NEST Kali Linux Tutorial: OpenVAS

“The world's most advanced Open Source vulnerability scanner and manager”

Catherine Zittlosen

November 2013

http://openvas.org/

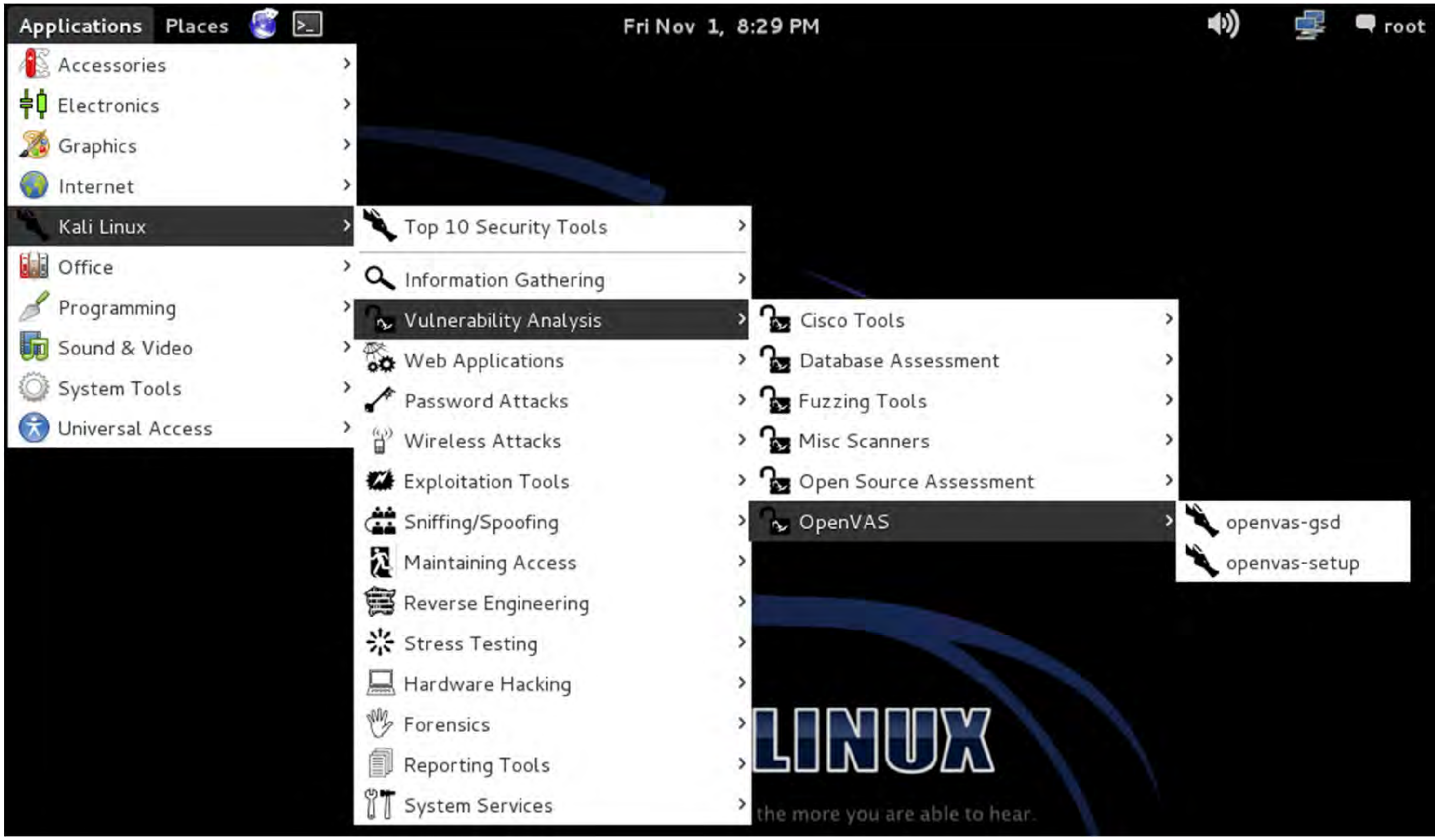
UNM CENTER *for* INFORMATION ASSURANCE RESEARCH *and* EDUCATION (CIARE)

Introduction

- OpenVAS is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution.
- If you are a Sysadmin, IT Manager or Security Manager, you need to protect your network. You need to know where your weaknesses are, so that you can put together a plan to fix them.

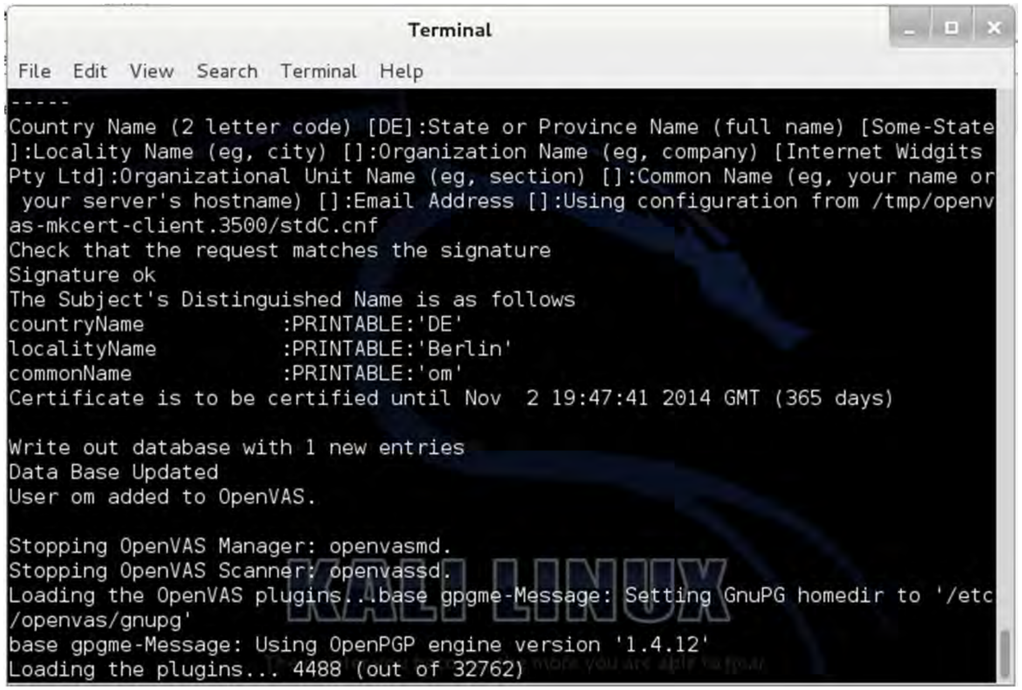
OpenVas Setup

- Applications > Kali Linux > Vulnerability Analysis > OpenVAS > openvas-setup



Download Plugins

- OpenVAS will now download all the required plugins (this will take a few minutes)

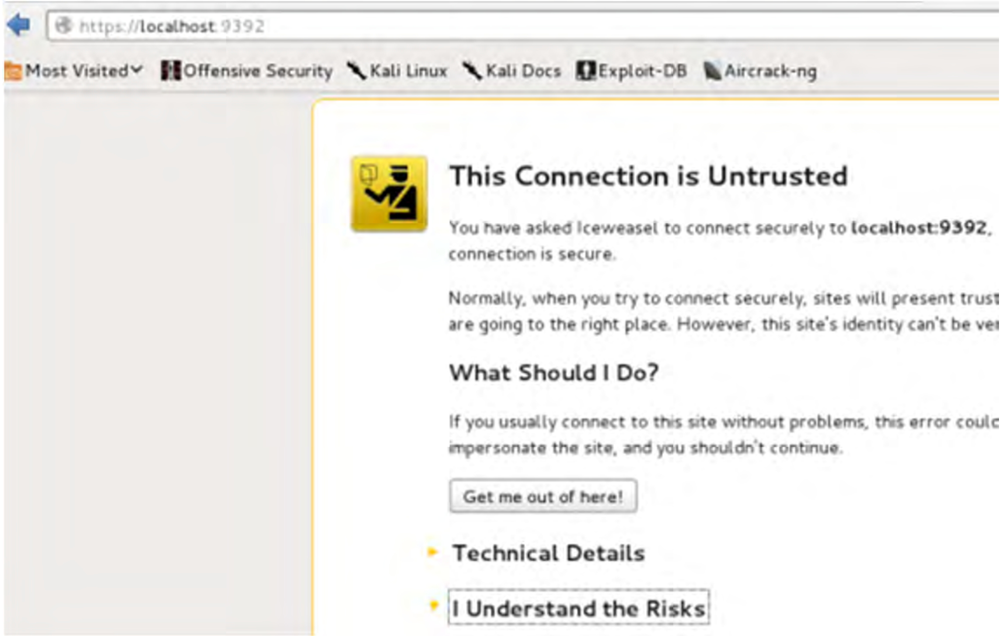


```
-----
Country Name (2 letter code) [DE]:State or Province Name (full name) [Some-State
]:Locality Name (eg, city) []:Organization Name (eg, company) [Internet Widgits
Pty Ltd]:Organizational Unit Name (eg, section) []:Common Name (eg, your name or
 your server's hostname) []:Email Address []:Using configuration from /tmp/openv
as-mkcert-client.3500/stdC.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'DE'
localityName          :PRINTABLE:'Berlin'
commonName            :PRINTABLE:'om'
Certificate is to be certified until Nov  2 19:47:41 2014 GMT (365 days)

Write out database with 1 new entries
Data Base Updated
User om added to OpenVAS.

Stopping OpenVAS Manager: openvasmd.
Stopping OpenVAS Scanner: openvassd.
Loading the OpenVAS plugins...base gpgme-Message: Setting GnuPG homedir to '/etc
/openvas/gnupg'
base gpgme-Message: Using OpenPGP engine version '1.4.12'
Loading the plugins... 4488 (out of 32762)
```

- The default user id is “admin”.
- Enter a password that you can remember.

Iceweasel Browser

- Applications > Internet > Iceweasel Web Browser
- Navigate to: https://localhost:9392
- Click “I Understand the Risks” and “Confirm Security Exception”



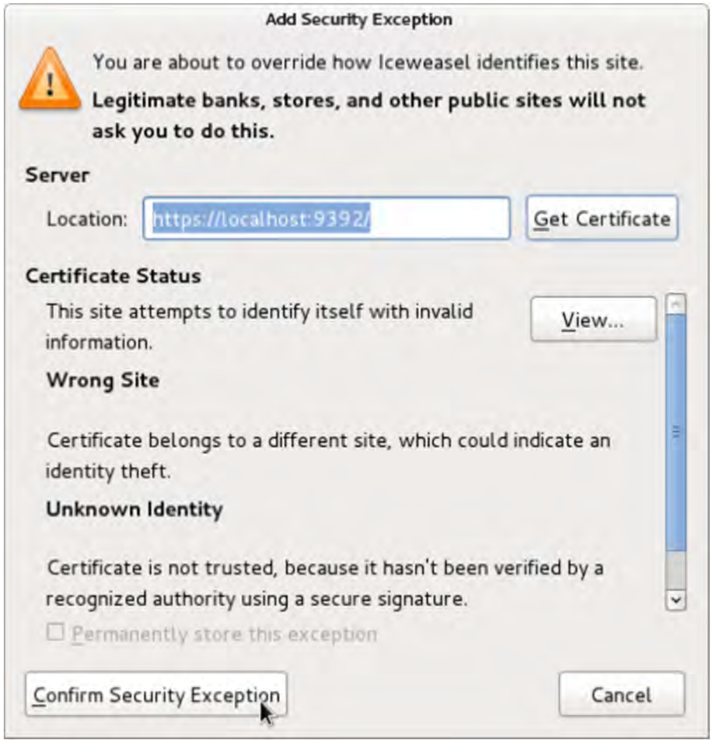
This Connection is Untrusted

You have asked Iceweasel to connect securely to **localhost:9392**, connection is secure.

Normally, when you try to connect securely, sites will present trust are going to the right place. However, this site's identity can't be ve

What Should I Do?

If you usually connect to this site without problems, this error coulc impersonate the site, and you shouldn't continue.



Add Security Exception

You are about to override how Iceweasel identifies this site.

Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://localhost:9392/

Certificate Status

This site attempts to identify itself with invalid information.

Wrong Site

Certificate belongs to a different site, which could indicate an identity theft.

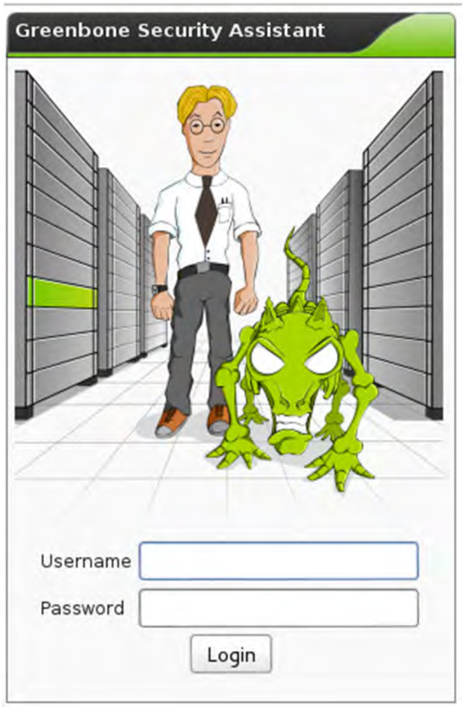
Unknown Identity

Certificate is not trusted, because it hasn't been verified by a recognized authority using a secure signature.

☐ Permanently store this exception

Login

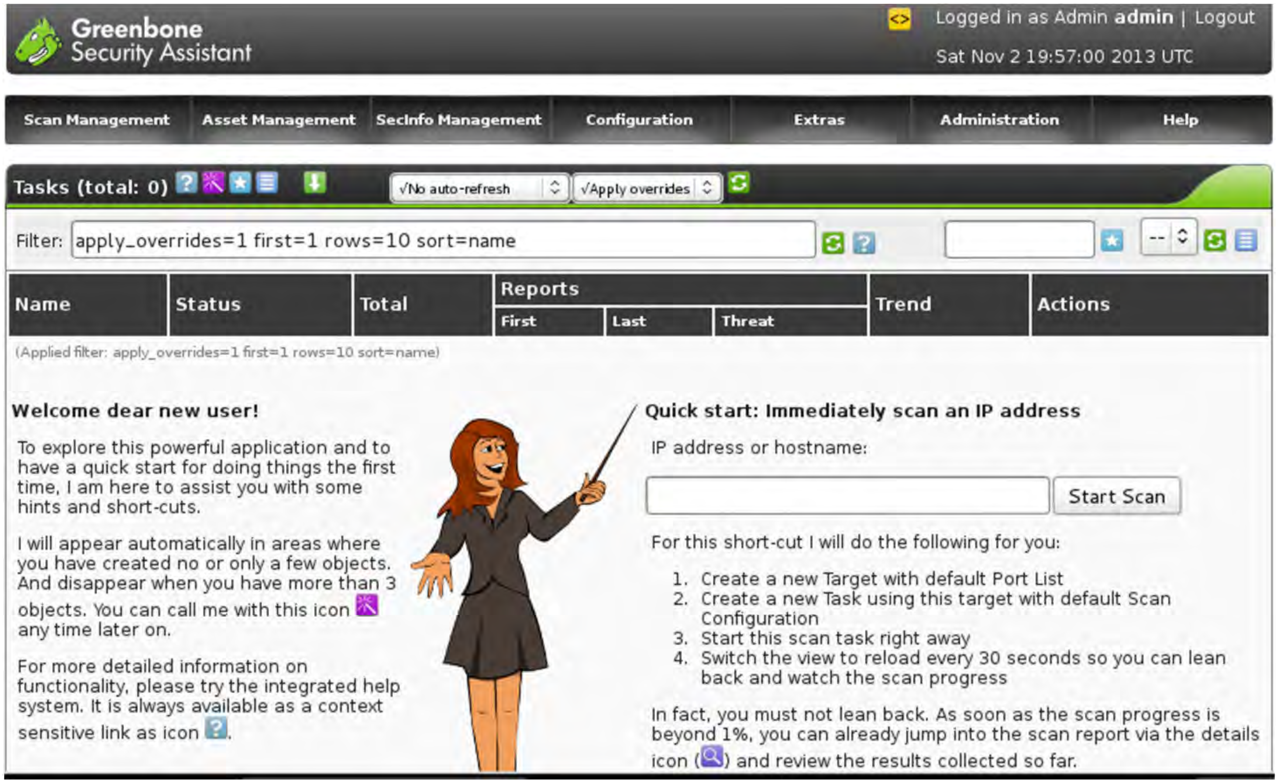
- Log into the OpenVAS web console.



- Default username = admin
- Password (whatever you entered during setup)

Web Console

- OpenVAS Security Assistant screen (Hermione Granger wizard appears)



Logged in as Admin **admin** | Logout

Sat Nov 2 19:57:00 2013 UTC

Tasks (total: 0)

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

Name	Status	Total	Reports			Trend	Actions
			First	Last	Threat		

(Applied filter: apply_overrides=1 first=1 rows=10 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.

For more detailed information on functionality, please try the integrated help system. It is always available as a context sensitive link as icon ?.

Quick start: Immediately scan an IP address

IP address or hostname:

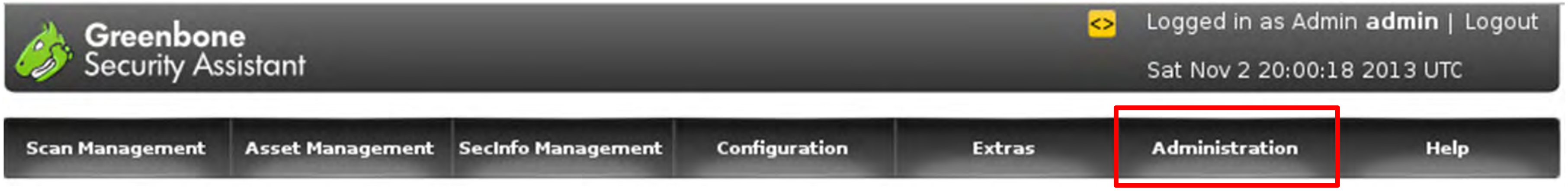
For this short-cut I will do the following for you:

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 details icon (🔍) and review the results collected so far.

Update Database Feeds

- Within the OpenVAS web console, go to:
  - Administration > NVT Feed > Synchronize with Feed now



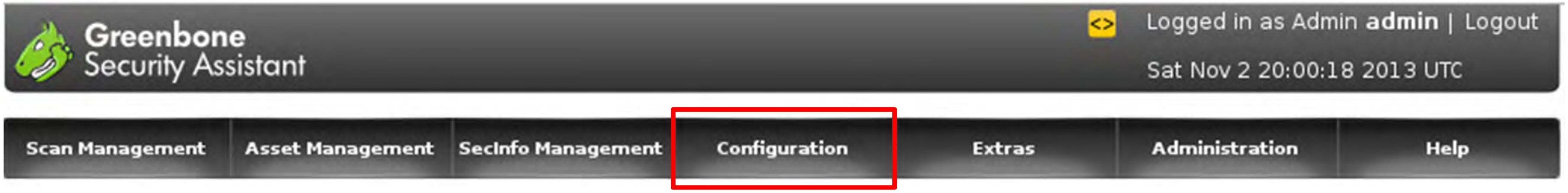
- This step is critical. If you do not update the vulnerability database feeds, it will generate errors later on.

Update Database Feeds

- Repeat for the other database feeds:
  - Administration > SCAP Feed (these are xml files for the reports)
  - Administration > Cert Feed

Update Database Feeds

- Within the OpenVAS web console, go to:
  - Configuration > Targets



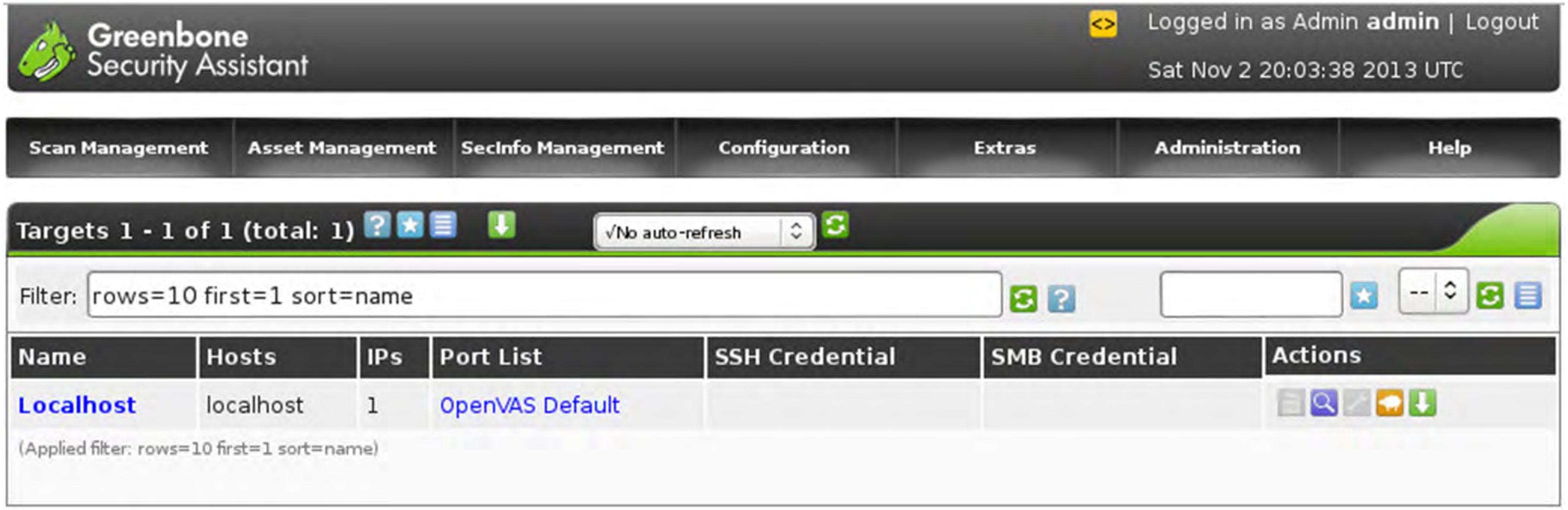
Greenbone Security Assistant

Logged in as Admin **admin** | Logout

Sat Nov 2 20:00:18 2013 UTC

Set Targets

- Localhost will be there by default.
- Scan your XP VM as well (192.168.0.101)



Logged in as Admin **admin** | Logout

Sat Nov 2 20:03:38 2013 UTC

Targets 1 - 1 of 1 (total: 1)

√No auto-refresh

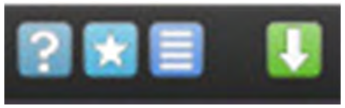
Filter: rows=10 first=1 sort=name

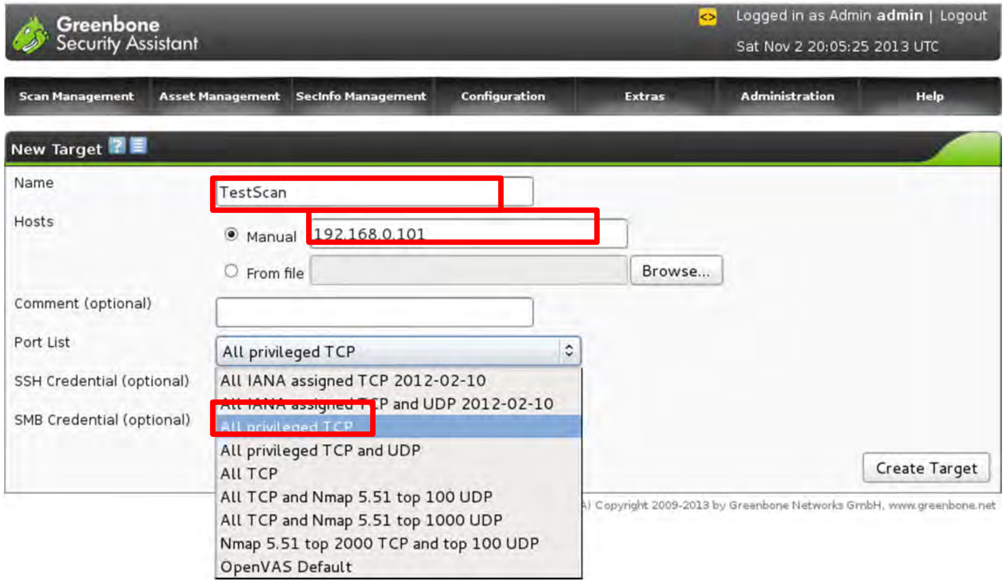
Name	Hosts	IPs	Port List	SSH Credential	SMB Credential	Actions
Localhost	localhost	1	OpenVAS Default			

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

Add Target

- Click on the blue box with a white star to add a new target.





Greenbone Security Assistant
Logged in as Admin admin | Logout
Sat Nov 2 20:05:25 2013 UTC
Scan Management
Asset Management
SecInfo Management
Configuration
Extras
Administration
Help

New Target

Name: TestScan

Hosts: ● Manual 192.168.0.101

○ From file Browse...

Comment (optional):

Port List: All privileged TCP

- All IANA assigned TCP 2012-02-10
- All IANA assigned TCP and UDP 2012-02-10
- All privileged TCP
- All privileged TCP and UDP
- All TCP
- All TCP and Nmap 5.51 top 100 UDP
- All TCP and Nmap 5.51 top 1000 UDP
- Nmap 5.51 top 2000 TCP and top 100 UDP
- OpenVAS Default

SSH Credential (optional)

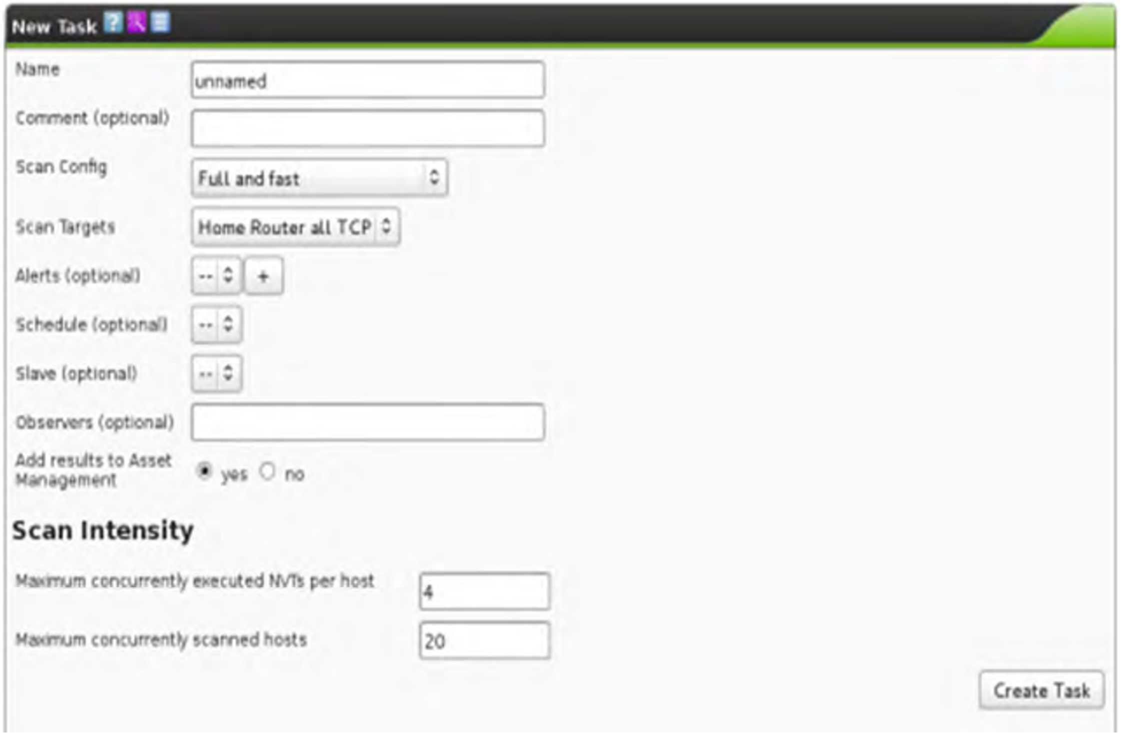
SMB Credential (optional)

Create Target

- Enter name, IP address (192.168.0.101), and port options (all privileged TCP)
- Click “Create Target”

Create Task

- Go to Scan Management > New Task



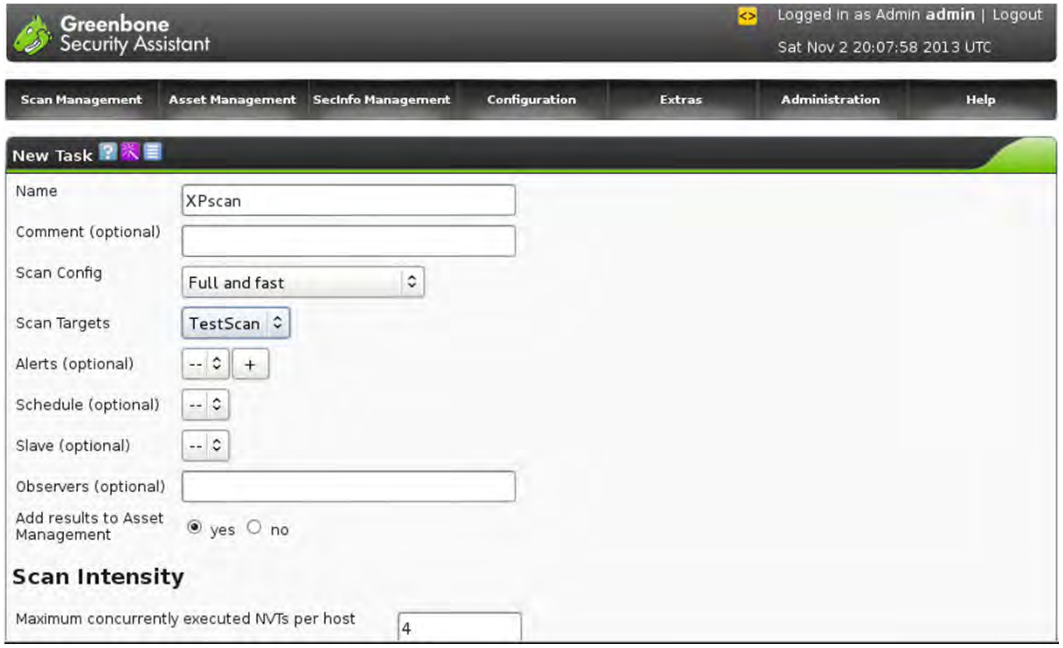
Name	unnamed
Comment (optional)	
Scan Config	Full and fast
Scan Targets	Home Router all TCP
Alerts (optional)	-- +
Schedule (optional)	--
Slave (optional)	--
Observers (optional)	
Add results to Asset Management	● yes ○ no

Scan Intensity

Maximum concurrently executed NVTs per host	4
Maximum concurrently scanned hosts	20

Task Settings

- Name the task whatever you want - eg. XPscan
- Scan Config should default to “Full and Fast”
- Select your XP machine as your scan target
- Click “Create Task”



New Task

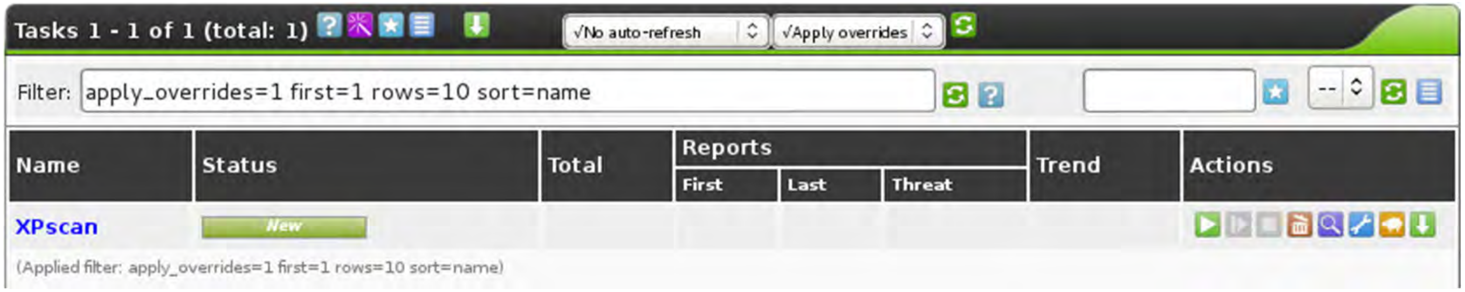
Name	XPscan
Comment (optional)	
Scan Config	Full and fast
Scan Targets	TestScan
Alerts (optional)	-- +
Schedule (optional)	--
Slave (optional)	--
Observers (optional)	
Add results to Asset Management	● yes ○ no

Scan Intensity

Maximum concurrently executed NVTs per host	4

Run Task

- The new task should show up with a green bar that says “New”



Tasks 1 - 1 of 1 (total: 1)

√No auto-refresh

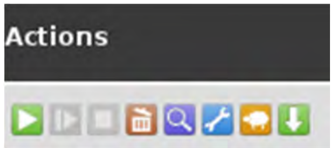
√Apply overrides

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

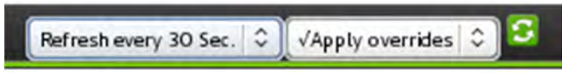
Name	Status	Total	Reports			Trend	Actions
			First	Last	Threat		
XPscan	New						

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

- Click the green arrow to run this new task.



- To watch the scan live, Set the “No auto-refresh” dropdown box to “Refresh every 30 Sec.”

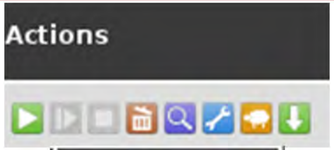


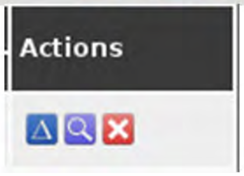
Refresh every 30 Sec.

√Apply overrides

- The scan should take a few minutes to complete.

Report





- Click on the purple magnifying glass
- Scroll down and click on it again.
- On “Full Report”, select “HTML” under “Download”
- Click the green arrow and open with Iceweasel
- Threats will be categorized as High, Medium, or Low.
- You can scroll down and review each vulnerability and the proposed solutions (if available).

References

- http://www.kalilinux.net/community/threads/tutorial-vulnerability-scanning-with-openvas.137/
- http://uwnthesis.wordpress.com/2013/08/31/kali-openvas-vulnerability-scanner-how-to-use-openvas-on-kali-debian-linux/