

Client Side Attacks (Contd)

Tools in Kali Linux

Module #24

Kali Linux: Nessus?

Nessus does not come pre-installed with Kali. You will need to obtain a registration code from Tenable to use Nessus. Tenable gives a home feed option, but is limited to scanning 16 IP addresses. If you would like to scan more IPs, you must purchase a professional feed from Tenable.

Nessus HomeFeed is available for non-commercial, personal use only. If you will use Nessus at your place of business, you must purchase Nessus ProfessionalFeed. To get an activation code for Nessus go to <http://www.tenable.com/products/nessus/nessus-homefeed>

Kali Linux: Nessus installation on Kali Linux?

1. Download Nessus for Debian. Go to the site <http://www.tenable.com/products/nessus/select-your-operating-system> to download Nessus for Debian 64-bit.
2. Go to the directory where you downloaded Nessus and issue the following commands:
ar vx Nessus-5.2.1-debian6*
tar -xzvf data.tar.gz
tar -xzvf control.tar.gz

There will now be an etc directory and an opt directory.

Kali Linux: Nessus installation on Kali Linux?

3. Copy the nessus directory in /tmp/opt/ to the /opt directory; make the /

opt directory if it doesn't exist. Issue the following commands:

mkdir /opt (You may get an error stating the /opt directory exists however, move to the next command).

```
cp -Rf /<installed folder>/opt/nessus /opt
```

```
cp -Rf /<installed folder>/etc/init.d/nessus* /etc/init.d
```


4. You can delete the contents of the Nessus download from the /tmp directory.

5. To start Nessus, issue the following command:

```
/etc/init.d/nessusd start
```

6. Log onto the Nessus management interface. Open a browser and navigate to <https://127.0.0.1:8834> .

Kali Linux: Using Nessus

 Nessus

Initial Account Setup

First, we need to create an admin user for the scanner. This user will have administrative control on the scanner; the admin has the ability to create/delete users, stop ongoing scans, and change the scanner configuration.

Login:

Password:

Confirm Password:

Because the admin user can change the scanner configuration, the admin has the ability to execute commands on the remote host. Therefore, it should be considered that the admin user has the same privileges as the "root" (or administrator) user on the remote host.

Registration

When a new vulnerability is discovered and released into the public domain, Tenable's research staff ("plugins") that enable Nessus to detect their presence. The plugins contain vulnerability information to test for the presence of the security issue, and a set of remediation actions. To use Nessus, you must subscribe to a "Plugin Feed" to obtain an Activation Code.

Activation Code

Activation Code:

Kali Linux: Nessus usage?

Once all the updates have been downloaded and initialized, you will be presented with the login screen. Use the username and password you set up during the initial installation.



Kali Linux: Using Nessus

New Scan

Scan Title

CloudCentrics

Scan Type

Run Now

Scan Policy

External Network Scan

Scan Targets

www.cloudcentrics.com

Upload Targets

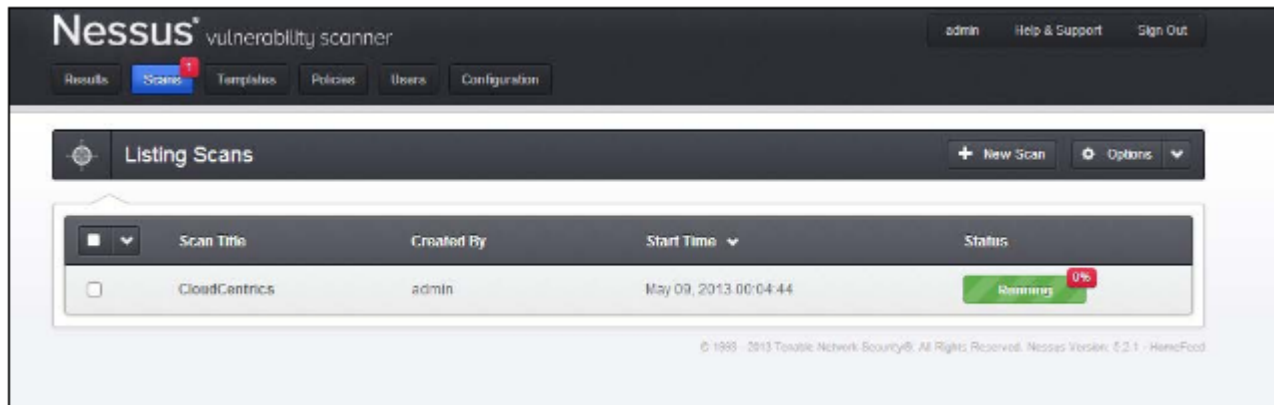
Choose File

No file chosen

Create Scan

Cancel

Kali Linux: Using Nessus

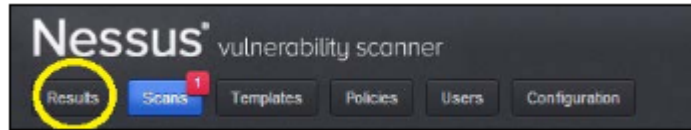


The screenshot displays the Nessus vulnerability scanner web interface. At the top, the header includes the 'Nessus' logo and 'vulnerability scanner' text. Navigation tabs for 'Results', 'Scans', 'Templates', 'Policies', 'Users', and 'Configuration' are visible, with 'Scans' being the active tab. User links for 'admin', 'Help & Support', and 'Sign Out' are in the top right. The main content area is titled 'Listing Scans' and features a '+ New Scan' button and an 'Options' dropdown. Below this is a table with the following columns: a checkbox, 'Scan Title', 'Created By', 'Start Time', and 'Status'. One scan is listed: 'CloudCentrics' created by 'admin' on 'May 09, 2013 00:04:44'. The status is 'Remaining' with a green progress bar and a red '0%' indicator. A copyright notice at the bottom reads: '© 1999 - 2013 Tenable Network Security®. All Rights Reserved. Nessus Version: 5.2.1 - Hameed'.

	Scan Title	Created By	Start Time	Status
<input type="checkbox"/>	CloudCentrics	admin	May 09, 2013 00:04:44	Remaining 0%

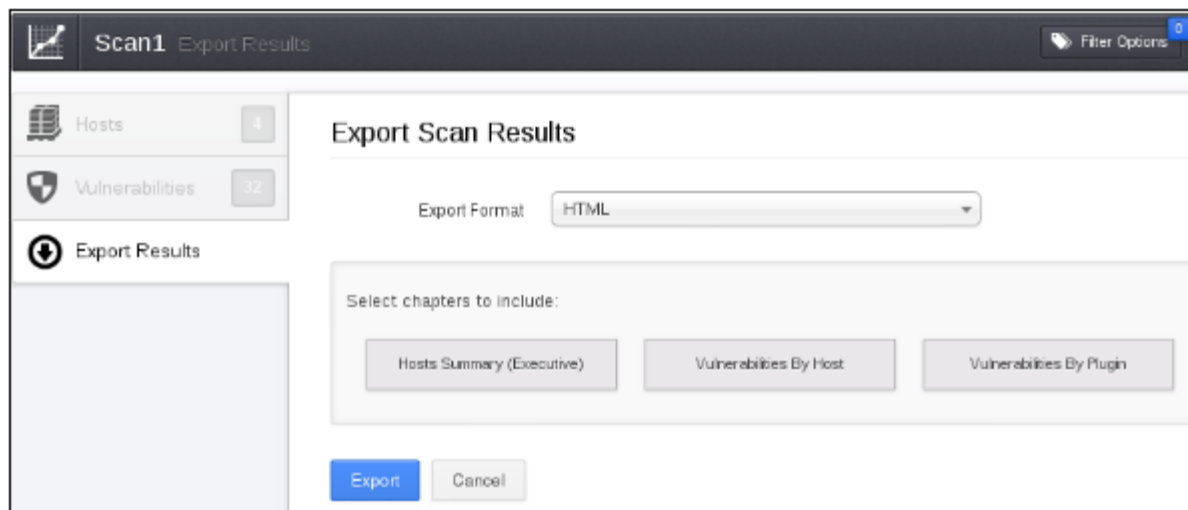
Kali Linux: Nessus usage?

After the scan is completed, the results can be viewed by clicking on the Results tab. This will provide the administrator a report of what Nessus found.



	Results Title	Last Updated	States
<input type="checkbox"/>	Internal_web	May 09, 2013 00:13:23	Completed ✕
<input type="checkbox"/>	securityblogger.com	May 09, 2013 00:12:20	Running
<input type="checkbox"/>	CloudCentrics	May 09, 2013 00:04:44	Running

Kali Linux: Nessus usage?



Nessus Export Scan

Kali Linux: Nessus usage?

Vulnerability Summary			Sort Options	Filter Vulnerabilities
critical	MS04-022: Microsoft Windows Task Scheduler Remote Overflow	Windows	1	
critical	MS05-027: Vulnerability in SMB Could Allow Remote Code Execu...	Windows	1	
critical	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code	Windows	1	
critical	MS05-007: Microsoft Windows Server Service Crafted RPC	Windows	1	
critical	MS03-026: Microsoft RPC Interface Buffer Overrun (82060) (a...	Windows	1	
critical	MS03-039: Microsoft RPC Interface Buffer Overrun (82414) (a...	Windows	1	
critical	MS04-007: ASN.1 Vulnerability Could Allow Code Execution (82...	Windows	1	
critical	MS04-011: Security Update for Microsoft Windows (825732)	Windows	1	
critical	MS04-012: Cumulative Update for Microsoft RPC/DCOM (825741)	Windows	1	
critical	MS05-040: Vulnerability in Server Service Could Allow Remote...	Windows	1	
critical	MS05-043: Vulnerability in Printer Spooler Service Could All...	Windows	1	
high	MS06-035: Vulnerability in Server Service Could Allow Remote...	Windows	1	
high	MS02-045: Microsoft Windows SMB Protocol	Windows	1	
medium	MS05-007: Vulnerability in Windows Could Allow Information D...	Windows	1	
medium	Microsoft Windows SMB NULL Session Authentication	Windows	1	
medium	SMB Signing Disabled	Mac	1	

Thank You