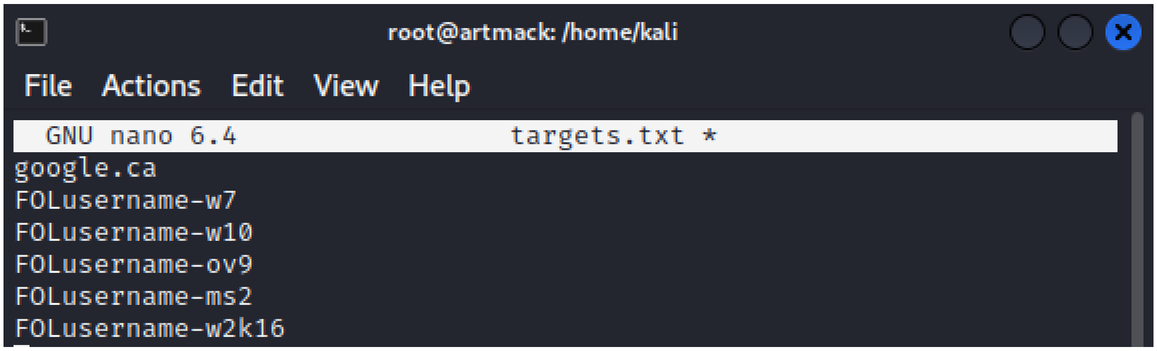
Name	Roles	Groups	Host Access	Authentication Type	Actions
admin	Admin		Allow all and deny:	Local	
artmack-01	Observer		Deny all and allow: 10.0.0.0/24	Local	
artmack-02	User		Deny all and allow: 10.0.0.0/24	Local	

Slide 02:

- Take a screenshot that shows the three current users and their settings as shown in the example above

Power on your other VMs and confirm connectivity

Update the **/etc/hosts** file on Kali Linux to include an entry for the OpenVAS9 VM. Your hosts file on Kali should now be able to resolve IPs to your other VMs. Create a new file named targets.txt in /home/kali with the following contents:

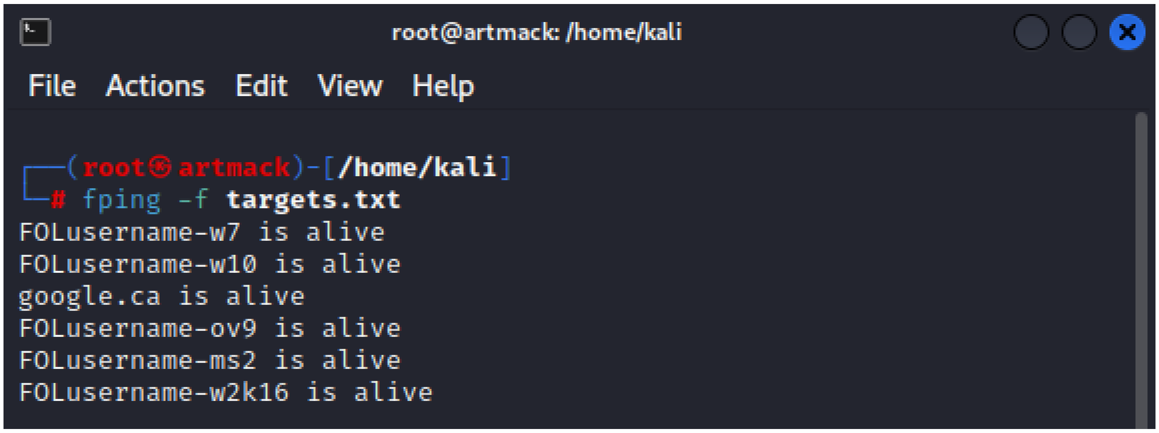


```
  GNU nano 6.4                targets.txt *
google.ca
FOLusername-w7
FOLusername-w10
FOLusername-ov9
FOLusername-ms2
FOLusername-w2k16
```

Save and exit the file

You can use ping to check if each host is up, but another option is to use **fping** as it allows you to ping numerous hosts at once. You can use a list from a file with the **-f** option:

fping -f targets.txt



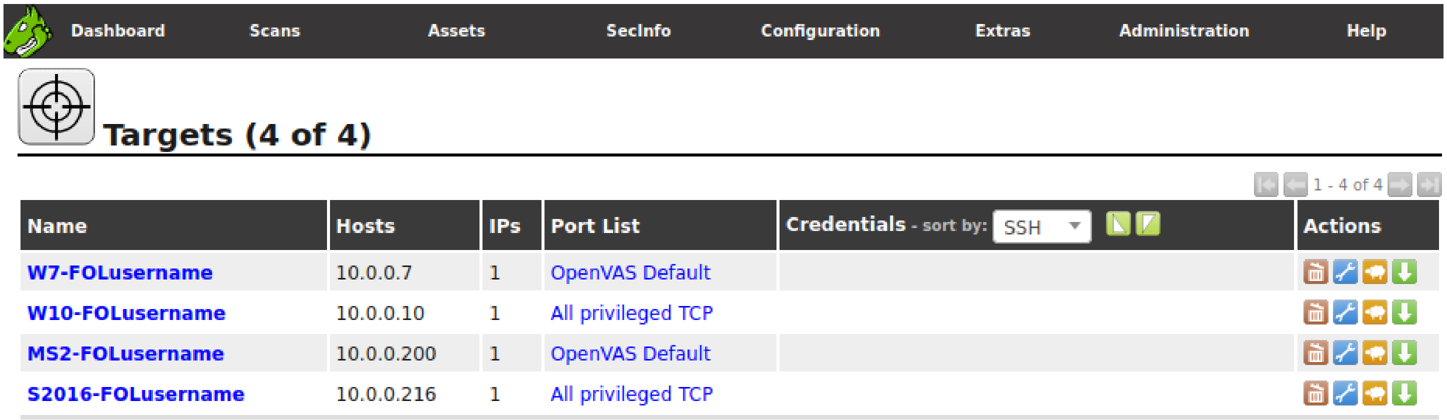
```
┌──(root㉿artmack)-[/home/kali]
└─# fping -f targets.txt
FOLusername-w7 is alive
FOLusername-w10 is alive
google.ca is alive
FOLusername-ov9 is alive
FOLusername-ms2 is alive
FOLusername-w2k16 is alive
```

Slide 03:
- From Kali, ping google, your 4 targets, and the OpenVAS9 scanner VM
- All pings need to show as alive

Part 02: Create Alerts, Tasks & Events

Create Targets

- Before we can do any scans we need to create the targets: one for each VM
- You create targets under **Configuration → Targets**
- Click on the star symbol ⭐ to create a *New Target*
- Use the naming scheme and configuration information as shown below:



Targets (4 of 4)

Name	Hosts	IPs	Port List	Credentials - sort by: SSH	Actions
W7-FOLusername	10.0.0.7	1	OpenVAS Default		
W10-FOLusername	10.0.0.10	1	All privileged TCP		
MS2-FOLusername	10.0.0.200	1	OpenVAS Default		
S2016-FOLusername	10.0.0.216	1	All privileged TCP		

Slide 04:
- Take a screenshot of the 4 targets as shown in the example above
- Sort your list by ascending IPs

Create an Alert

- You can create alerts to let you know when certain types of vulnerabilities are found
- Under **Configuration → Alerts**, create an alert with the following parameters: (defaults for anything else)

Name: High Vulnerability Found
Event: Done
Condition: Severity Level of at least 3.0
To Address: FOLusername@info6065.lab
From Address: nobody@nobody.ca

Create Tasks

- Now that we have some targets, we can create some tasks
- One for each of the 4 targets you set up in the previous step
- Under **Scans → Tasks** create four new tasks
  - Include the alert you just created for all the targets

Use the following settings:

Names	Scan Config	Scan Target	Alert
MS2-FOLusername	Full and fast	MS2-FOLusername	High Vuln.
S2016-FOLusername	Full and fast	S2016-FOLusername	High Vuln.
W7-FOLusername	Full and fast	W7-FOLusername	High Vuln.
W10-FOLusername	Full and fast	W10-FOLusername	High Vuln.

Before running your scans click on the name of each scan in the task list and check your settings. Sometimes they don't take, and you need to delete, then recreate the task.

Run Scans

- You should still have connectivity to all 4 target VMs
- Go back to the tasks list and start these two scans (only two scans at a time)
- Change the **auto-refresh to every 30 seconds** so you can see the progress
  - You will need to hit the refresh button once for it to take effect
- As your scans finish, you can start another (e.g. when W7 finishes, start MS2)
- You don't want more than two scans running at a time

You can proceed with the rest of the lab while you wait for all 4 scans to finish

Schedule an Event

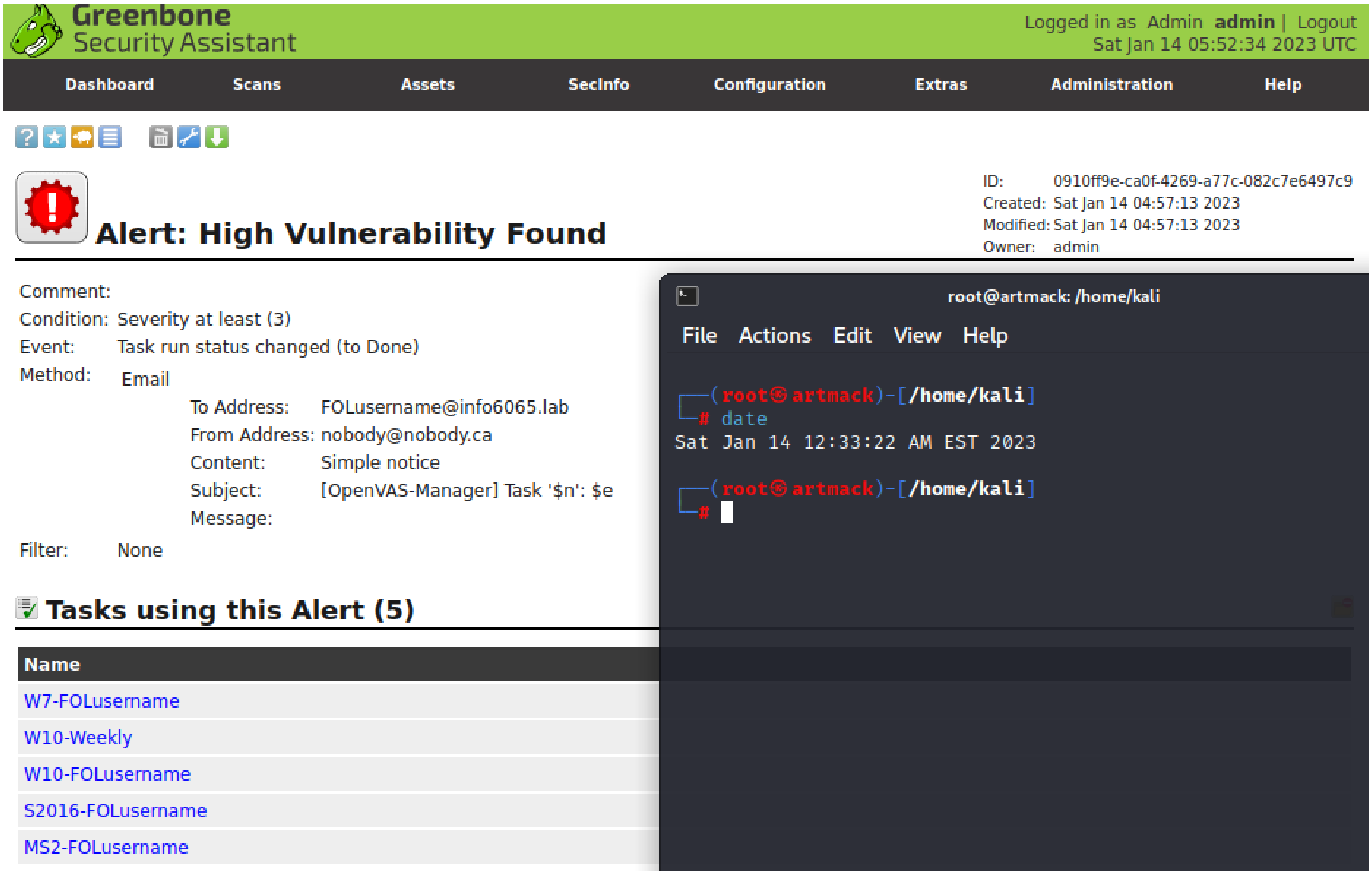
- Under configuration create a scheduled event called **Weekly** that will run a scan every week at 3:00a.m., starting on October 02, 2020 (*set to a date in the past*)
  - You don't need to set a duration
- View the Schedule details once it is created

Create Another Task With New Options

Create a new task to scan the W10 VM

Name: W10-Weekly
Comment: Weekly Scan of W10 VM
Scan Config: Full and Fast
Target: W10-FOLusername
Alerts: High Vulnerability Found
Schedule: Weekly

Once you have saved the weekly task, go to **Configuration → Alerts** and click on the Alert you created previously to view the details:



Alert: High Vulnerability Found

ID: 0910ff9e-ca0f-4269-a77c-082c7e6497c9
Created: Sat Jan 14 04:57:13 2023
Modified: Sat Jan 14 04:57:13 2023
Owner: admin

Comment:
Condition: Severity at least (3)
Event: Task run status changed (to Done)
Method: Email
To Address: FOLusername@info6065.lab
From Address: nobody@nobody.ca
Content: Simple notice
Subject: [OpenVAS-Manager] Task '$n': $e
Message:
Filter: None

Tasks using this Alert (5)

Name
W7-FOLusername
W10-Weekly
W10-FOLusername
S2016-FOLusername
MS2-FOLusername

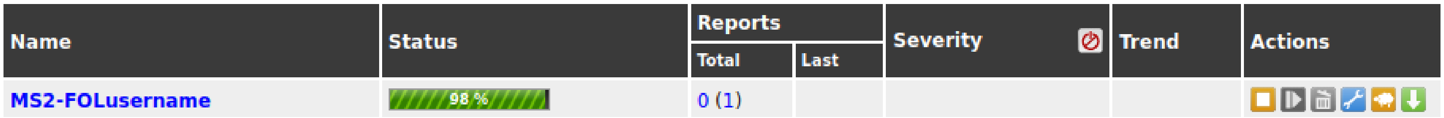
```
┌──(root㉿artmack)-[/home/kali]
└─# date
Sat Jan 14 12:33:22 AM EST 2023

┌──(root㉿artmack)-[/home/kali]
└─# 
```

Slide 05:

- Show the details for the Alert you created earlier by clicking on the Alert name
- Include the 5 tasks using this alert and the output of the **date** command in the terminal

View Your Scans

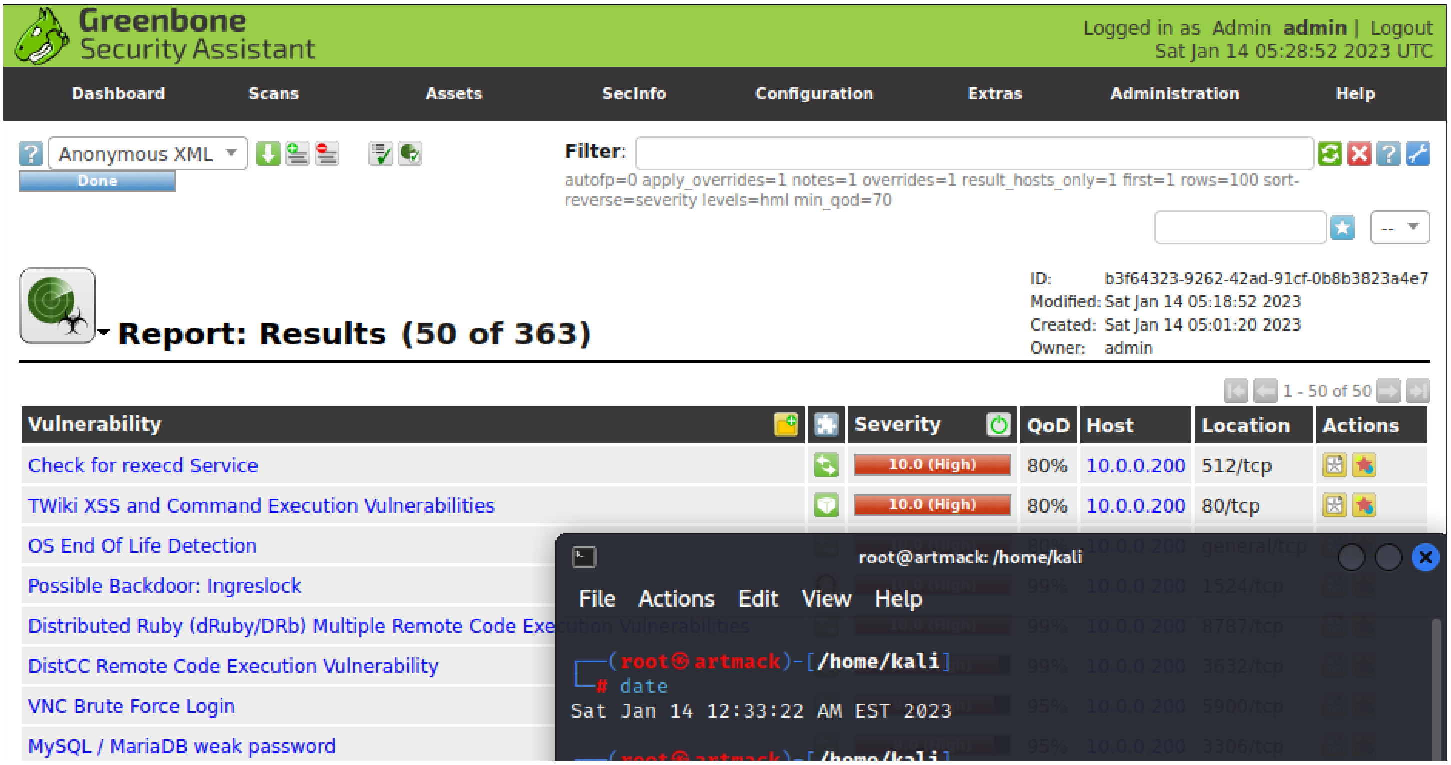
- The scan for Metasploitable2 will take a while, as Metasploitable2 has the most vulnerabilities
  - It will sit at 98% for a long, long time…



Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
MS2-FOLusername	98 %	0 (1)				

- If the scan looks like it is stuck, you can open Wireshark to see if it is still scanning the target
- This is a good opportunity to examine some of the packets to see what OpenVAS is doing

Once the MS2 scan is finished, click on the date of the scan to view the scan results page:



Logged in as Admin **admin** | Logout
Sat Jan 14 05:28:52 2023 UTC

Filter:
autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70

Report: Results (50 of 363)

ID: b3f64323-9262-42ad-91cf-0b8b3823a4e7
Modified: Sat Jan 14 05:18:52 2023
Created: Sat Jan 14 05:01:20 2023
Owner: admin

1 - 50 of 50

Vulnerability		Severity	QoD	Host	Location	Actions
Check for rexecd Service		10.0 (High)	80%	10.0.0.200	512/tcp	
TWiki XSS and Command Execution Vulnerabilities		10.0 (High)	80%	10.0.0.200	80/tcp	
OS End Of Life Detection		10.0 (High)	80%	10.0.0.200	general/tcp	
Possible Backdoor: Ingreslock		10.0 (High)	99%	10.0.0.200	1524/tcp	
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities		10.0 (High)	99%	10.0.0.200	8787/tcp	
DistCC Remote Code Execution Vulnerability		[illegible]	99%	10.0.0.200	3632/tcp	
VNC Brute Force Login		[illegible]	95%	10.0.0.200	5900/tcp	
MySQL / MariaDB weak password		9.0 (High)	95%	10.0.0.200	3306/tcp	

root@artmack: /home/kali

```
┌──(root㉿artmack)-[/home/kali]
└─# date
Sat Jan 14 12:33:22 AM EST 2023

┌──(root㉿artmack)-[/home/kali]
```

Slide 06:

- Take a screenshot of the Report Results Page for MS (click on the date of the scan)
- Include the output of the **date** command

- Download the Metasploitable2 report as a pdf file and view it in the document viewer
- List five different pieces of useful information you can find in the report (can be done later)