

Lab 3

CSCI6658-01 & Lab #3.1/3.2

Crafting and deploying malware using a remote access trojan and performing a denial-of-service attack from the WAN

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

Table of Contents

1. [Executive Summary 2](#_Toc131179811)

[Lab 3.1](#_Toc131179812)

[LAB 3.2](#_Toc131179813)

[Objectives](#_Toc131179814)

1. [Lab Description Details 2](#_Toc131179815)

[Procedure](#_Toc131179816)

[LAB 3.1](#_Toc131179817)

[LAB 3.2](#_Toc131179818)

1. [Supporting Evidence 4](#_Toc131179819)

[LAB 3.1](#_Toc131179820)

[LAB 3.2](#_Toc131179821)

1. [Conclusion & Wrap-Up 18](#_Toc131179822)

[Summary with observations, Success & Failures, Challenges](#_Toc131179823)

# Executive Summary

## Lab 3.1

Within the lab there will be a breach and comprise of a host on the network. By utilizing the scanning tool nmap/Zenmap to find open ports on the pfSense Firewall. After, Bruter will be used as the choice of network brute force tool to gain access to the username and password on the windows system making use of a dictionary attack to execute this attack. After credentials gainged will be put to use in a Remote Desktop Protocol session

## LAB 3.2

For this lab there will be the experimentation of the execution of multiple denial-of-service attacks from a WAN utilizing multip;le different methods such as TCP, UDP, and HTTP flood to execute a denial-of-service. After establishing the connection it will be flood the services on host in order to make the server stop responding to requests.

## Objectives

Lab 3.1

* Use nmap/Zenmap to scan the windows network to detect pfSense firewall.
* Gain access by using the Bruter tool to exploit a system vulnerability
* Use the system commands to enumerate and list resources on a target system.

Lab 3.2

* Use a TCP flood to perform dDoS attack on a server
* Use UDP flood to perfom the dDoS attack on server

# Lab Description Details

## Procedure

## LAB 3.1

* 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 ran go through zenmap and run an intense scan on the same ip address as listed above, and click 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 verify they are there by hitting the refresh button on the bottom of the window

## LAB 3.2

* Begin by clicking on the Linux sniffer virtual machine type in the user as root and the password as toor then proceed to open the terminal on the Linux machine
* Start by utilizing the command cat ip2.txt and then the same but for the flag, after type into the command line ifconfig eht0 0.0.0.0 up in order to initialize this etherenet port.
* Once that is complete and you verify there is no ipv4 address set for this host proceed to type in  tcpdump –i eth0 -nntttt -s 0 -w TCPcapture.cap in order to capture the packet traffic analysis to verify that the flood has taken hold
* Click on the windows 8.1 attack machine and then launch the LOIC shortcut to begin the flooding, type in the IP address of 203.0.113.100 and then lock on to it, after lock on begin select the method to be TCP (This will be the same for the rest of the lab except it will be UDP, and the HTTP after)
* After this is done press the imma chargin mah lazer button and begin the flood attack, after 30 seconds press the control c command to stop the reading on the Linux machine and verify that there have been multiple packets captured.
* After type in the same command  tcpdump –i eth0 -nntttt -s 0 -w TCPcapture.cap except replace TCP with UDP and repeat the same process of letting the Linux machine listen and then navigate back to the windows 8 machine and where you selected TCP select UDP instead, launch the attack wait 30 seconds and then stop press control c on the Linux listening machine and verify that the packets were floodied
* After once again type in the command tcpdump –i eth0 -nntttt -s 0 -w TCPcapture.cap but replace TCP with HTTP this time and inside the windows 8 attack machine where you selected the TCP and UDP select HTTP select the button to launch the attack and then wait 30 seconds to press control c on the Linux machine and verify that there were a flood of packets on the HTTP line,
* Do the same thing as before except this time change HTTP to HTTP2 and then proceed to the windows machine and uncheck wait for reply, wait 30 seconds then navigate back to the other machine and press control c and verify that the packets were transferred via HTTP
* Now log onto the windows server machine and log in using the username administrator and the password as P@ssw0rd once in the computer navigate to the start menu and select computer
* Click on the C: drive and navigate to the xmap folder within this will be a folder for the flag open the text document and retrieve the flag, navigate to the appache folder and then find the logs file within this you can also verify that the flooding attack worked and within the folder you will also find the challenge flags here as well in a text document. Once in the Logs file navigate to the access log file and then read until you find the flag 6 within the logs and also verify that the attacks have gone through

# Supporting Evidence

## Graphical user interface, text, application Description automatically generatedLAB 3.1

Figure 1

Graphical user interface, application

Description automatically generatedFigure 2

Graphical user interface, application, Word

Description automatically generatedFigure 3

Graphical user interface, application

Description automatically generated

Figure 4

Graphical user interface

Description automatically generated

Graphical user interface, text, application, email

Description automatically generatedFigure 5

Figure 6

Graphical user interface, table

Description automatically generatedFigure 7

A picture containing diagram

Description automatically generatedFigure 8

A picture containing text, electronics, display, screenshot

Description automatically generated

Figure 9

A picture containing text, device, fan

Description automatically generated

Figure 10

## LAB 3.2

Text

Description automatically generated

Figure 11

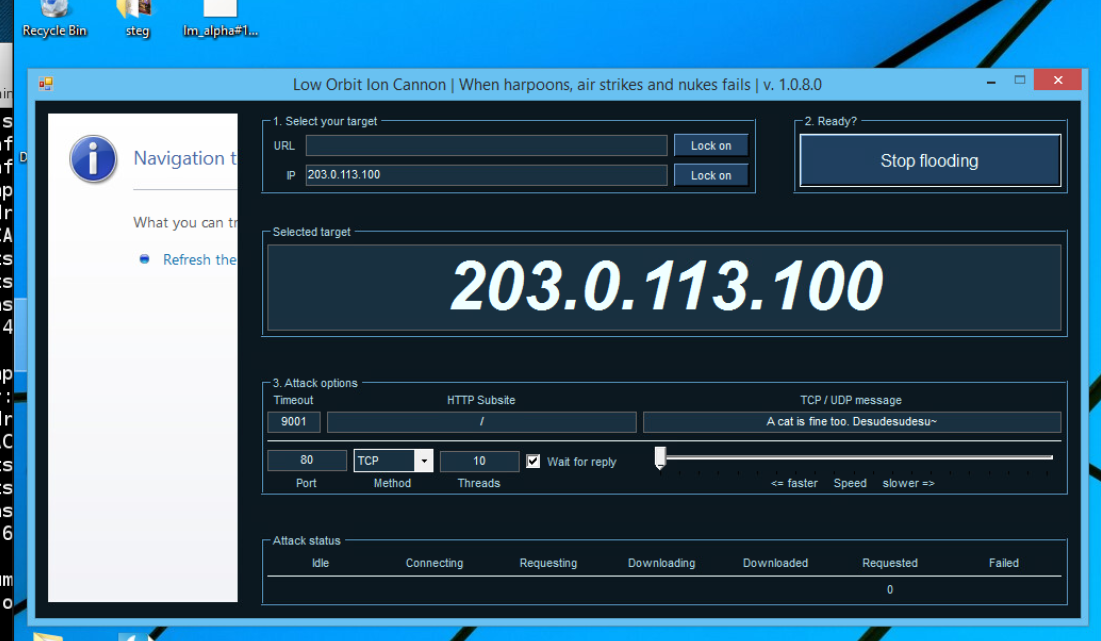


Figure 12

Text

Description automatically generated

Figure 13

Figure 14

Text

Description automatically generated

Figure 15

Text

Description automatically generated

Figure 16

Text

Description automatically generated

Figure 17

Graphical user interface, application, Word

Description automatically generated

Figure 18

Graphical user interface, application, Word

Description automatically generated

Figure 19

Graphical user interface, application, Word

Description automatically generated

Figure 20

Text

Description automatically generated

Figure 21

Text

Description automatically generated

Figure 22

Text

Description automatically generated

Figure 23

Text

Description automatically generated

Figure 24

# 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 deployment of a malware that was created on the attack machine using the darkcomet program and after a successful attack using bruter could be deployed on the system in order to retrieve the death start plans. The second lab was a success in launching the multiple attacks of denial of service on TCP, UDP, and HTTP. Overall, the lab was a success, and the objectives were completed and requirements met.