

Information security - IV
Prof. Vasan
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Module - 24
Lecture - 24
Client Side Attacks-Tools in Kali Linux


So, in this session we are going to continue seeing few more tools that is typically used with a penetration tester for doing the client side attack.

(Refer Slide Time: 00:24)

[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>



So, the tool that we are going to look at is what is called as a Nessus. So, Nessus does not come by default typically pre installed with Kali Linux ah; we can actually obtain Nessus and install it as part of Kali Linux. Because this is something that is available for download from the promoters of Nessus called as a Tenable right. So, they basically give you home feed option, which could potentially scan up to 16 IP addresses and if at all the tester would need to scan more than 16 IP addresses, they could actually buy a professional license from the Tenable organization.

This particular tool is actually available for non commercial personal use and you could actually get an activation code; if one wants to purchase by going into this particular site in Tenable dot com. And get an activation code after which it could basically be working without any kind of restrictions on how many IP addresses it could scan.


(Refer Slide Time: 01:32)

[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.



What exactly does this tool? So, this tool is basically a tool that is typically used for a scanning a particular target device. So, now when we say scanning; what exactly is done is that before that particular target could be actually attacked with certain kind of an exploits or whatever mechanism that one is adopting; the attacker should basically come to know what are all the details of that particular target right.

So, what is it that is required is that what platform it is running; that is basically what operating system is running, what version of that operating system it is actually running? Other than that what kind of software applications are installed on that? And what are the versions of those software applications? Right because just imagine the that either with this tool with some other mechanism; the person who is actually trying to attack a particular target system has these details right ah

As we were discussing this some of our earlier tools once this combination is know that is what is a operating system running on that particular target what kind of what is a operating system version ah? So, if I basically say it is Ubuntu; Linux the moment I know it is 14.04 or 16.04 and I also come to know what are the applications that is running.

So, for example, samba is running on that particular Ubuntu server and I know what is the samba version let us say version 3.2.0 a very very quick search is what is required to determine what are all the vulnerabilities that are present in samba version 3.2.0 running

on Ubuntu Linux version 16.04 right, then it becomes easily become very easy for the attacker to find out what vulnerabilities are there which could potentially be exploited by some tool like a metasploit or whatever it is right.


So, this tool is actually going to be helping one to identify what kind of software applications are running on a particular targeted system. So, I could actually download the tool from this particular site. So, I could easily download for debian 64 bit or for some of the other flavours of Linux also. But because we are going to be actually using it on Kali Linux and Kali Linux is a debian distribution is a is a derivative from debian distribution; we would actually take this particular distribution and this particular version of the Nessus for debian and download it right. So, once we download this we a basically get two different compressed tar a ball images. So, one is what is called as data and another what is called as control right.

So, these two things are extracted using the tar command. So, if I use x zvf option directly with g zip file; the gnu tar will directly do and uncompressal of it and also extract the contents from the tar in one shot right. So, these two compressed g zipped tar files are basically uncompressed and un tar and it will basically now, have a etc and a opt directory right.

(Refer Slide Time: 05:00)

[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>.



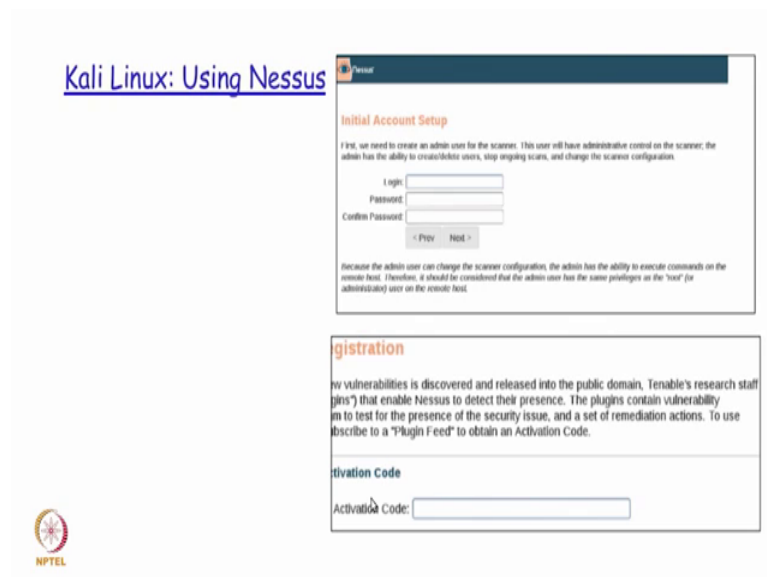
So, we basically move all the contents of the opt directory contents that is there into slash opt and whatever god created under etc init dot d Nessus as part of that directory into the

directory etc init dot d. Suppose in that particular system by any chance opt directory is not there.

So, this has got to be created first, but if this directory is already present ah; if you do a make the opt, make the slash opt; it will just report you that this particular directory is already existing. So, in this case this error could be ignored without a really taking that into consideration. So, after that the demon service has to be actually started Nessus the start.

And once it is actually started it will actually be running on the port number 8834 on the local host. So, one could access in the browser with this URL https colon double slash 127 dot 0 dot 0 dot 1 colon 8834 right.

(Refer Slide Time: 06:07)

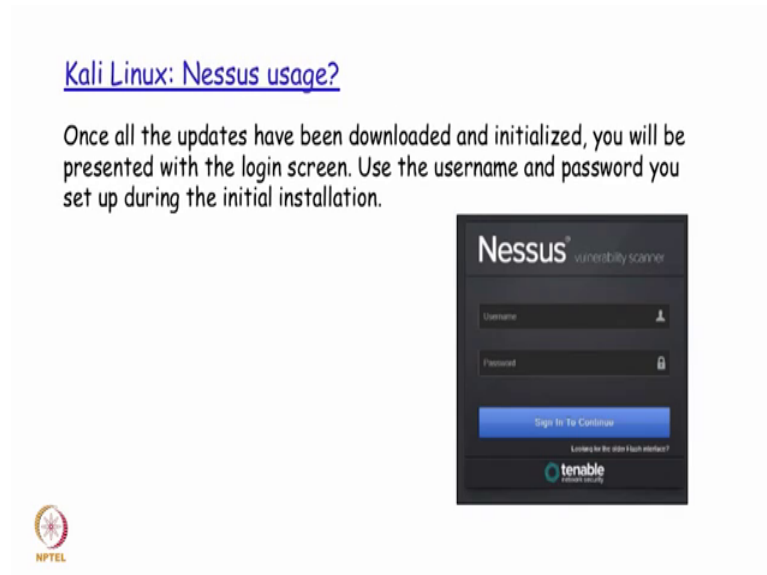


So, this will throw open the management interface; in which I could actually do lot of things like trying to create initial account. So, this account will be the account that will actually have administrative control. So, and also give the password and confirm the password as well right. So, once this is actually done if at all the user wants to do a registration.

So, the activation code could also be given as part of the registration process. So, that all kinds of limitations that is there in the free version will not be applicable in your installation right. But if your requirement is hardly less than 16 IP addresses that you

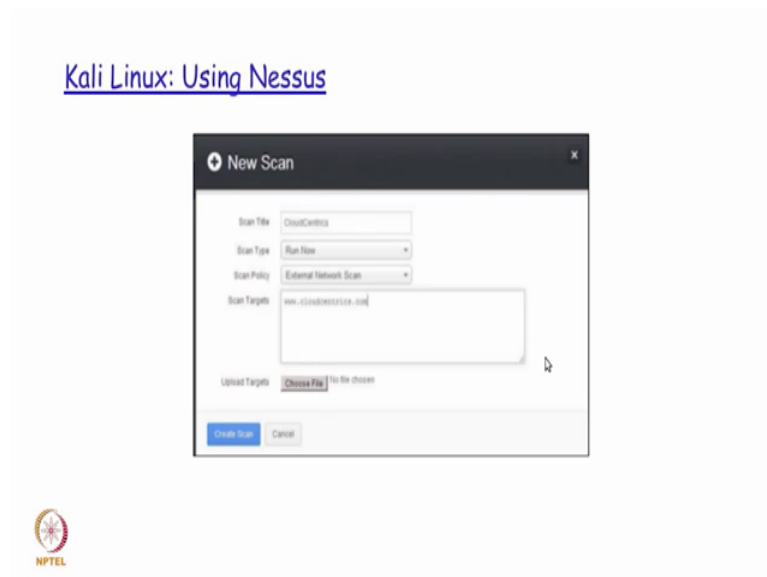
would potentially be scanning, then you could actually use the free feed itself instead of actually trying to buy a professional feed version getting activation code and then doing a activation of that.

(Refer Slide Time: 06:55)



So, once this is actually created then the login screen whatever is created user name password has to be entered.

(Refer Slide Time: 07:09)



And then it has to be actually locked then before one could actually start using that right. Now if the first way by; which the stool would actually be made use of is to do a new

scan. So, the new scan will actually be done on a particular URL; so, that URL is actually a specified here as part of the scan target textbox field. And I also have an option to give a meaningful title for me to easily referred to it later. And I could also say whether I want to run it now or schedule it in future right. Now the scan policy is whether it is an external network scan or internal network scan ah; based on that appropriate policies will actually have to be used by the tool.

So, instead of also specifying the URL target; I could also have a file that could actually be uploaded which should be containing the targets that needs to be scanned one after the other in each line within that file right. So, the file also could be used by to be given as an input by choose by choosing the file and in pressing this button and choosing the file instead of specifying the URLs as part of this targets field right.

(Refer Slide Time: 08:26)



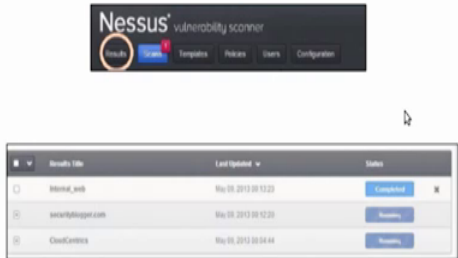
So, when this is done? We are going to create the scan and the scan will basically be giving a status report when it is actually running. Because depending on the complexity of that particular scan and what we were asking it to do; it could potentially take any amount of time.

So, this will basically list down that this particular scan is currently running or it has got completed or whatever it is.

(Refer Slide Time: 08:49)

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.



The screenshot shows the Nessus vulnerability scanner interface. At the top, there is a navigation bar with the following tabs: Results, Scans, Templates, Policies, Users, and Configuration. Below the navigation bar, there is a table with the following columns: Scan's Title, Last Updated, and Status. The table contains three rows of scan results:

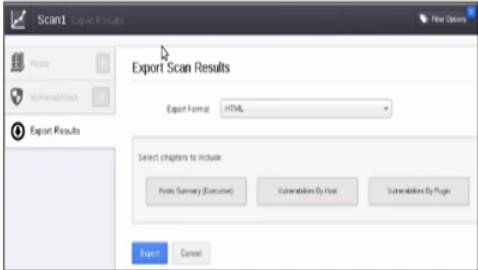
Scan's Title	Last Updated	Status
Internet_web	Thu 08 2013 09 12:23	Completed
www.kali.org.com	Thu 08 2013 09 12:23	Running
CloudControl	Thu 08 2013 09 04:44	Results

NPTEL

So, this will basically be a status tab that will say what is completed and what is currently running and after the scan is completed the results that can be viewed by clicking on the results tab.

(Refer Slide Time: 09:00)

Kali Linux: Nessus usage?



The screenshot shows the 'Export Scan Results' dialog box in the Nessus interface. The dialog box has a title bar that says 'Scan1 Export Results'. On the left side, there is a sidebar with the following options: Home, Vulnerabilities, and Export Results. The main area of the dialog box is titled 'Export Scan Results' and contains the following elements:

- An 'Export Format' dropdown menu set to 'HTML'.
- A 'Select chapters to include' section with three buttons: 'Vuln Summary (Executive)', 'Vulnerabilities By Host', and 'Vulnerabilities By Plugin'.
- 'Export' and 'Cancel' buttons at the bottom.

Nessus Export Scan

NPTEL

So, how does a results tab going to look like? So, it is basically going to say what is the format in which I want to have the report results displayed right? So, whether we wanted in html format or x format; whatever it is. And then may we say export, it is going to

basically export the entire set of results found out as part of the scan into the corresponding format that has been given.

(Refer Slide Time: 09:25)



So, if you see here; so, this is one example of the report that is getting printed out of the tool right. Now the different vulnerabilities that they are getting displayed here for example, if you see right; so, Microsoft, Windows; SMB vulnerabilities remote code; so, if I know this particular vulnerability is present. And it also tries to mark the category of that a vulnerability as per its own classification right.

So, anything marked as a critical would essentially mean that this is something which has to be addressed immediately or the penetration tester could easily make use of this as an entry point into this particular system right. So, the moment the penetration tester gets a result saying for example, these many critical vulnerabilities are there; the penetration tester will know that moment this particular vulnerability.

For example, the Microsoft windows assembly vulnerabilities remote code is present on this particular server what is that corresponding metasploit payload that; he has to run to exploit this particular vulnerability right. So, this is basically how a tool like Nessus would be potentially used by the penetration tester from a client machine to identify and determine what are all the vulnerabilities that are there; Because the moment he find what are the vulnerabilities that are there it is very easy and readymade information that is actually available for the penetration tester, wherein we will know exactly what exploit

to basically run using a tools something called as a metasploit that we saw earlier and exploit this particular vulnerability and get access into this particular system.

So, that is how a tool like Nessus which actually tries to find out what operating system, what version, what kind of software's are running on it? And including the version of the software helps the penetration tester to get the list of vulnerabilities which he could potentially make use of to penetrate into the system.

Thank you.