

Lab 4

CSCI6658-01 & Lab #4.1/4.2

Using Browser Exploitation to Take Over a Host’s Computer and Attack Webservers from the WAN

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TC-GitHub |  |  |  |  |

Table of Contents

1. [Executive Summary 2](#_Toc132133144)

[Lab 4.1](#_Toc132133145)

[LAB 4.2](#_Toc132133146)

[Objectives](#_Toc132133147)

1. [Lab Description Details 2](#_Toc132133148)

[Procedure](#_Toc132133149)

[LAB 4.1](#_Toc132133150)

[LAB 4.2](#_Toc132133151)

1. [Supporting Evidence 4](#_Toc132133152)

[LAB 4.1](#_Toc132133153)

[LAB 4.2](#_Toc132133154)

1. [Conclusion & Wrap-Up 17](#_Toc132133155)

[Summary with observations, Success & Failures, Challenges](#_Toc132133156)

# Executive Summary

## Lab 4.1

Within the lab the method of breaching a host computer through a browser exploit will be executed for the testing of vulnerabilities within a systems defense. A report will be written to ensure these get fixed and patched via a detailed breakdown and short breakdown of the process taken to enact this and the results along with how to fix these issues and what protocols they could.

## LAB 4.2

Within this lab you will mount an attack on a web server from the wide area network (WAN) with a kali Linux attack machine and then utilize the Microsoft remote desktop connection (RDP) to connect to the victim’s machine once they are exploited with a vulnerability.

## Objectives

Lab 4.1

* Use the Metasploit tool to exploit the browser vulnerability.
* Utilize a spear phishing attack to track a user into launching the web browser with the vulnerability within, to gain access to the host computer.
* Gaining Access to the host machine using this vulnerability and accessing the flags to demonstrate what one can access with the vulnerability.

Lab 4.2

* Use nmap and zenmap to scan the WAN and then utilize the bruter tool to exploit SMTP by a brute force attack.
* Once brute forced utilize credentials recovered to enter the credentials to access the Remote desktop protocol and then deface a website
* Make sure to cover tracks on the hacks that you have performed.

# Lab Description Details

## Procedure

## LAB 4.1

* First begin by opening the windows attack machine and proceed to the command prompt.
* Proceed to run a nmap on 203.0.113.100 and after successful confirmation of the ports in *Figure 1* below.
* After nmap is run go through zenmap and run an intense scan on the same ip address as listed above and sclick on the ports tab and identify the same ports as the picture are listed as well.
* After closing the applications and access bruter and begin a brute force attack on the ip address 203.0.113.100 with the username set to administrator and then where the dictionary is selected and browse local files and select the wordlist folder.
* Following this you need to extract the dark comment file to the folder dark comet and launch the darkcomet.exe
* Retrieve the first flag within this folder by clicking on the flag3.
* The darkcomet.exe will ask to access the firewall allow for it to access it once inside of the application click the listen but and listen on port 443 access the full editor in the menu
* And click on the network settings, in order to create a new stip with the IP/DNS field being 175.45.176.200 and selecting port 443 add it and navigate to the custom icon and select the Firefox logo
* Following navigate to the stub finalization tab and select UPX nand save it to the desktop of your virtual machine.
* After create a copy of the firefox and then navigate to the cmd and type in the mstsc once the remote desktop protocol opens write in the fillowing ip address 203.0.113.100 log in with the credentials administrator and P@ssw0rd after paste the firfox package generated by you in darkstar and click on it on the windows server
* After The connection will appear in the darkcomet program as 1 user, double click on that user and then navigate to the system info page and then select the computer information tab (be sure to refresh on the bottom of the window)
* Click on the files manager and navigate to explorer files once in a window will open where the attacker (you) are on the left and the victim is on the right, click on the victims c drive and navigate to the share folder and enter the death start folder
* Once inside the deathstar folder select all of the blueprint images for the deathstar and open up your c drive and navigate to the users public and then documents and then select the receive button to copy the files over to your machine
* After verifying they are there by hitting the refresh button on the bottom of the window

## LAB 4.2

* Begin by selecting the windows 8.1 attack machine with the external address of 175.45.176.200, once inside the attack machine open the cmd shortcut and then type in the command nmap ww.campus.edu
* Take note of the sample flag that is listed in there then type in zenmap and launch into the graphical user interface of zenmap within the target type www.campus.edu and hit scan.
* Take note of the many Microsoft services that are running and then select scan within the top right of zen map and then exit the program once exited type exit in the command prompt.
* Double click the bruter.exe program on the desktop and then set the target as www.campus.edu within the protocol drop down box select SMTP, then select the option box next to it and set the authentication to LOGIN and the domain to campus.edu and in the user type administrator after go to the dictionary selection and select browse, navigate to the local disk and find the wordlist.txt file and open it to select this for the brute force attack
* Start the attack and then wait, take note of the Bruter cycle and go to the testing tab to see all the passwords it is testing go back to the result tab to discover the user’s password P@ssw0rd. s
* Run bruter with the same parameters as before except the user replace with flag3 and then begin the brute force attack to get access to the flag for that users account.
* Now to alter the website double click on the iexplore shortcut and then in the URL type http://www.campus.edu then hit enter now that you are on the page it should display Windows 2008 Internal Server exit out and then go back to the CMD prompt and type nmap www.campus.edu -p 3389.
* Within the url for campus.edu add a forward /flag3.txt it should look like http://www.campus.edu/flag3.txt
* Following this type in mstsc to begin the remote desktop session and within the computer box type in the www.campus.edu and then hit connect once prompted enter the passwords that you have cracked from the brute force attack (user: administrator, pass: P@ssw0rd and then click yes when prompted
* Once inside the windows server click on the start button and right click it and select the computer icon and double click on the xampp folder and then double click on the htdocs.folder and right click on the index.html folder and select open with and chose notepad
* Highlight Windows 2008 Internal Server in the index.html file and then type in Hacked Web Server
* When inside the index.html notepad scroll to the bottom to find the associated flag for this challenge
* From the notepad menu select file and then save to make sure the changes take effect, from the windows explorer menu bar select file and then close now minimize the remote desktop session and on your desktop double click on the iexplore shortcut on the desktop within the url type http://www.campus.edu and then press enter if message hasn’t changed refresh the page and then you will see the message typed within the index.html file Hacked Web Server then proceed to close out of the internet Explorer
* Now to cover the tracks click on the RDP connection that you have previously minimized and open the cmd prompt by clicking on the icon on the windows server desktop.
* Type in the following command net stop Apache2.2 and hit enter after the service has stopped type exit.
* Now click on the start in the bottom left and click on computer and open the local disk c:\, then double click and open the xampp folder and once again on the Apache folder, then navigate to the logs folder and double click to enter the folder and find the access.log file.
* Click on the flag files5.txt to retrieve the flag within the logs folder and within the access log scroll to discover flag 6 within the access log file.
* After opening the logs file highlight all the entries that have the IP address 174.45.176.200 now remove them using the cut option in the edit tool bar once you have deleted the text save the file and then exit
* After navigating back to the desktop of the windows server and double click on the command prompt shortcut and type in net start Apache2.2 to restart the service then proceed to type edit after service starts
* Open the firefox option on the desktop and then type in the URL 127.0.0.1 into the URL bar and verify once more that the website is still hacked close out of Firefox and click on the start button in the bottom left corner then click the arrow to log off the computer.

# Supporting Evidence

## LAB 4.1

Text

Description automatically generated

Figure 1

Graphical user interface, application

Description automatically generatedFigure 2

Graphical user interface, text, application, Word

Description automatically generatedFigure 3

Text

Description automatically generatedFigure 4

*Graphical user interface, application

Description automatically generated*

Figure 5

Graphical user interface, application

Description automatically generatedFigure 6

Figure 7

A picture containing diagram

Description automatically generated

Figure 8

Graphical user interface

Description automatically generated

Figure 9

Diagram

Description automatically generated with medium confidence

## LAB 4.2

Figure 10

Text

Description automatically generated

Figure 11

Text, calendar

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Figure 12

Graphical user interface

Description automatically generated

Figure 12

Graphical user interface, text, application

Description automatically generated

Figure 13

Graphical user interface, text, application, email

Description automatically generated

Figure 14

Graphical user interface, text, application

Description automatically generated

Figure 15

Text, letter

Description automatically generated

Figure 16

Graphical user interface, text, application, email

Description automatically generated

Figure 17

Graphical user interface, text, application

Description automatically generated

Figure 18

Text

Description automatically generated

Figure 19

A close-up of a document

Description automatically generated with medium confidence

Traces of 175.45.176.200 are removed from the log files

# Conclusion & Wrap-Up

## Summary with observations, Success & Failures, Challenges

To conclude this lab was successful in each of the task stated in the objective there was a successful implementation of the web server vulnerability and then intern affecting the target user to gain access to import documentation and copy it over to our machine using a web server exploit. This was another success in the alternate deployment of an exploit where SMTP is exploited and utilizing bruter with a wordlist to brute force attack the server there was successful retrieval of the user id and password. The user and password were successfully utilized to remote desktop into the windows server and then alter the text of the website. Along with this a successful clean up with no data left behind of the hack and successful logoff and completion. Overall, this lab was a success, allowing for the exploitation of the web service and then the SMTP service. Also allowing for practice with spear phishing attacks and how they can be effective in gaining access to a victim’s computer. The implementation of labs Using Browser Exploitation to Take Over a Hosts Computer and Attack Webservers from The WAN was a success.