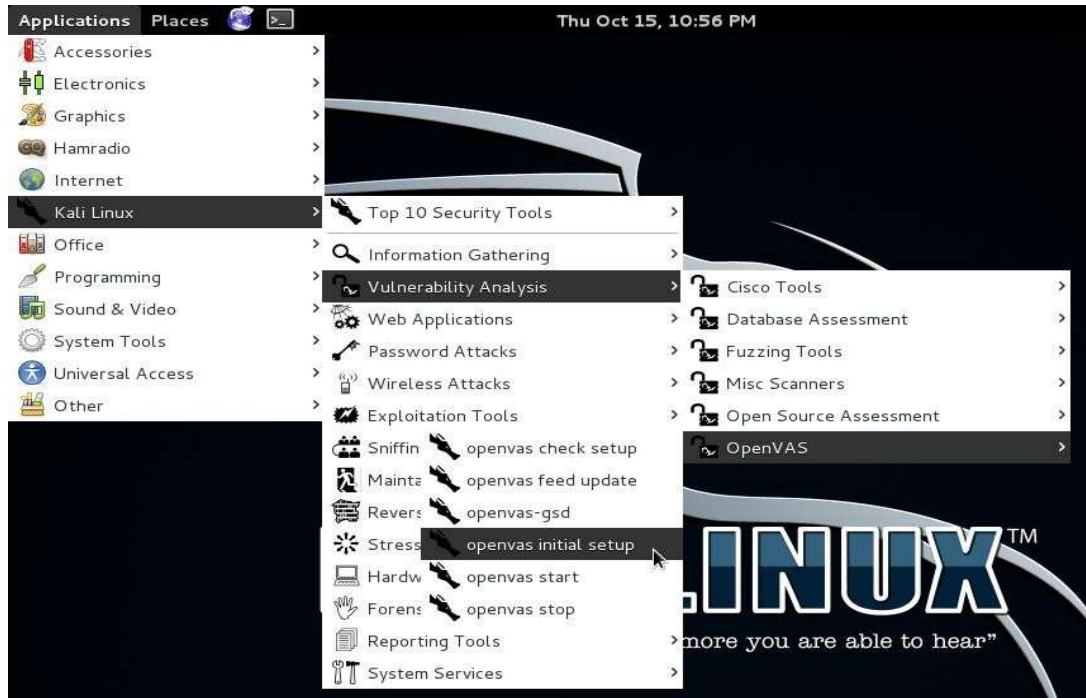


Practical – 6

Aim: Find out the vulnerability of network and perform penetration testing using OpenVas.

- OpenVAS (Open Vulnerability Assessment System the name of the fork originally known as GNESSUs) is a framework of several services and tools offering a vulnerability scanning and vulnerability management solution.
- Setup and Start OpenVAS
On the first run of openvas on kali linux you need to run a setup script: apps > kali linux > vulnerability analysis > openvas > openvas initial setup



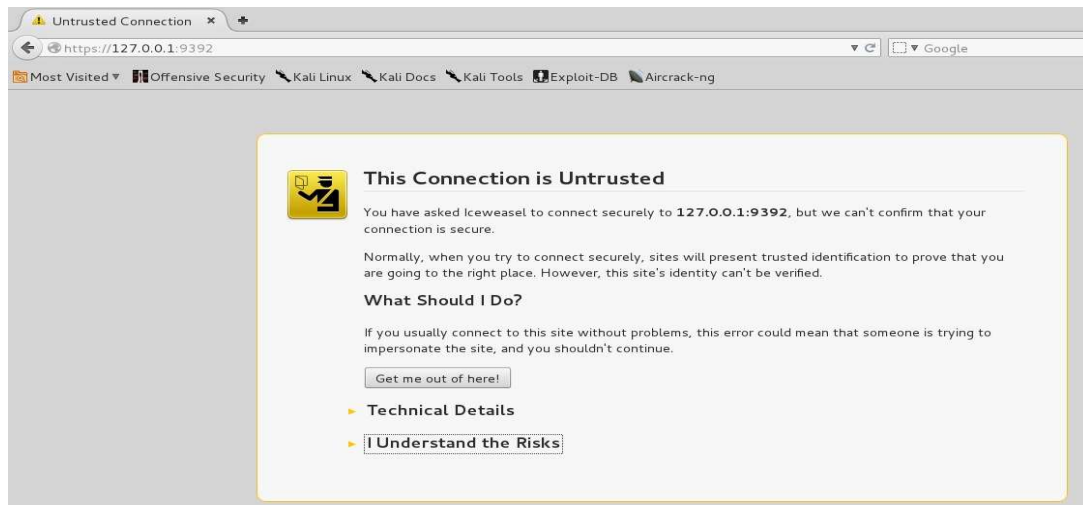
```
[i] This script synchronizes an NVT collection with the 'OpenVAS NVT Feed'.
[i] The 'OpenVAS NVT Feed' is provided by 'The OpenVAS Project'.
[i] Online information about this feed: 'http://www.openvas.org/openvas-nvt-feed.html'.
[i] NVT dir: /var/lib/openvas/plugins
[w] Could not determine feed version.
[i] rsync is not recommended for the initial sync. Falling back on http.
[i] Will use wget
[i] Using GNU wget: /usr/bin/wget
[i] Configured NVT http feed: http://www.openvas.org/openvas-nvt-feed-current.tar.bz2
[i] Downloading to: /tmp/openvas-nvt-sync.aG0be7f2vG/openvas-feed-2015-10-10-1189.tar.bz2
--2015-10-10 19:00:43-- http://www.openvas.org/openvas-nvt-feed-current.tar.bz2
Resolving www.openvas.org (www.openvas.org)... 5.9.98.186, 64:ff9b::509:62ba
Connecting to www.openvas.org (www.openvas.org)[5.9.98.186]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 17751802 (17M) [application/x-bzip2]
Saving to: '/tmp/openvas-nvt-sync.aG0be7f2vG/openvas-feed-2015-10-10-1189.tar.bz2'

-feed-2015-10-10-1189.tar.b 37%[=====>]vc.aG0e7fov-ep
as-feed-2015-10-10-1189 46%[=====>] 7.92M 102KB/s eta 1m 53s
```

- We only need to run this once
- We will then need to start the openvas services:
apps > kali Linux > vulnerability analysis > openvas > start openvas



- Once openvas has started, open browser and point it to:
<https://127.0.0.1:9392>



- After pointing to the address we found above page on screen we have to click on "I Understand the Risk" and "add the Exception" respectively.
- After adding Exception this opens the 'greenbone' web interface for openvas as shown in bellow image.



- Login with default user name "admin" and password "password".
- If Failed to login and found "login failed. omp service is down " then open terminal and fire bellow commands.
openvasmd --user=admin --new-password=password

```

root@divyang: ~
File Edit View Search Terminal Help
root@divyang:~# openvasmd --user=admin --new-password=password
root@divyang:~#

```

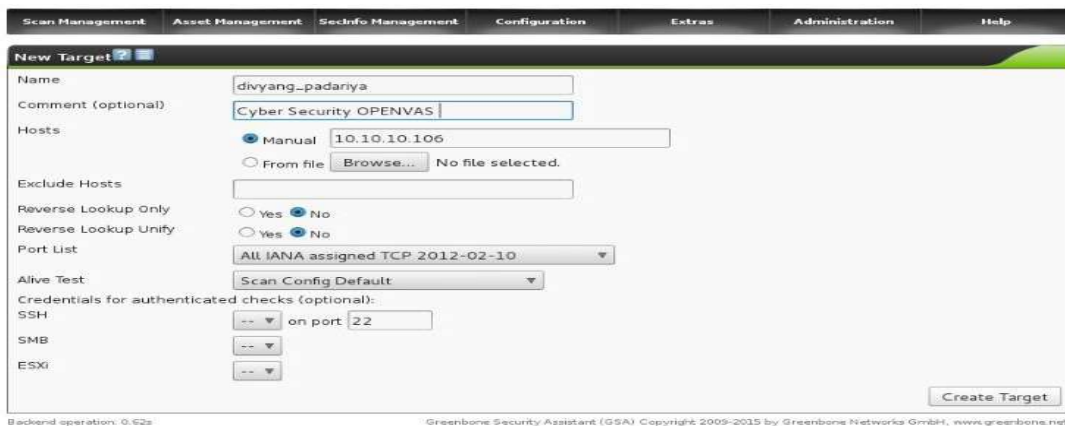
- Now go to Configuration > Targets



- Now Click On New Target As shown in Bellow Figure.



- Now Insert Details Which will required for target and then Click on "Create Target".



- After Creating Target You Will Found following page which shows all the details about created target

Greenbone Security Assistant Logged in as Admin admin | Logout
Sun Oct 11 12:32:09 2015 UTC

Scan Management | Asset Management | SecInfo Management | Configuration | Extras | Administration | Help

Target Details

Name: divyang_padariya
Comment: Cyber Security OPENVAS
Hosts: 10.10.10.106
Exclude Hosts:
Reverse Lookup Only: No
Reverse Lookup Unify: No
Maximum number of hosts: 1
Port List: All IANA assigned TCP 2012-02-10
Alive Test: Scan Config Default
Credentials for authenticated checks:
SSH:
SMB:
ESXi:

ID: e81941a5-f39c-470e-ac92-5863c109900f
Created: Sun Oct 11 12:32:09 2015
Last modified: Sun Oct 11 12:32:09 2015
Owner: admin

Tasks using this Target: None

User Tags for 'divyang_padariya': none

Backend operation: 0.88s Greenbone Security Assistant (GSA) Copyright 2009-2015 by Greenbone Networks GmbH, www.greenbone.net

- Now Go to Scan Management > Tasks and create a new task

Greenbone Security Assistant Logged in as Admin admin | Logout
Sun Oct 11 12:33:59 2015 UTC

Scan Management | Asset Management | SecInfo Management | Configuration | Extras | Administration | Help

Tasks 1 - 2 of 2 (total 2)

Name	Hosts	IPs	Port List	Credentials	Actions
divyang_padariya (Cyber Security OPENVAS)	10.10.10.106	1	All IANA assigned TCP 2012-02-10	SSH SMB ESXi	
localhost	localhost	1	OpenVAS Default		

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

Backend operation: 0.51s Greenbone Security Assistant (GSA) Copyright 2009-2015 by Greenbone Networks GmbH, www.greenbone.net


Tasks (total: 0) 1 - 2 of 2 (total 2)

Filter: **New Task**

apply_overrides=1 rows=10 first=1 sort=name

Name	Status	Reports	Severity	Trend	Actions
		Total	Last		

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

Welcome dear new user!
 To explore this powerful application and to have a quick start for doing things the first time, I am here to assist you with some hints and short-cuts.
 I will appear automatically in areas where you have created no or only a few objects. And disappear when you have more than 3 objects. You can call me with this icon  any time later on.
 If you want help creating new scan tasks but also more options, you can select "Advanced Task Wizard" from the wizard selection menu at the top of this window.

Quick start: Immediately scan an IP address
 IP address or hostname: **Start Scan**

For this short-cut I will do the following for you:

1. Create a new Target with default Port List
2. Create a new Task using this target with default Scan Configuration
3. Start this scan task right away
4. Switch the view to reload every 30 seconds so you can lean back and watch the scan progress

In fact, you must not lean back. As soon as the scan progress is beyond 1%, you can already jump into the scan report via the link in

[new_task&next=get_task&filter=apply_overrides=1 rows=10 first=1 sort=name&filt_id=&token=a8ce6c2b-d667-4ea7-804e-fd14cf6a9](#)

- Now add details for create a new task and click on "Create Task"

New Task

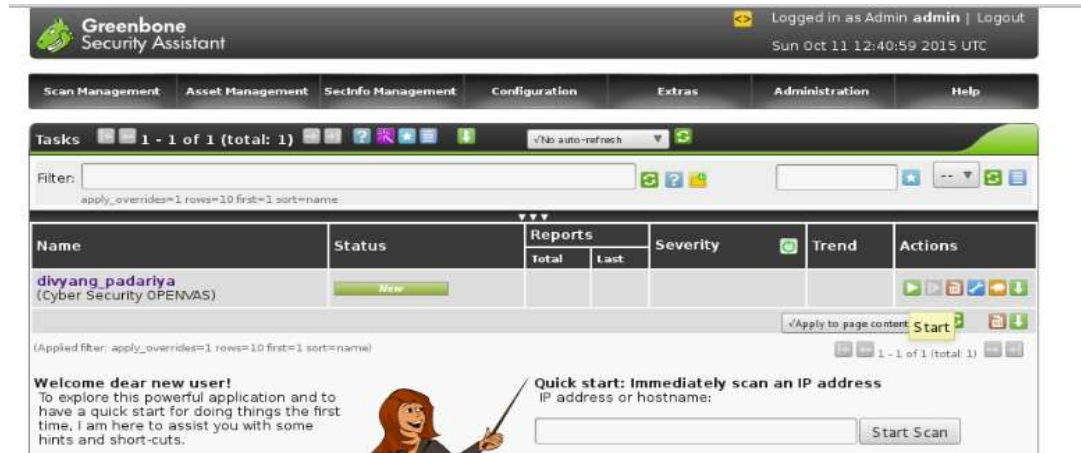
Name: divyang-padariya
Comment (optional): Cyber Security OPENVAS
Scan Targets: divyang-padariya
Alerts (optional): ☐ ☐ ☐
Schedule (optional): ☐ Once
Add results to Asset Management: ☒ yes ☐ no
Alterable Task: ☐ yes ☒ no

Scanner:

☒ OpenVAS Scanner
Scan Config: OpenVAS Default
Slave (optional): Full and fast ultimate
Network Source Interface:
Order for target hosts: Sequential
Maximum concurrently executed NVTs per host: 4
Maximum concurrently scanned hosts: 20

Create Task

- After Creating New Task Go to the Tasks



- Now Click on Start Button in "Actions" and by clicking on the start button Status change from "New" to "Requested".



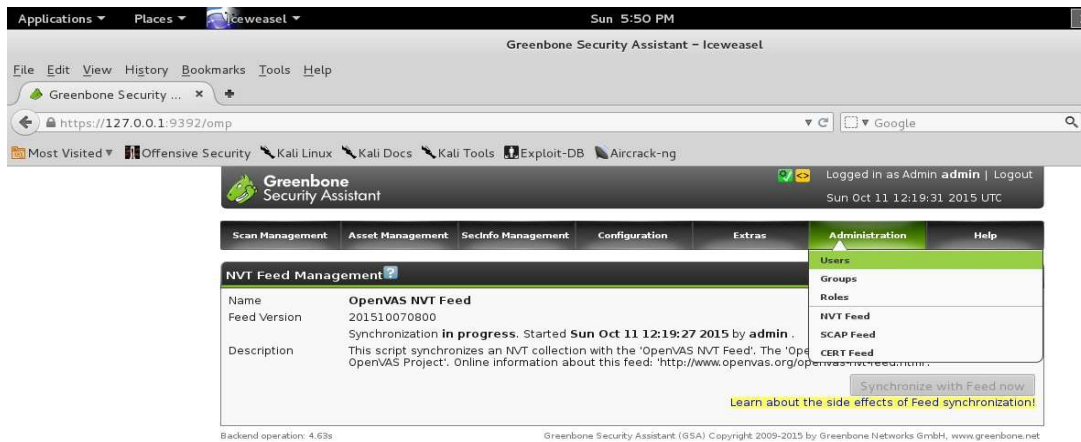
- Now as shown in above picture click on dropdown list and select "Refresh every 30 sec" which will refresh the status of scanning on every 30 seconds.
- After Completion of 100% scanning it shows "Done" status in Status portion.



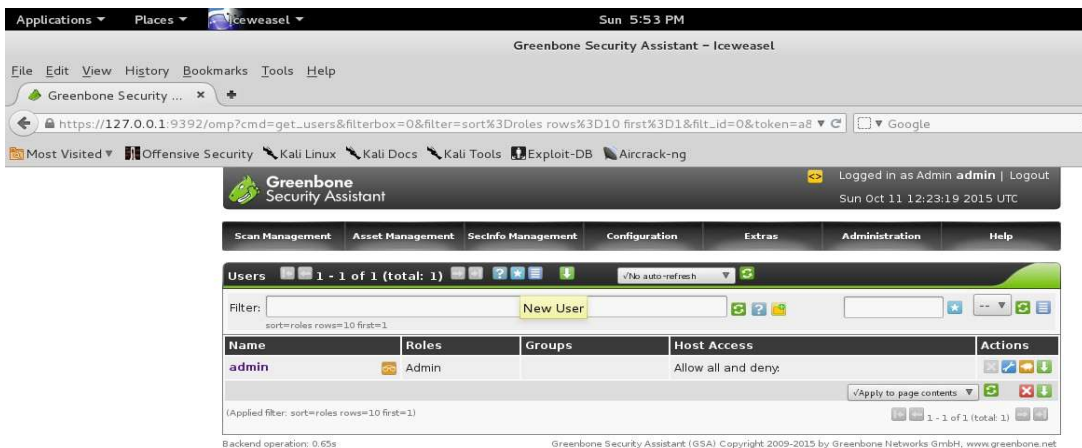
- Now as shown in Bellow picture we can see the details of scanning and we can also download generated report in various format.



- We can also create new User in open vas by following bellow pictures.
- Goto Assministration > users.



- Now Click on new User and fill details of new user.



- By clicking on Create User new user created.

