CSCI-6658-01

ETHICAL HACKING

Infoseclablearning Assignment-4

Attacking Webservers from the WAN

Student Info:

Name : Akhila Parankusham

Student ID: 00810899

Email: apara7@unh.newhaven.edu

TABLE OF CONTENTS

Executive Summary

Highlights

In this lab, we will conduct a wide area network (WAN) assault against a web server using a Kali Linux attack machine. The objective of the attack is to find vulnerabilities and obtain unauthorized access to the server.

The lab has been broken down into several phases:

- **Reconnaissance**: During the reconnaissance phase, we will use tools such as Nmap or Zenmap to find open ports and services on the web server's firewall. This is similar to scanning the network for possible points of entry.
- **Exploitation**: We will use Bruter to launch a brute-force dictionary attack that targets the SMTP service on port 25 in order to retrieve the administrator password.
- **Gaining Access:** The objective is to connect to the web server remotely once we have the administrator credentials. This is usually accomplished by using Remote Desktop Protocol (RDP).
- **Maintaining Access:** After obtaining access to the web server, we can decide to make changes to the index.html file of the website in order to vandalize it and create an obvious indication of this involvement.
- **Covering Tracks:** We must remove pertinent log entries from the access.log file in order to avoid detection and erase proof of the attac\k. We can further hide the evidence after vandalizing the website by pausing and starting the Apache web server.

The purpose of this lab is to teach students how to use tools like Bruter, nmap, RDP, and other technologies to try to hack and compromise a web server from a distance. Emphasizing the value of network security and alertness, it gives students insights into how hackers could avoid notice, persist, and obtain illegal access.

Objectives

- Understanding how to handle attacks from both the WAN and LAN perspectives is crucial, as WAN attacks come from outside sources.
- Nmap is a useful tool for finding active hosts, open ports, services, and the underlying operating systems during the reconnaissance phase.
- Wordlists and dictionaries are used in brute-force attacks to break passwords and obtain unauthorized access.
- Maintaining control requires persistence, and access to compromised credentials is essential.
- Website modifications or vandalism can be facilitated by taking advantage of holes in input validation and permissive file permissions.
- To prevent discovery, it is necessary to erase all evidence of the attack, including files, event logs, etc.
- Using proxies, VPNs, and other strategies improves one's capacity to evade detection by helping them hide their identity and activities.
- We can increase our influence by changing our strategy and conducting more network attacks from a compromised server when needed.

- Metasploit and other similar tools make the process of creating exploits and attacks faster and more efficient.
- It is crucial to comprehend the legal ramifications of unapproved system access because these activities might carry harsh penalties.
- In order to protect enterprises against malicious threats, penetration testing, and ethical hacking require a strong understanding of the tools, techniques, and methodologies that these professionals employ.

Lab Description Details

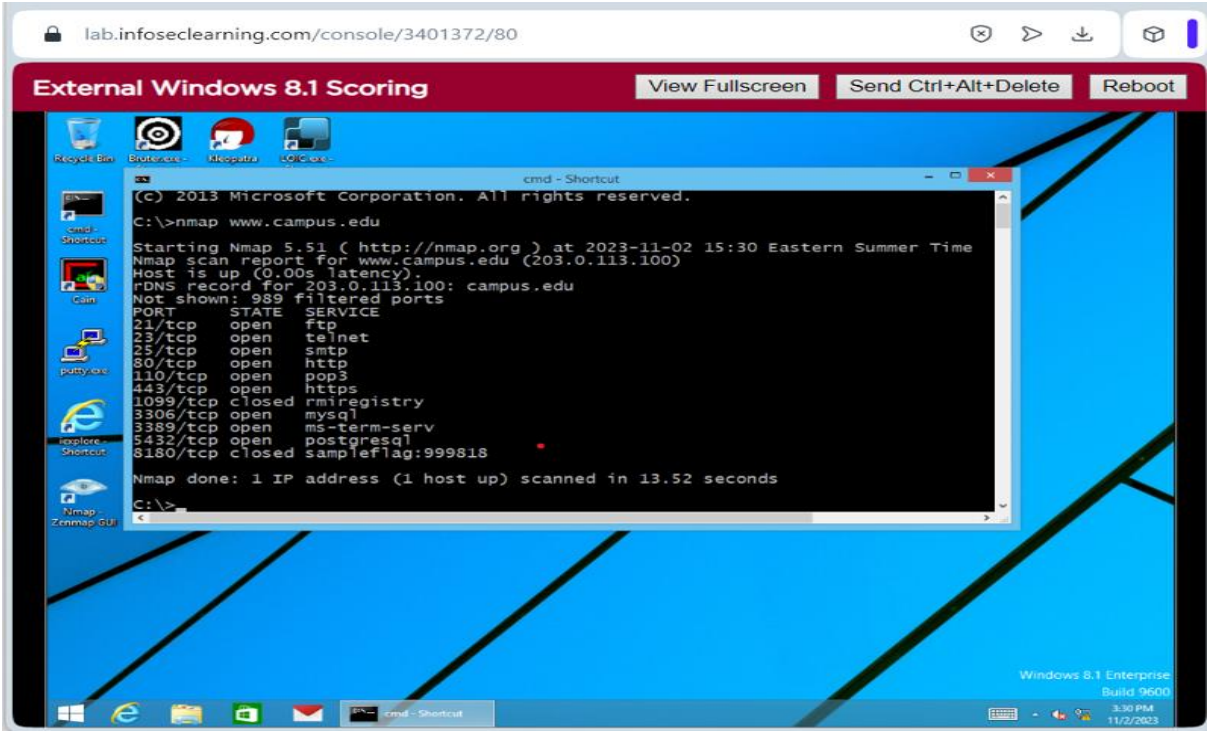
Steps Taken, Notes, & Screen Shots demonstrating completion of lab objectives

Supporting Evidence

Step 1: Launch Windows 8.1 Attack Machine (175.45.176.200-North Korea) and open cmd.

Step 2: Determine the open ports on the firewall.

nmap www.campus.edu



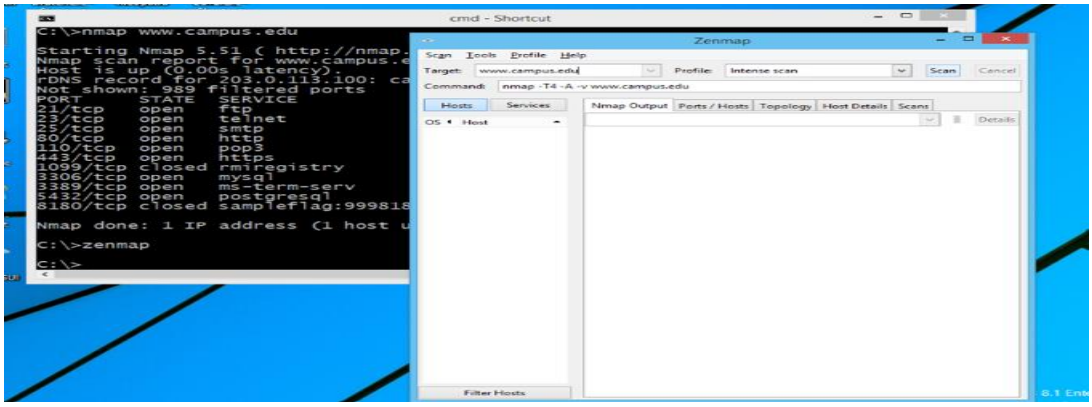
Step 3: Capture the sample flag.

SAMPLE CHALLENGE

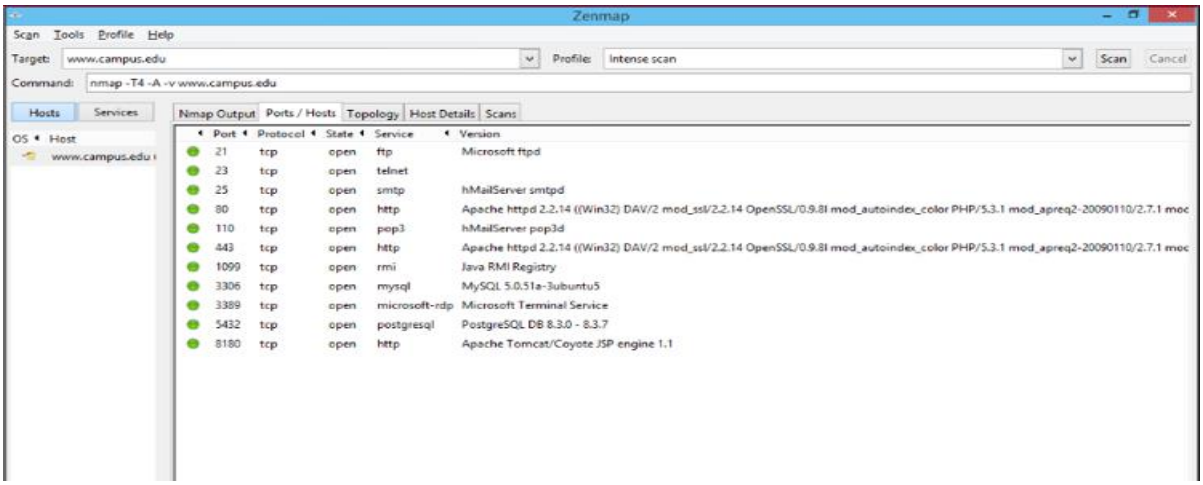
```
443/tcp  open    https
1099/tcp closed  rmiregistry
3306/tcp open    mysql
3389/tcp open    ms-term-serv
5432/tcp open    postgresql
8180/tcp closed  sampleflag:999818
```

Step 4: Open Zenmap. Set the target as www.campus.edu and launch an intense scan.

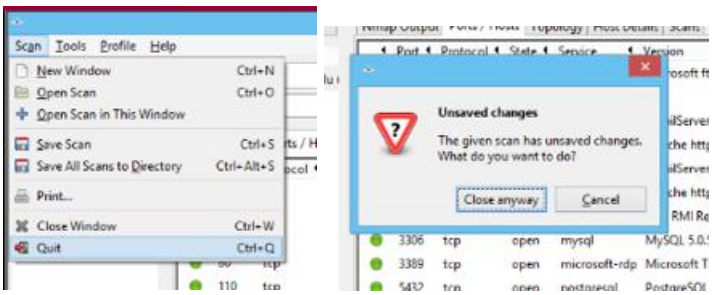
Zenmap



Step 5: After the scan, check for the open ports and banner messages that are displayed.

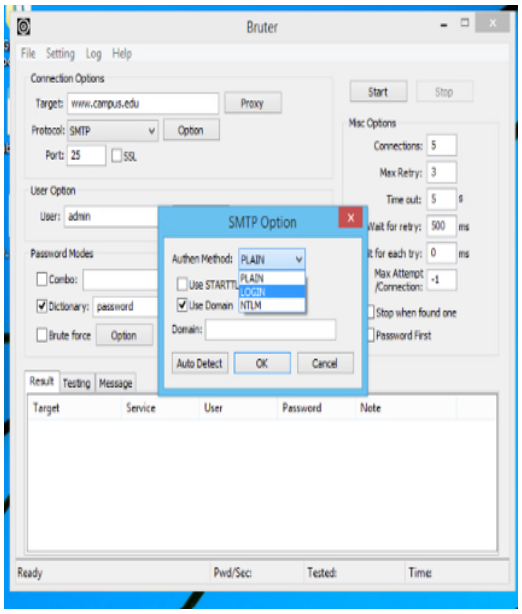


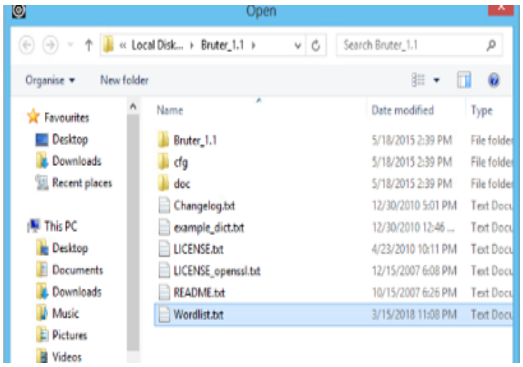
Step 6: Select scan>Quit>Close anyway

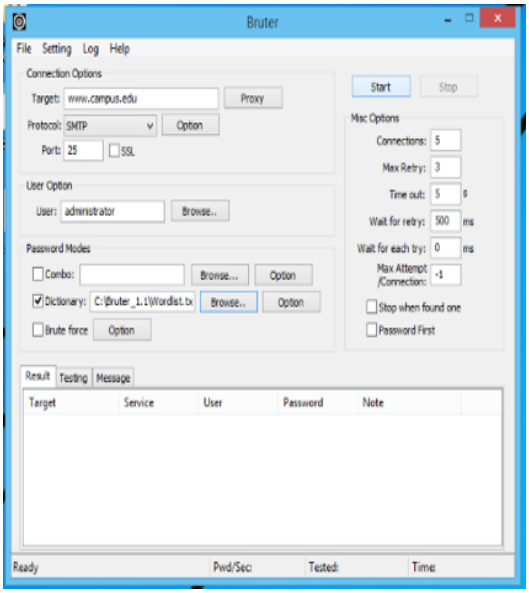


Step 7: Exit from cmd.

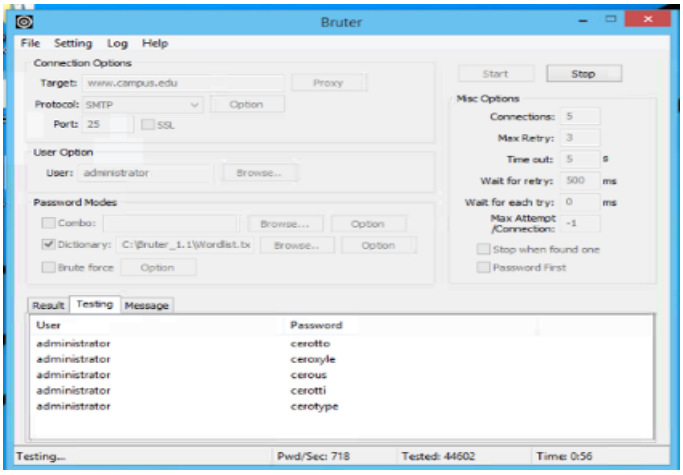
Step 8: Open Bruter.exe>Set target as www.campus.edu >SMTP as protocol>Choose SMTP option>Set Domain to login>User as administrator>Select Browse next to dictionary>Open Wordlist.txt and launch the attack.



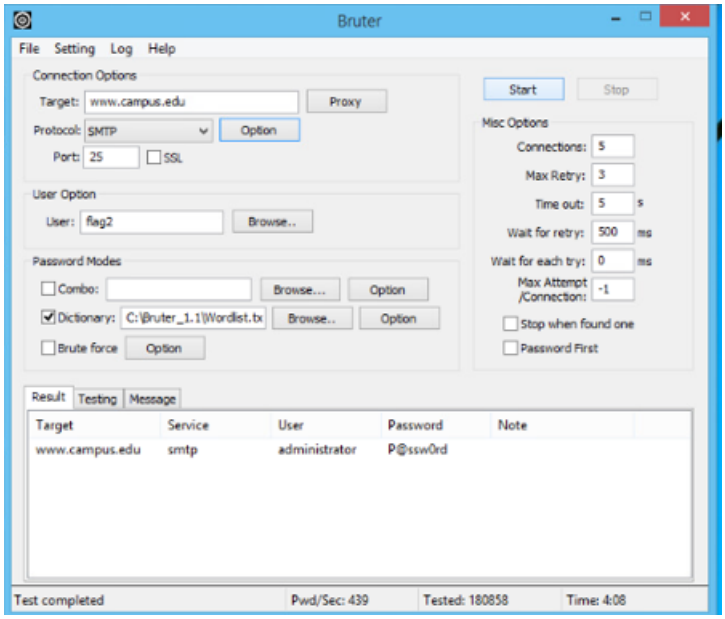




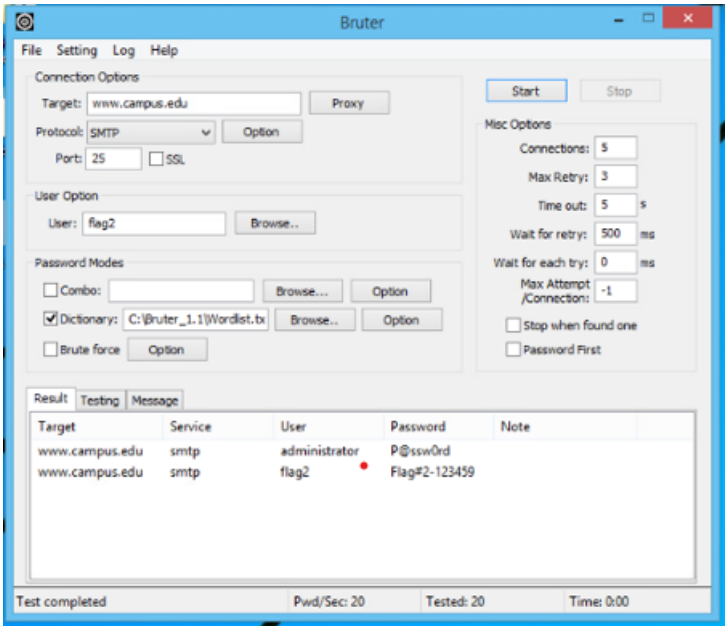
Step 9: Check for the bruter cycle in the testing tab.



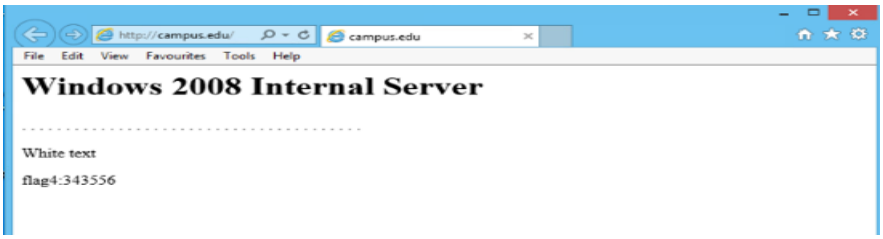
Step 10: The password is displayed on the result tab after a few minutes.



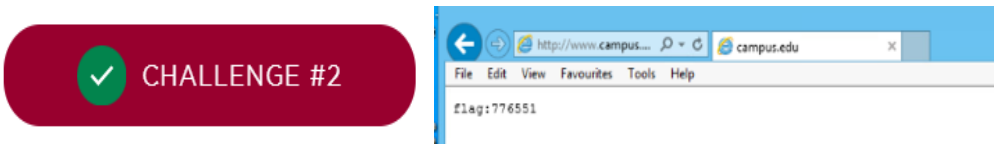
Step 11: Solving challenge 1 by using the steps below and changing the user to flag2 to retrieve the flag details.



Step 12: Open iexplore and enter the URL as http://www.campus.edu in the browser.

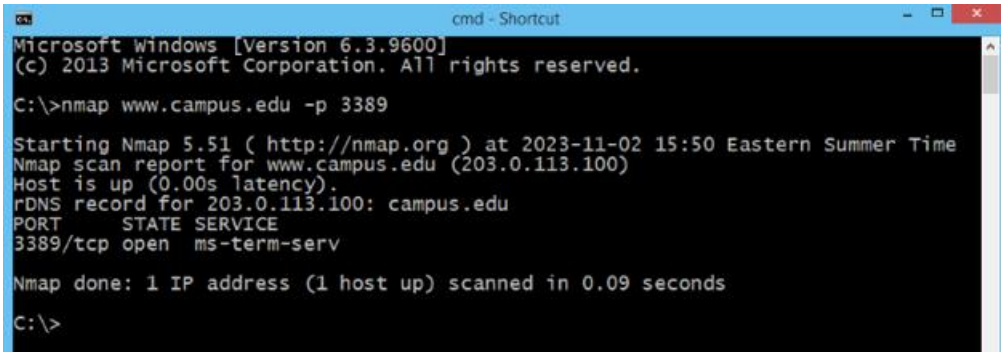


Step 13: Solving the challenge 2 using the previous step.



Step 14: Open cmd and check whether RDP is open on the firewall.

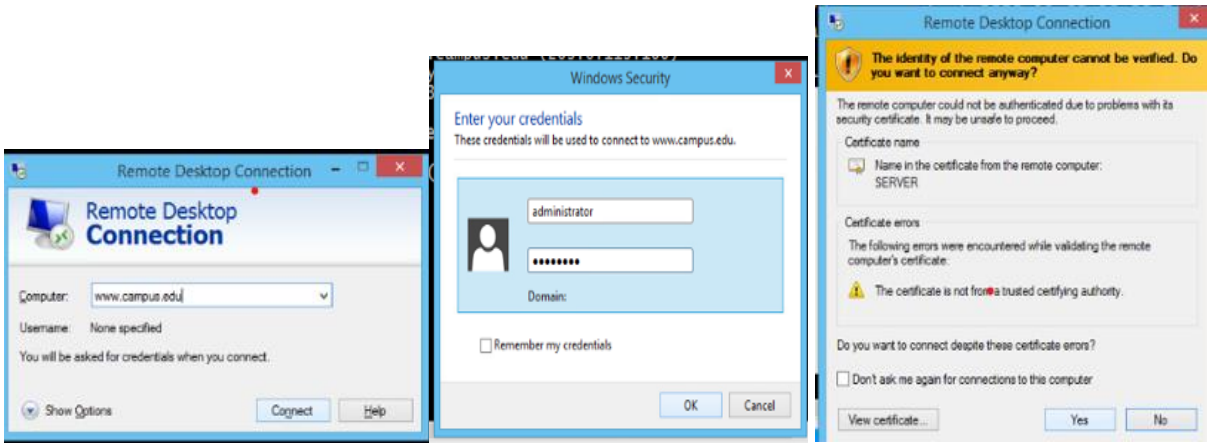
nmap www.campus.edu -p 3389



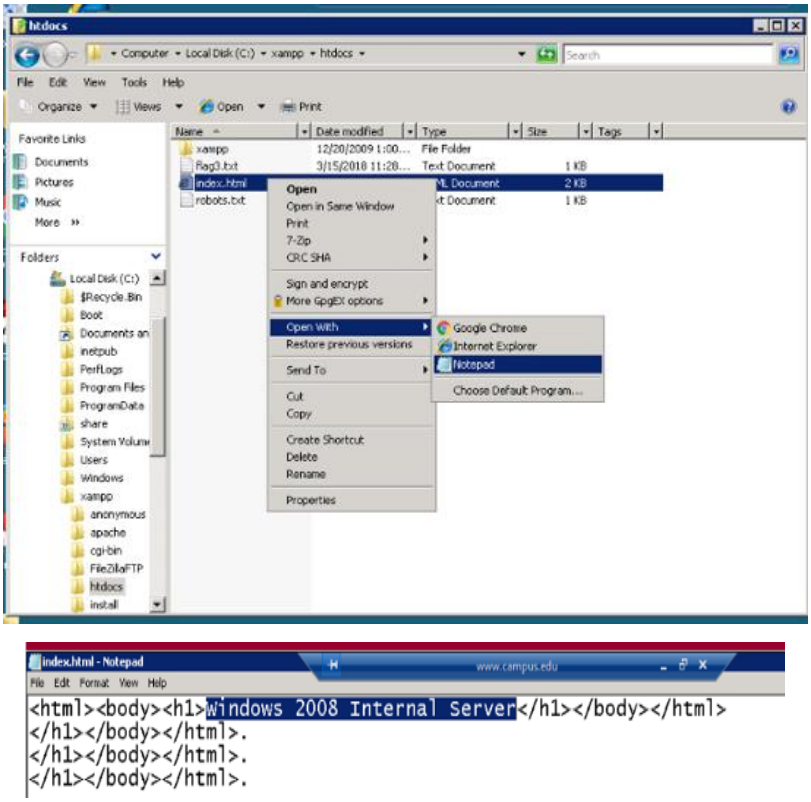
Step 15: Launch Microsoft Terminal Service Client.

#mstsc

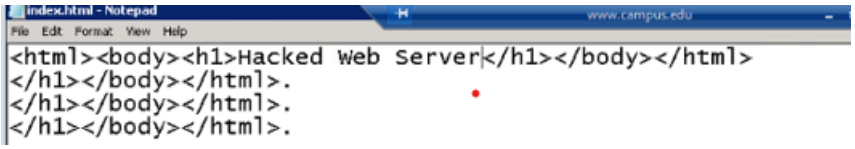
>Select www.campus.edu> Connect>Set username as administrator>Set P@ssw0rd as password>Click yes to the warning



Step 16: On Windows 2008 Server desktop, Click Start>Computer>C: Drive>xampp folder>htdocs folder>index. html(open with notepad).



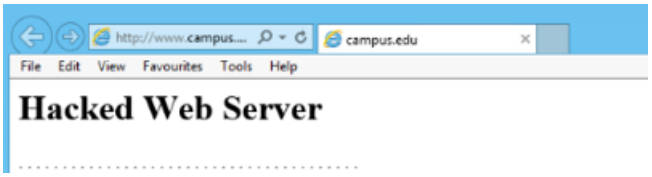
Step 17: Highlight Windows 2008 Internal Server and replace it with Hacked Web Server in the index.html file.



Step 18: Solving the challenge 3

Step 19: Save the edited file and close it. Minimize the window.

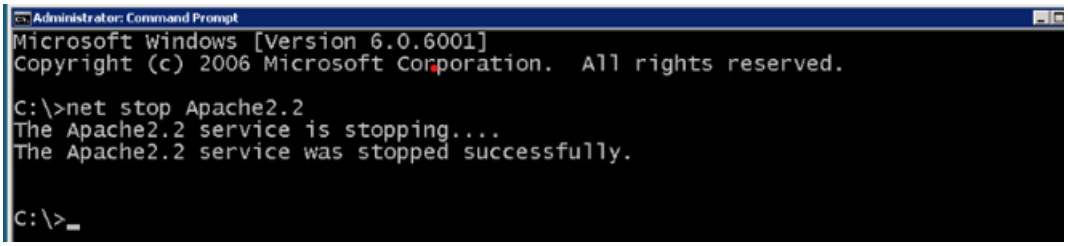
Step 20: Open iexplore and enter the URL as http://www.campus.edu in the browser. You can see the saved changes.



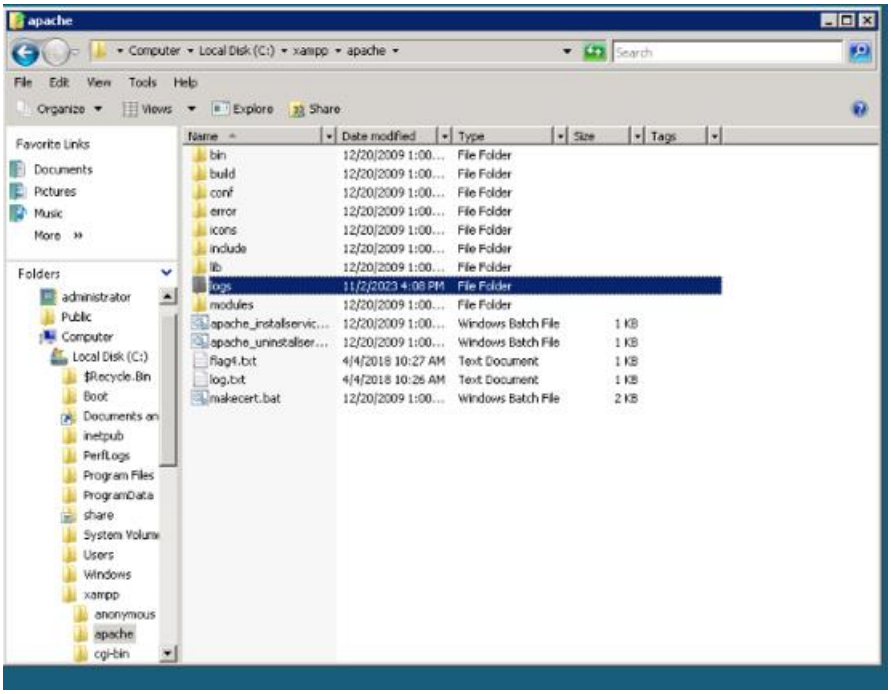
Step 21: Click on the RDP connection to www.campus.edu again.

Step 22: Stop the Apache Web Service and exit from cmd.

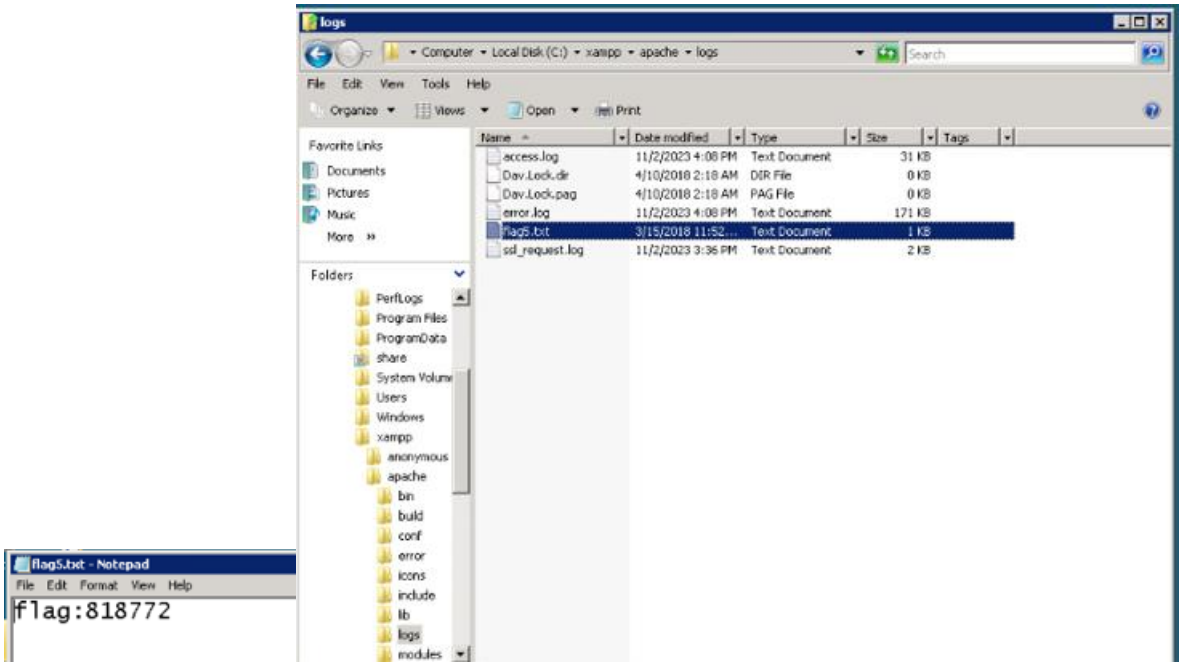
>net stop Apache2.2



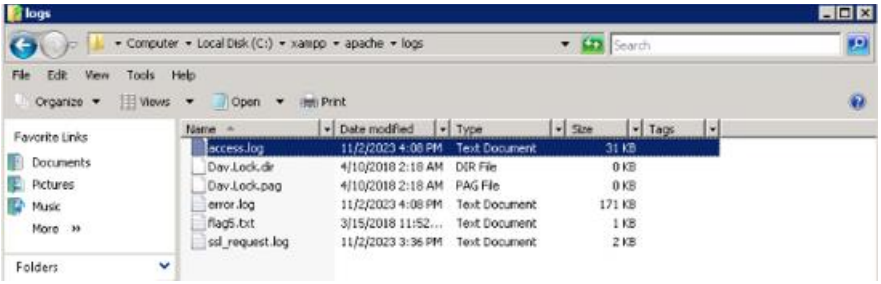
Step 23: Start>Computer>C:>xampp folder>apache folder>logs folder



Step 24: Solving the challenge 4.

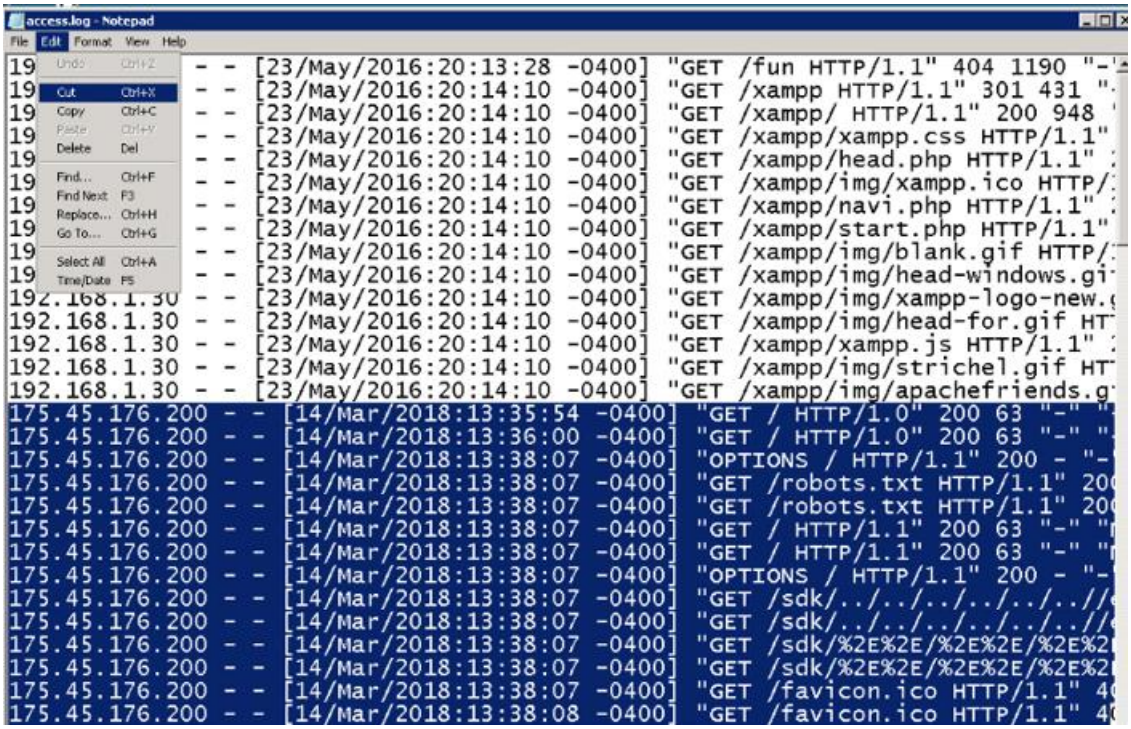


Step 25: Choose access.log file.



Step 26: Solving the challenge 5.

Step 27: Highlight the entries which begin with 175.45.176.200 and cut from the file and then save it.

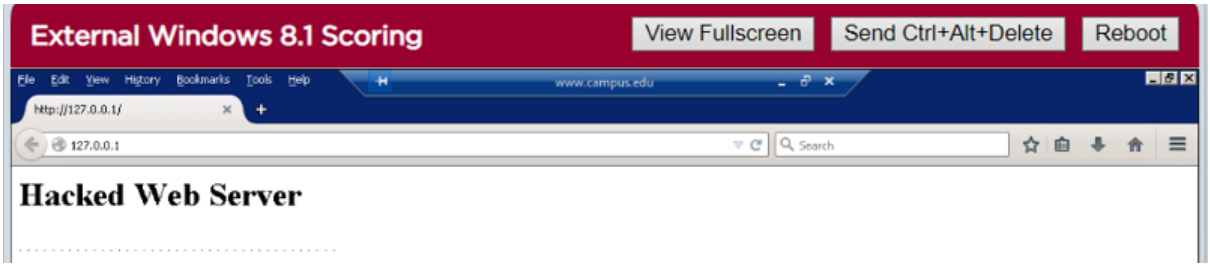


Step 28: Open cmd and start the Apache Web Service.

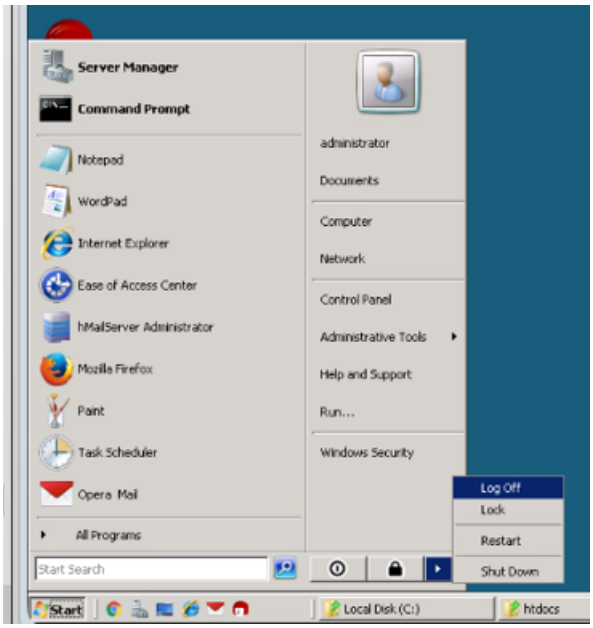
>net start Apache2.2

>exit

Step 29: Open Mozilla Firefox and enter the URL as 127.0.0.1 to verify whether the site is up and running.



Step 30: Start>Log off



Conclusion

Summary with Observations, Success & Failures, Challenges

In conclusion, this lab offered a hands-on example of how to use Kali Linux to initiate an attack on a web server from a wide area network. The procedure comprised using a range of instruments and methods to take advantage of weaknesses and obtain illegal access.

Observations:

- The lab session did a good job of demonstrating how to use Kali Linux to initiate a WAN assault on a web server.
- Bruter, RDP, nmap, and other tools were used to take advantage of weaknesses at various phases of the attack.
- Once access was gained, the attacker was able to hide their footprints and deface the website.

Successes:

- Utilizing Nmap/Zenmap, the attacker was able to map the network completely and identify open ports and running hosts.
- It took Bruter about ten minutes to successfully carry out a brute-force assault on the SMTP password.
- The web server was remotely accessible through the successful use of RDP and stolen passwords.
- To deface the website, vandals were able to successfully modify the index.html file.
- To effectively mask the traces of the attacker, log entries were removed and the Apache web server was restarted.

Challenges:

- The website had to be restarted after being defaced in order for the modifications to take effect.
- The tedious and labor-intensive process of removing traces from the log files increased the difficulty of hiding the attack.

Risks:

- Vulnerable applications and web servers can be exploited, opening the door for attackers to enter and possibly take control of internal systems, steal information, or harm websites.
- Unauthorized access can be made possible by authentication flaws including using weak passwords and being vulnerable to brute force attacks.
- The attack surface is expanded when ports and services are made public, which gives prospective attack vectors more possibilities.
- Operating systems and software lacking necessary patches introduce numerous known vulnerabilities.
- The efforts to respond to incidents and detect them are hampered by insufficient log visibility or logging capability.

- Weak access controls and permissions increase the risk of unauthorized access to resources.
- The lack of network segmentation or firewall rules allows for easier lateral movement within a system, which could increase the severity of an assault.

Remediations:

- Maintaining software updates and strengthening web servers using security measures. Conducting a penetration test in order to find and fix vulnerabilities.
- Establishing a strong password policy and using Multi-Factor Authentication (MFA) to prevent brute force attacks on authentication systems.
- To lessen the attack surface, deactivate any unused ports and services. To regulate and restrict entry points, impose access restrictions.
- Keep up a continuous vulnerability identification and remediation procedure that includes timely software patch deployment.
- To improve visibility and expedite incident response activities, establish a centralized system for log analysis and logging.
- To reduce the possibility of unwanted access, implement Access Control Lists (ACLs), use the least privileged model, and allocate discrete roles.