


ECE-GY 9383 Network Security LAB 5 - Web Application

What to Return: A PDF file that contains answers to all the questions below.

Note: This lab does not require you to use Digital Ocean or any other cloud services *if* your computer is based on X86 architecture. If your computer is an Apple M1, please use the following link to set up the lab: [Azure windows desktop setup](#).

Task 1. Set up the Kali & Metasploitable (5 points)

Steps

1. Download and Install the VirtualBox if you haven't done so already
2. Adds a new NAT network with a specified Network CIDR
3. Download [Get Kali | Kali Linux](#), and import it, make sure that the Kali Network is attached to the NAT network you created and promiscuous mode is 'Allow All'
4. Download [Metasploitable 2.0](#)
 - Machine->New... (Ctrl+N)
 - Name: Metasploitable
 - Type: Linux
 - Version: Ubuntu 32-bit
 - Default RAM
 - Use existing virtual hard disk -> Metasploitable.vmdk
 - You will need to manually add it 
5. Make sure that the Metasploitable Network is attached to the NAT network you created and promiscuous mode is 'Allow All'
6. Enter Kali username and password both as kali
7. Boot both systems. Enter Metasploitable username and password both as msfadmin

Questions

1. Include screenshots that show IP address of both Kali & Mmetasploitable in their terminal (2 points)
2. Try to ping from each other. Include screenshots that show Kali ping metasploitable and metasploitable ping Kali (3 points)

Task 2. Nmap (10 points)

Steps

1. In your Kali terminal, use nmap to scan all the open ports of metasploitable, with version detection

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

2. Use nmap and [NSE](#) to scan possible vulnerabilities of the metasploitable

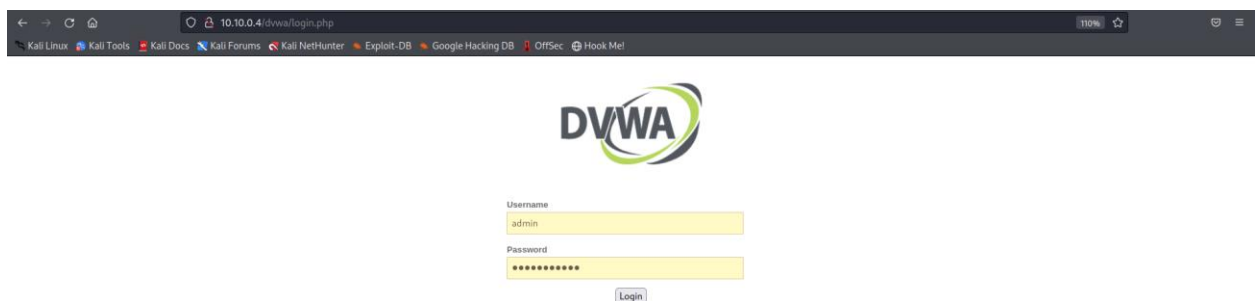
Questions

1. Provide your nmap command for step 1 and a screenshot that show the result of this step. (3 points)
2. With these many open ports you found from step1, pick a port that you find interesting, and briefly explain what kind/level of damage could you achieve if you find vulnerability in that port? (3 points)
3. Provide your nmap command for step 2 and a screenshot that show the result of this step 2. (4 points)

Task 3 DVWA : Damn Vulnerable Web App (17 points)

Steps

1. Launch firefox in Kali, type in the metasploitable ip + /dvwa, you should be able to see



with username admin and password password.

2. Go to DVWA Security section, set the security level to low
3. Navigate to the "Command Execution" page, find a way to print out /etc/passwd of metasploitable

4. Navigate to the "SQL injection" page, find a way to print out all users
5. Navigate to the "XSS reflected" page, find a way to create a pop-up window that says "Almost done!"
6. Navigate to the "CSRF" page, try to reset password
7. Navigate to the "XSS stored" page. Using the Stored XSS page, create a Message Post that will update the admin password to 'ECE-GY-9383' (this exploits both CSRF and XSS)

Note: the difference between XSS stored and XSS reflected is about the state of the data. One is persistent, the other is not.

Questions

1. Provide the payload of step 3, and screenshot that show the result of step 3 (3 points)
2. Provide the payload of step 4, and screenshot that show the result of step 4 (3 points)
3. Provide the payload of step 5, and screenshot that show the result of step 5 (3 points)
4. In step 6, you should see the browser url changes after you hit the 'change' button. What is the url now? If you directly modify the new browser url and change the password there, can you change your password? (3 points)
5. Provide the payload of step 7, and a screenshot that shows the result of step 7 (hint: it is helpful to press Ctrl + Shift + C in Firefox to open the developer tools and activate the "Pick element" tool.) (5 points)