Attacking webservers from the WAN

ETHICAL HACKING & LAB Assignment 4

Student Info
Name: SRIJA PABBA
Student ID: 00866719
Email:
spabb6@unh.newhaven.edu

Table of Contents

Executive Summary

Highlights

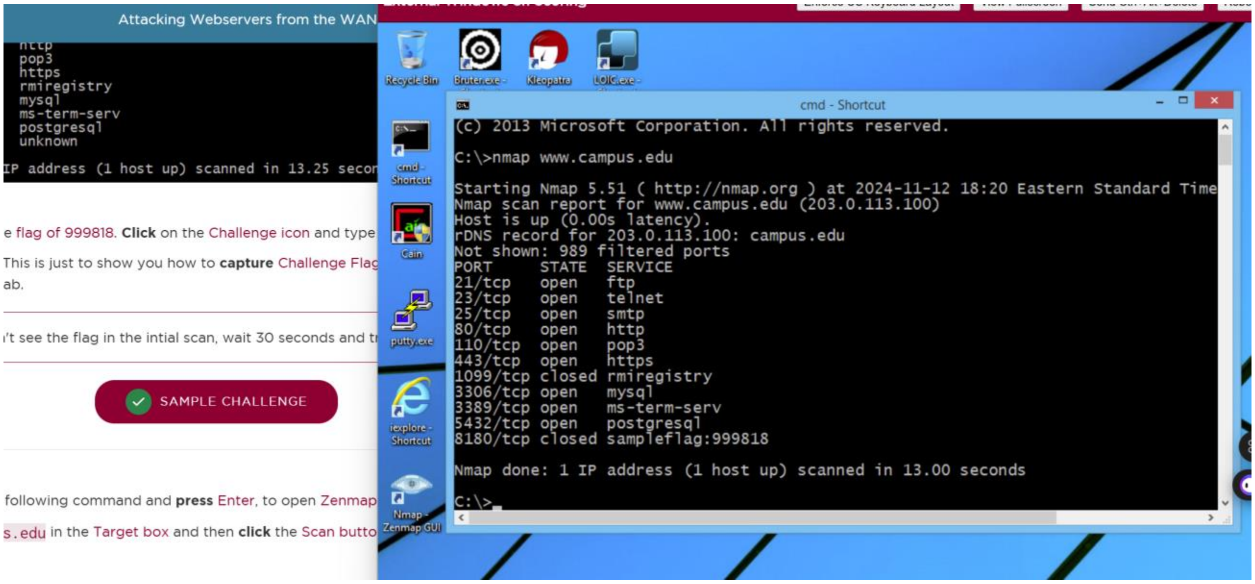
In this lab, I will conduct a cyberattack on a web server over a WAN using my Kali Linux Attack Machine. First, I'll perform reconnaissance by scanning the network with Nmap to find open ports, focusing on the SMTP port. Next, I'll use Bruter to carry out a brute-force dictionary attack on SMTP, aiming to capture administrator credentials. Once I have the credentials, I'll use RDP to access the server remotely. Following this, I'll deface the website as a post-exploitation step and then clear the logs to cover my tracks.

Objectives

My main objectives in this lab are to gain practical experience with network scanning and password cracking. I'll start by using Nmap to identify potential entry points and then move on to Bruter for a password attack on SMTP. After obtaining access credentials, I'll use RDP to remotely log into the server. The final objectives involve post-exploitation tasks, such as defacing the site and practicing stealth by removing any evidence of my actions from the logs. This lab helps me understand each stage of an attack, from reconnaissance to post-exploitation and cover-up.

Lab Description Details

To determine which ports are open on the firewall.



Attacking Webservers from the WAN

```
 http
 pop3
 https
 rmiregistry
 mysql
 ms-term-serv
 postgresql
 unknown

IP address (1 host up) scanned in 13.25 secon
```

e flag of 999818. **Click** on the Challenge icon and type

This is just to show you how to **capture** Challenge Flag
ab.

't see the flag in the intial scan, wait 30 seconds and t

SAMPLE CHALLENGE

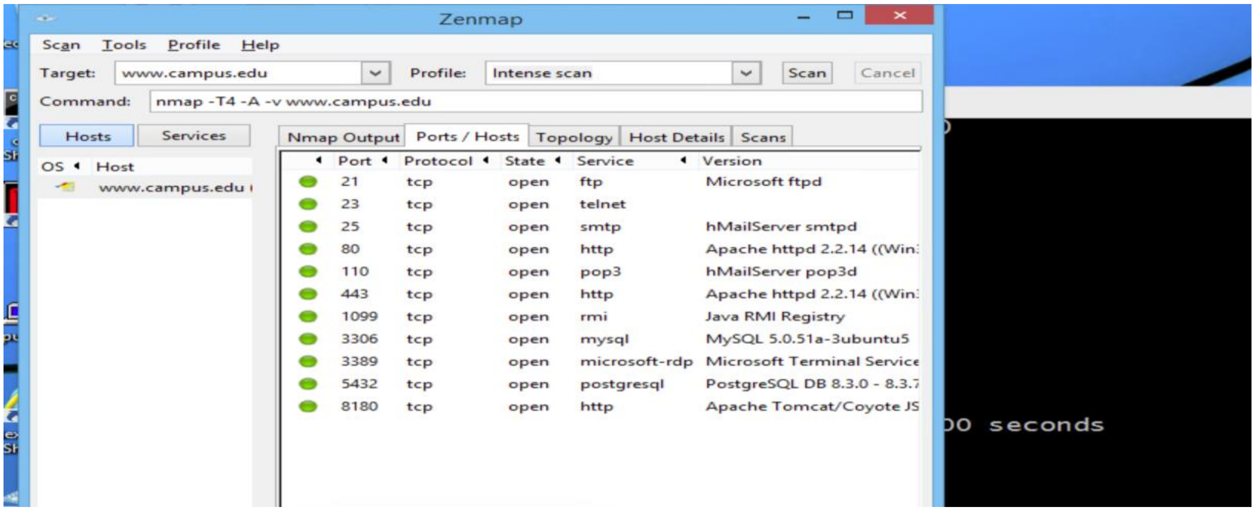
following command and **press** Enter, to open Zenmap

s.edu in the Target box and then **click** the Scan butto

```
(c) 2013 Microsoft Corporation. All rights reserved.

C:\>nmap www.campus.edu

Starting Nmap 5.51 ( http://nmap.org ) at 2024-11-12 18:20 Eastern Standard Time
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00s latency).
rDNS record for 203.0.113.100: campus.edu
Not shown: 989 filtered ports
PORT     STATE  SERVICE
21/tcp   open   ftp
23/tcp   open   telnet
25/tcp   open   smtp
80/tcp   open   http
110/tcp  open   pop3
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

Nmap done: 1 IP address (1 host up) scanned in 13.00 seconds

C:\>_
```

To open Zenmap we use this command “zenmap”. After it opens type “www.campus.edu” in the target box and click the scan button to launch an intense scan

After the scan is complete. In ports/ Hosts tab to view the open ports and corresponding banner messages that are displayed and we can notice many Microsoft services.

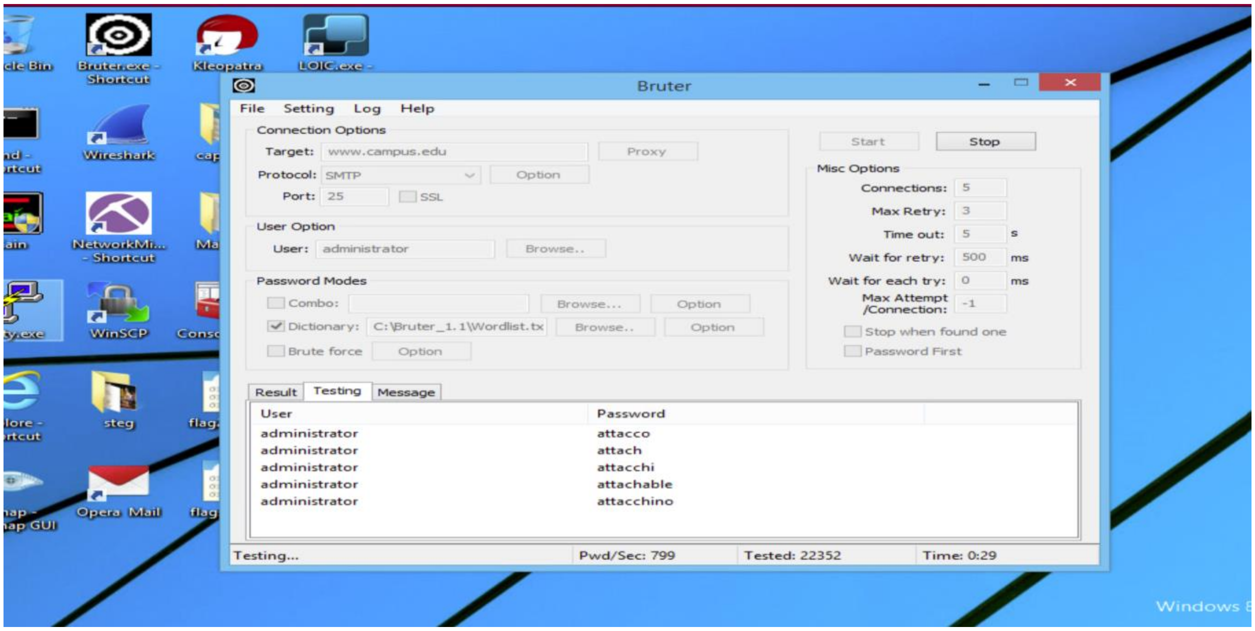


Target: www.campus.edu
Profile: Intense scan
Command: nmap -T4 -A -v www.campus.edu

OS	Host
	www.campus.edu

	Port	Protocol	State	Service	Version
●	21	tcp	open	ftp	Microsoft ftpd
●	23	tcp	open	telnet	
●	25	tcp	open	smtp	hMailServer smtpd
●	80	tcp	open	http	Apache httpd 2.2.14 ((Win:
●	110	tcp	open	pop3	hMailServer pop3d
●	443	tcp	open	http	Apache httpd 2.2.14 ((Win:
●	1099	tcp	open	rmi	Java RMI Registry
●	3306	tcp	open	mysql	MySQL 5.0.51a-3ubuntu5
●	3389	tcp	open	microsoft-rdp	Microsoft Terminal Service
●	5432	tcp	open	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
●	8180	tcp	open	http	Apache Tomcat/Coyote JS

After opening Bruter.exe we type the target “www.campus.edu” and select SMTP from the drop down. And in the option box set the Auten method as LOGIN and Domain as campus.edu then select ok. For the user we selected Administrator and in from the bowser selected the Wordlist.txt after everything is set . I selected start to launch the attack. After everything is done in result tab we can the passwords.



Connection Options
Target: www.campus.edu
Protocol: SMTP
Port: 25 □ SSL

User Option
User: administrator

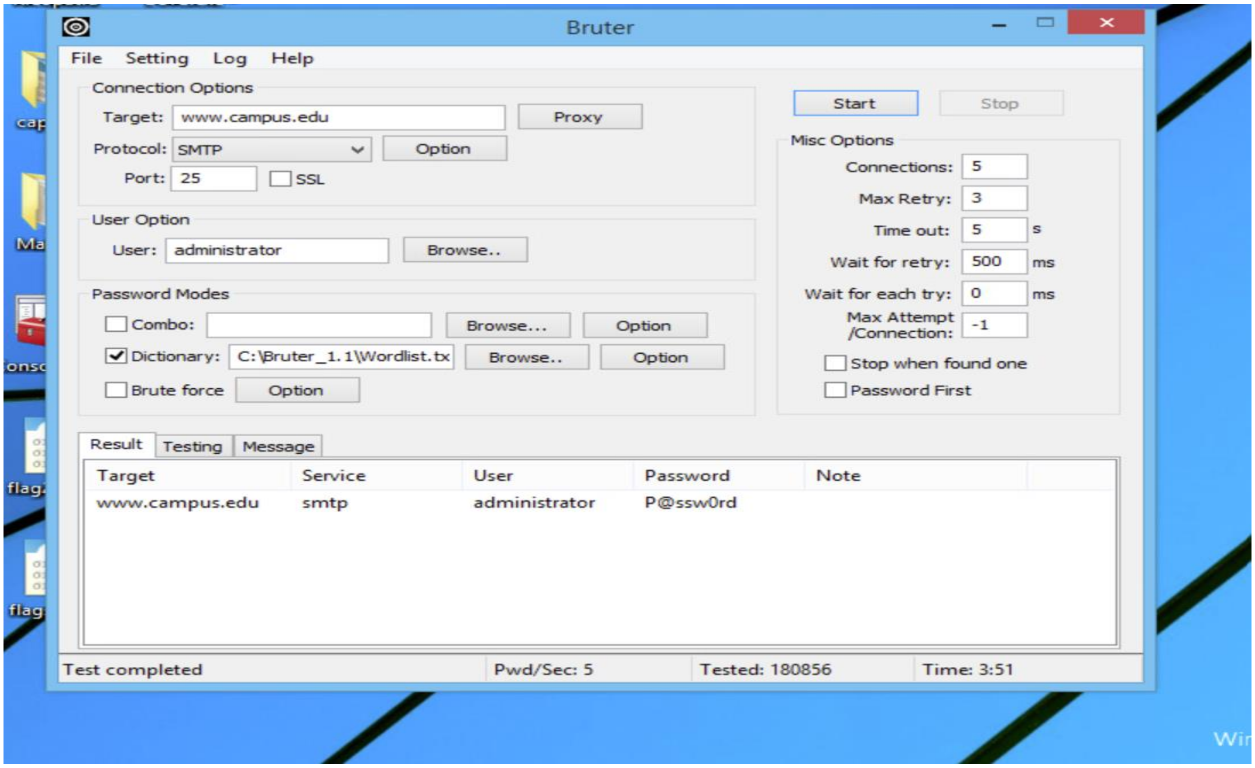
Password Modes
□ Combo:
☑ Dictionary: C:\Bruter_1.1\Wordlist.tx
□ Brute force

Misc Options
Connections: 5
Max Retry: 3
Time out: 5 s
Wait for retry: 500 ms
Wait for each try: 0 ms
Max Attempt /Connection: -1
□ Stop when found one
□ Password First

User	Password
administrator	attacco
administrator	attach
administrator	attacchi
administrator	attachable
administrator	attacchino

Testing... Pwd/Sec: 799 Tested: 22352 Time: 0:29

This screenshot shows the Displayed passwords in result tab



Connection Options

Target: www.campus.edu

Protocol: SMTP

Port: 25 □ SSL

User Option

User: administrator

Password Modes

□ Combo:

☑ Dictionary: C:\Bruter_1.1\Wordlist.tx

□ Brute force

Misc Options

Connections: 5

Max Retry: 3

Time out: 5 s

Wait for retry: 500 ms

Wait for each try: 0 ms

Max Attempt /Connection: -1

□ Stop when found one

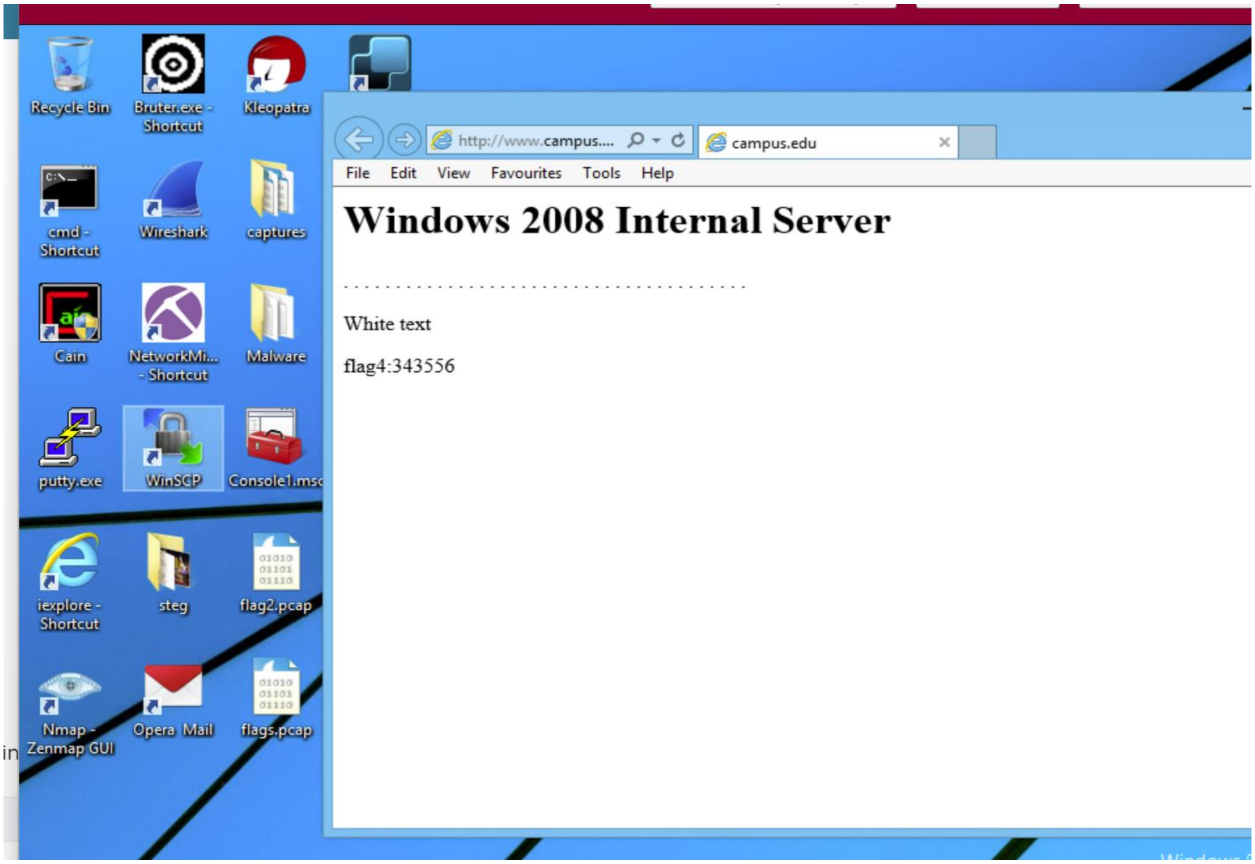
□ Password First

Target	Service	User	Password	Note
www.campus.edu	smtp	administrator	P@ssw0rd	

Test completed | Pwd/Sec: 5 | Tested: 180856 | Time: 3:51

This shows the password for the taget "www.campus.edu"

After Typing the "Campus.edu " URL in the URL bar this server is displayed



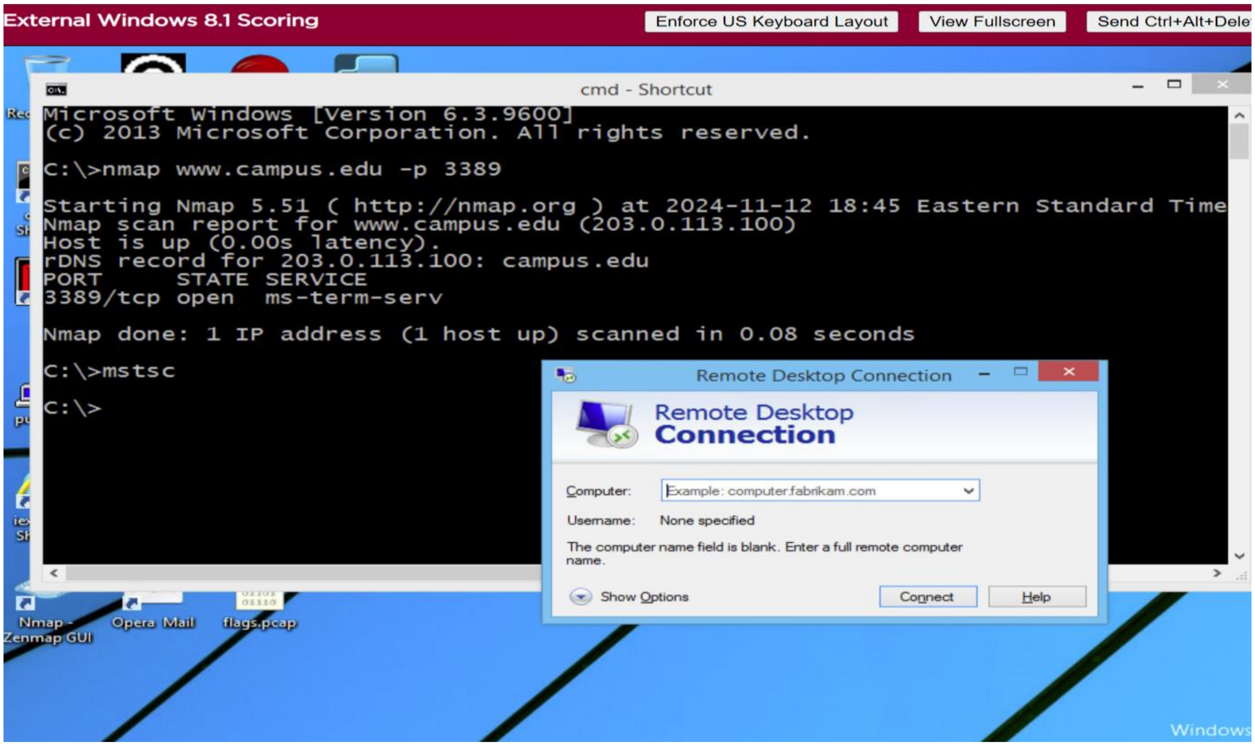
Windows 2008 Internal Server

. . . .

White text

flag4:343556

To determine if RDP is open on the firewall we type the following command.



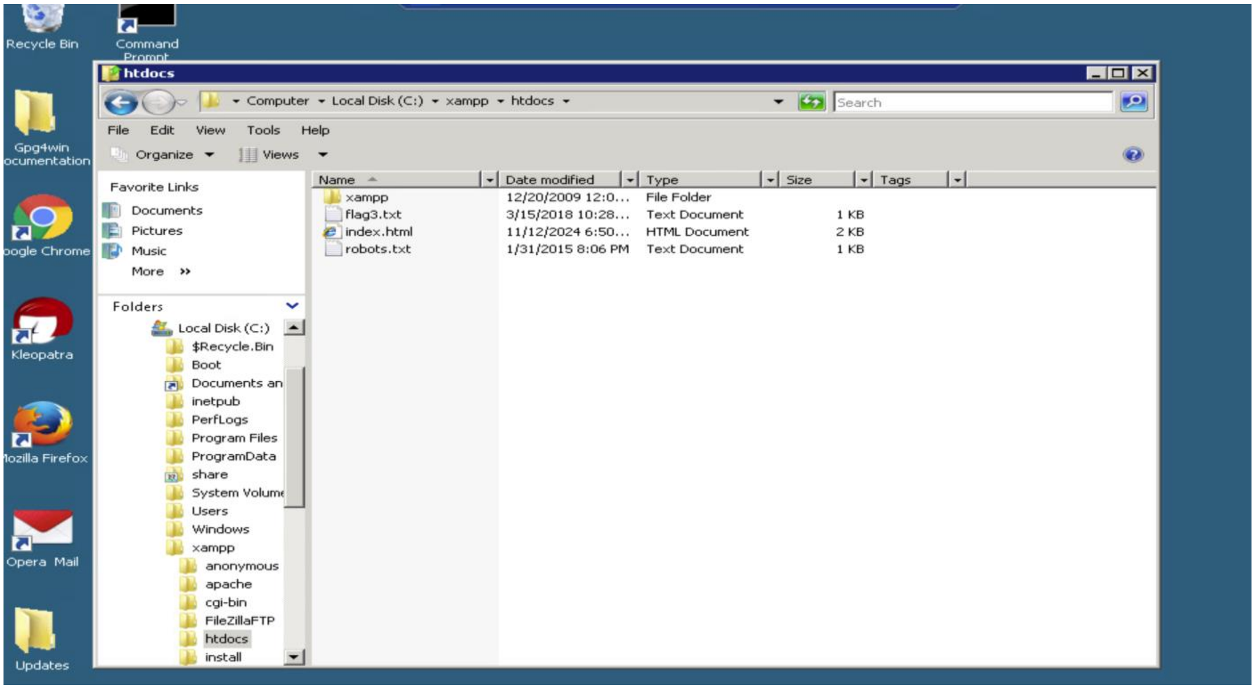
```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\>nmap www.campus.edu -p 3389

Starting Nmap 5.51 ( http://nmap.org ) at 2024-11-12 18:45 Eastern Standard Time
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00s latency).
rDNS record for 203.0.113.100: campus.edu
PORT     STATE SERVICE
3389/tcp open  ms-term-serv

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds

C:\>mstsc

C:\>
```

Computer: Example: computer.fabrikam.com

Username: None specified

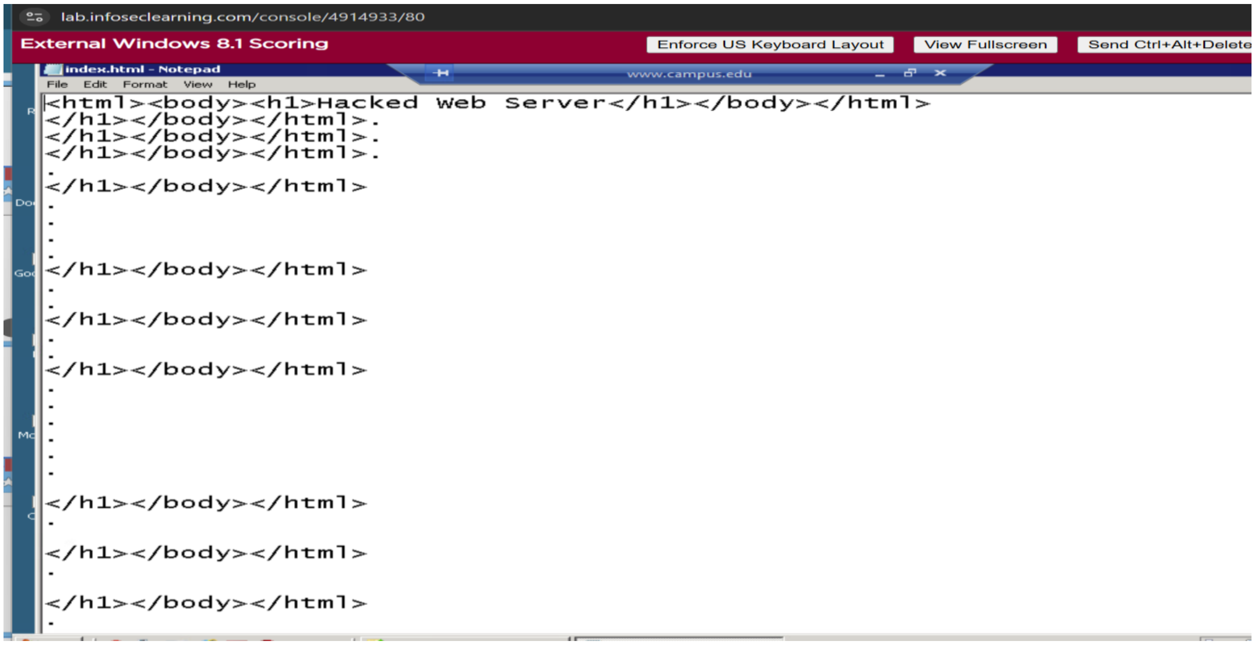
The computer name field is blank. Enter a full remote computer name.

To launch the Microsoft Terminal Service Client I used the command ”mstsc”. After connecting to the remote desktop in the start menu and after opening the computer link, In Local Disk xampp folder in that htdocs folder. I opened the index.html and opened with Notepad



Name	Date modified	Type	Size	Tags
xampp	12/20/2009 12:0...	File Folder		
flag3.txt	3/15/2018 10:28...	Text Document	1 KB	
index.html	11/12/2024 6:50...	HTML Document	2 KB	
robots.txt	1/31/2015 8:06 PM	Text Document	1 KB	

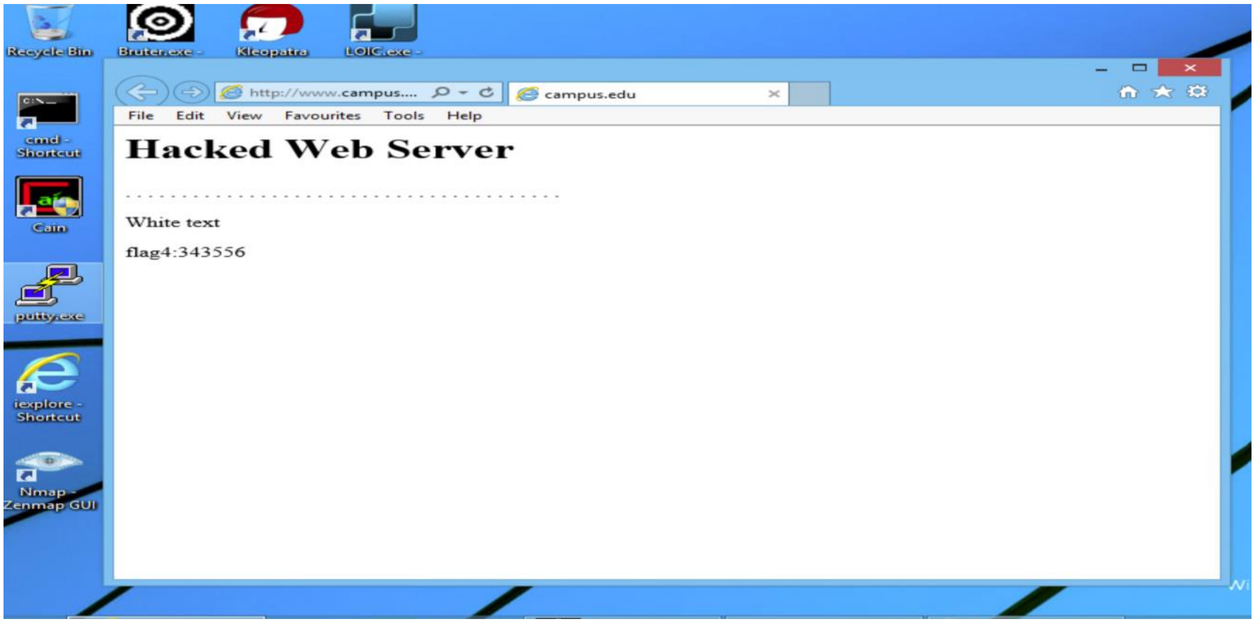
Highlighting the Windows 2008 internal Server in the index.html file and Typed the words "Hacked Web Server " to replace windows 2008 internal server in the index.html file


lab.infoseclearning.com/console/4914933/80
External Windows 8.1 Scoring
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
index.html - Notepad
File
Edit
Format
View
Help
www.campus.edu

```
<html><body><h1>Hacked web Server</h1></body></html>
</h1></body></html>.
</h1></body></html>.
</h1></body></html>.
.
</h1></body></html>
.
.
.
.
</h1></body></html>
.
</h1></body></html>
.
</h1></body></html>
.
.
.
.
.
</h1></body></html>
.
</h1></body></html>
.
</h1></body></html>
.
```

This Shows the typed words in html file

After changing the text in the html file Again entering the URL we can see the Message "Hacked Web Server"



Hacked Web Server

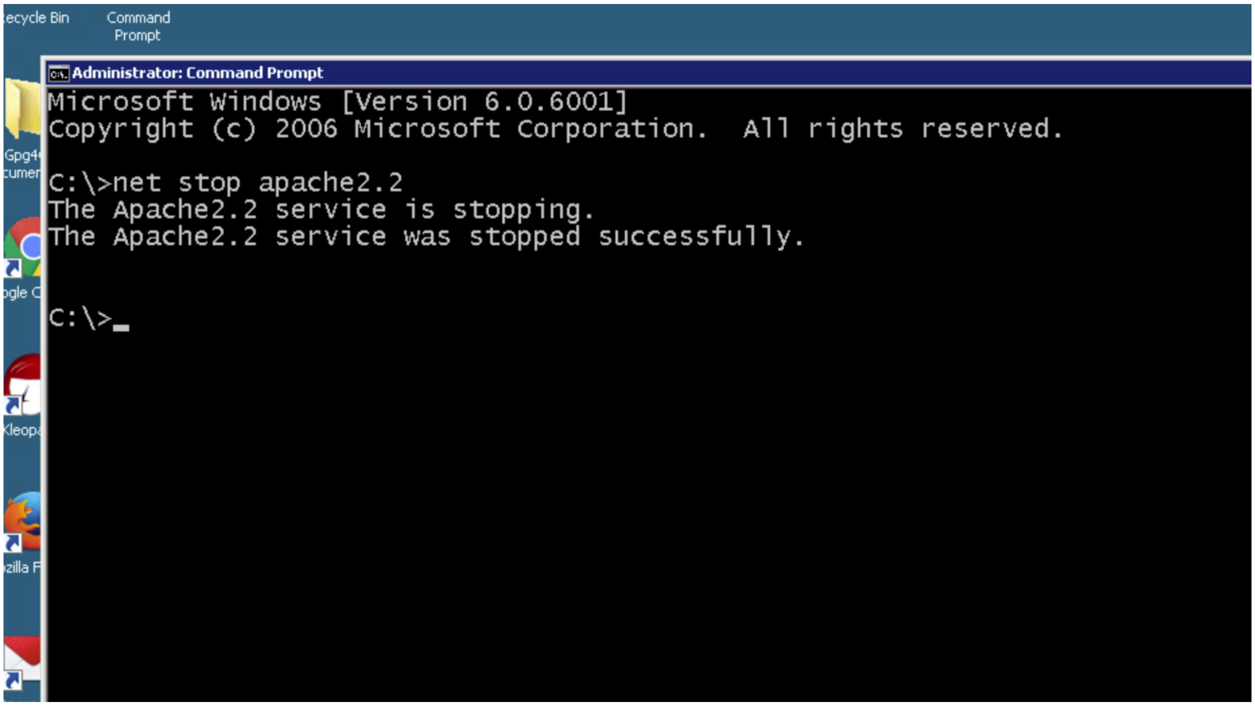
. . . .

White text

flag4:343556

This screenshot displays the web page with the typed message

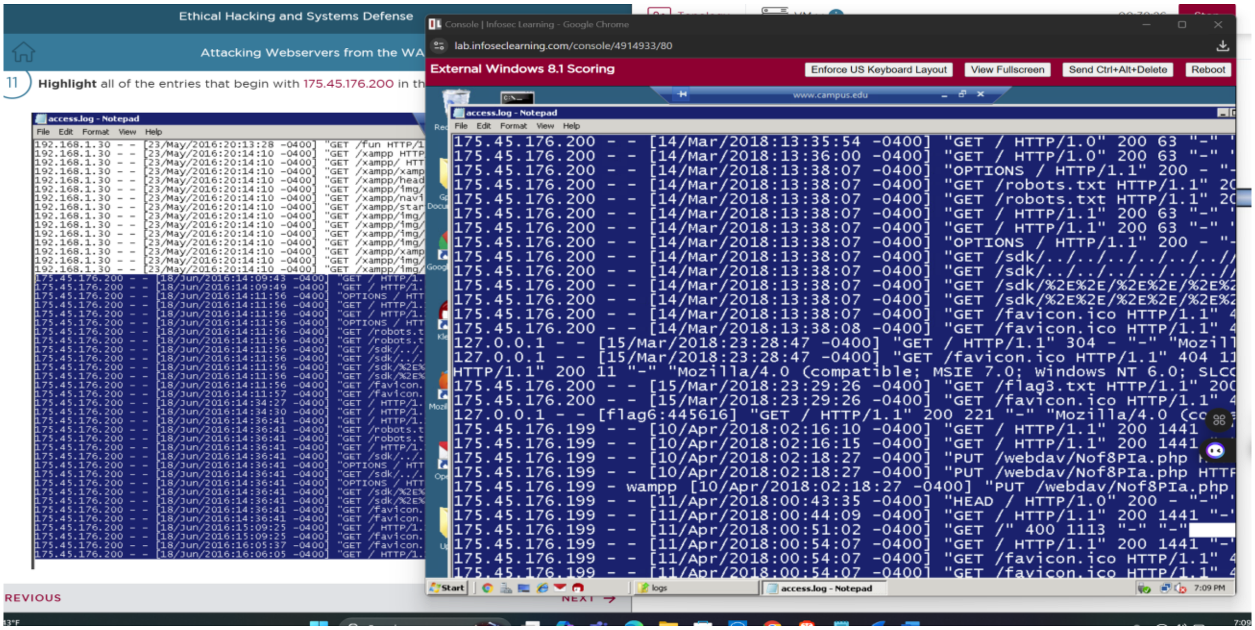
After Maximizing the RDP connection, In the command prompt to stop the apache web service we used the following command



```
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\>net stop apache2.2
The Apache2.2 service is stopping.
The Apache2.2 service was stopped successfully.


C:\>_
```

This screenshot shows the web service is stopped

In the Start Menu click the computer link, in the local disk open xampp folder and in the apche folder in that folder I found access.log file. In that it shows the list of all entries begin with 175.45.176.200


Ethical Hacking and Systems Defense
Attacking Webservers from the WA
access.log - Notepad
File Edit Format View Help
REVIOUS
NEXT →
Console | Infosec Learning - Google Chrome
External Windows 8.1 Scoring
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
www.campus.edu
Start
logs
access.log - Notepad
7:09 PM

11 **Highlight** all of the entries that begin with 175.45.176.200 in th

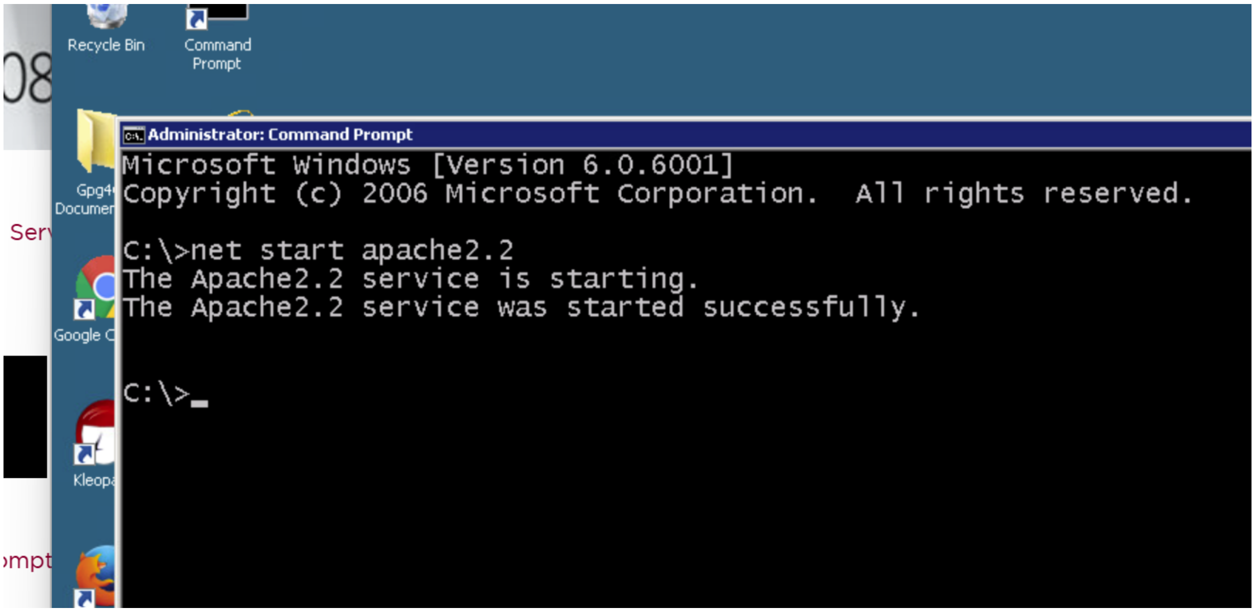
```
192.168.1.30 - - [23/May/2016:20:13:28 -0400] "GET /fun HTTP/1
192.168.1.30 - - [23/May/2016:20:14:10 -0400] "GET /xampp HTTP
192.168.1.30 - - [23/May/2016:20:14:10 -0400] "GET /xampp/ HTT
192.168.1.30 - - [23/May/2016:20:14:10 -0400] "GET /xampp/xamp
192.168.1.30 - - [23/May/2016:20:14:10 -0400] "GET /xampp/head
192.168.1.30 - - [23/May/2016:20:14:10 -0400] "GET /xampp/img/
192.168.1.30 - - [23/May/2016:20:14:10 -0400] "GET /xampp/navi
192.168.1.30 - - [23/May/2016:20:14:10 -0400] "GET /xampp/star
192.168.1.30 - - [23/May/2016:20:14:10 -0400] "GET /xampp/img/
192.168.1.30 - - [23/May/2016:20:14:10 -0400] "GET /xampp/img/
192.168.1.30 - - [23/May/2016:20:14:10 -0400] "GET /xampp/img/
192.168.1.30 - - [23/May/2016:20:14:10 -0400] "GET /xampp/img/
192.168.1.30 - - [23/May/2016:20:14:10 -0400] "GET /xampp/xamp
192.168.1.30 - - [23/May/2016:20:14:10 -0400] "GET /xampp/img/
192.168.1.30 - - [23/May/2016:20:14:10 -0400] "GET /xampp/img/
175.45.176.200 - - [18/Jun/2016:14:09:43 -0400] "GET / HTTP/1.
175.45.176.200 - - [18/Jun/2016:14:09:49 -0400] "GET / HTTP/1.
175.45.176.200 - - [18/Jun/2016:14:11:56 -0400] "OPTIONS / HTT
175.45.176.200 - - [18/Jun/2016:14:11:56 -0400] "GET / HTTP/1.
175.45.176.200 - - [18/Jun/2016:14:11:56 -0400] "GET / HTTP/1.
175.45.176.200 - - [18/Jun/2016:14:11:56 -0400] "OPTIONS / HTT
175.45.176.200 - - [18/Jun/2016:14:11:56 -0400] "GET /robots.t
175.45.176.200 - - [18/Jun/2016:14:11:56 -0400] "GET /robots.t
175.45.176.200 - - [18/Jun/2016:14:11:56 -0400] "GET /sdk/../.
175.45.176.200 - - [18/Jun/2016:14:11:56 -0400] "GET /sdk/../.
175.45.176.200 - - [18/Jun/2016:14:11:56 -0400] "GET /sdk/%2E%
175.45.176.200 - - [18/Jun/2016:14:11:56 -0400] "GET /sdk/%2E%
175.45.176.200 - - [18/Jun/2016:14:11:56 -0400] "GET /favicon.
175.45.176.200 - - [18/Jun/2016:14:11:57 -0400] "GET /favicon.
175.45.176.200 - - [18/Jun/2016:14:34:27 -0400] "GET / HTTP/1.
175.45.176.200 - - [18/Jun/2016:14:34:30 -0400] "GET / HTTP/1.
175.45.176.200 - - [18/Jun/2016:14:36:41 -0400] "GET / HTTP/1.
175.45.176.200 - - [18/Jun/2016:14:36:41 -0400] "GET /robots.t
175.45.176.200 - - [18/Jun/2016:14:36:41 -0400] "GET /robots.t
175.45.176.200 - - [18/Jun/2016:14:36:41 -0400] "GET / HTTP/1.
175.45.176.200 - - [18/Jun/2016:14:36:41 -0400] "GET /sdk/../.
175.45.176.200 - - [18/Jun/2016:14:36:41 -0400] "OPTIONS / HTT
175.45.176.200 - - [18/Jun/2016:14:36:41 -0400] "GET /sdk/../.
175.45.176.200 - - [18/Jun/2016:14:36:41 -0400] "OPTIONS / HTT
175.45.176.200 - - [18/Jun/2016:14:36:41 -0400] "GET /sdk/%2E%
175.45.176.200 - - [18/Jun/2016:14:36:41 -0400] "GET /sdk/%2E%
175.45.176.200 - - [18/Jun/2016:14:36:41 -0400] "GET /favicon.
175.45.176.200 - - [18/Jun/2016:14:36:41 -0400] "GET /favicon.
175.45.176.200 - - [18/Jun/2016:15:09:25 -0400] "GET / HTTP/1.
175.45.176.200 - - [18/Jun/2016:15:09:25 -0400] "GET /favicon.
175.45.176.200 - - [18/Jun/2016:16:05:37 -0400] "GET /favicon.
175.45.176.200 - - [18/Jun/2016:16:06:05 -0400] "GET / HTTP/1.
```

lab.infoseclearning.com/console/4914933/80

```
175.45.176.200 - - [14/Mar/2018:13:35:54 -0400] "GET / HTTP/1.0" 200 63 "-" '
175.45.176.200 - - [14/Mar/2018:13:36:00 -0400] "GET / HTTP/1.0" 200 63 "-" '
175.45.176.200 - - [14/Mar/2018:13:38:07 -0400] "OPTIONS / HTTP/1.1" 200 - "-
175.45.176.200 - - [14/Mar/2018:13:38:07 -0400] "GET /robots.txt HTTP/1.1" 20
175.45.176.200 - - [14/Mar/2018:13:38:07 -0400] "GET /robots.txt HTTP/1.1" 20
175.45.176.200 - - [14/Mar/2018:13:38:07 -0400] "GET / HTTP/1.1" 200 63 "-" '
175.45.176.200 - - [14/Mar/2018:13:38:07 -0400] "GET / HTTP/1.1" 200 63 "-" '
175.45.176.200 - - [14/Mar/2018:13:38:07 -0400] "OPTIONS / HTTP/1.1" 200 - "-
175.45.176.200 - - [14/Mar/2018:13:38:07 -0400] "GET /sdk/../../../../../../
175.45.176.200 - - [14/Mar/2018:13:38:07 -0400] "GET /sdk/../../../../../../
175.45.176.200 - - [14/Mar/2018:13:38:07 -0400] "GET /sdk/%2E%2E/%2E%2E/%2E%2
175.45.176.200 - - [14/Mar/2018:13:38:07 -0400] "GET /sdk/%2E%2E/%2E%2E/%2E%2
175.45.176.200 - - [14/Mar/2018:13:38:07 -0400] "GET /favicon.ico HTTP/1.1" 4
175.45.176.200 - - [14/Mar/2018:13:38:08 -0400] "GET /favicon.ico HTTP/1.1" 4
127.0.0.1 - - [15/Mar/2018:23:28:47 -0400] "GET / HTTP/1.1" 304 - "-" "Mozill
127.0.0.1 - - [15/Mar/2018:23:28:47 -0400] "GET /favicon.ico HTTP/1.1" 404 11
HTTP/1.1" 200 11 "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; SLCC
175.45.176.200 - - [15/Mar/2018:23:29:26 -0400] "GET /flag3.txt HTTP/1.1" 200
175.45.176.200 - - [15/Mar/2018:23:29:26 -0400] "GET /favicon.ico HTTP/1.1" 4
127.0.0.1 - - [flag6:445616] "GET / HTTP/1.1" 200 221 "-" "Mozilla/4.0 (co
175.45.176.199 - - [10/Apr/2018:02:16:10 -0400] "GET / HTTP/1.1" 200 1441
175.45.176.199 - - [10/Apr/2018:02:16:15 -0400] "GET / HTTP/1.1" 200 1441
175.45.176.199 - - [10/Apr/2018:02:18:27 -0400] "PUT /webdav/Nof8PIa.php
175.45.176.199 - - [10/Apr/2018:02:18:27 -0400] "PUT /webdav/Nof8PIa.php HTTP
175.45.176.199 - wampp [10/Apr/2018:02:18:27 -0400] "PUT /webdav/Nof8PIa.php
175.45.176.199 - - [11/Apr/2018:00:43:35 -0400] "HEAD / HTTP/1.0" 200 - "-" '
175.45.176.199 - - [11/Apr/2018:00:44:09 -0400] "GET / HTTP/1.1" 200 1441 "-'
175.45.176.199 - - [11/Apr/2018:00:51:02 -0400] "GET /" 400 1113 "-" "-"
175.45.176.199 - - [11/Apr/2018:00:54:07 -0400] "GET / HTTP/1.1" 200 1441 "-
175.45.176.199 - - [11/Apr/2018:00:54:07 -0400] "GET /favicon.ico HTTP/1.1" 4
175.45.176.199 - - [11/Apr/2018:00:54:07 -0400] "GET /favicon.ico HTTP/1.1" 4
```

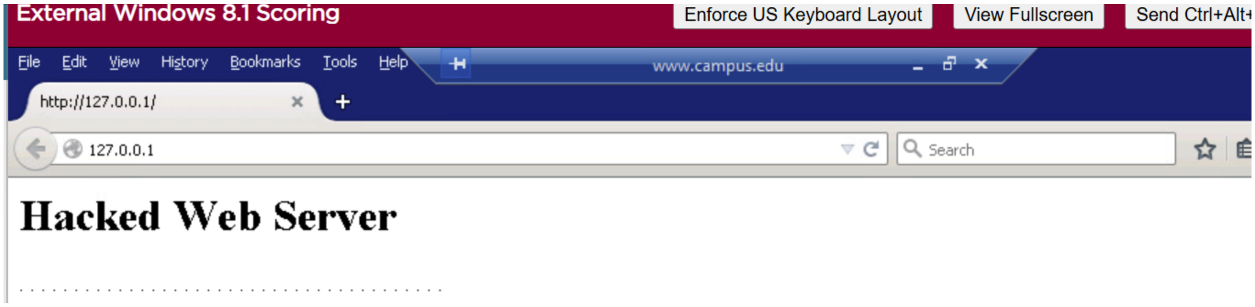
This Screenshot shows the highlighted entries all begin with “175.45.176.200”

To start the apache web server, used the following command



```
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\>net start apache2.2
The Apache2.2 service is starting.
The Apache2.2 service was started successfully.


C:\>_
```

After opening the firefox and typing the URL “127.0.0.1” to connect to verify the sute is up and running

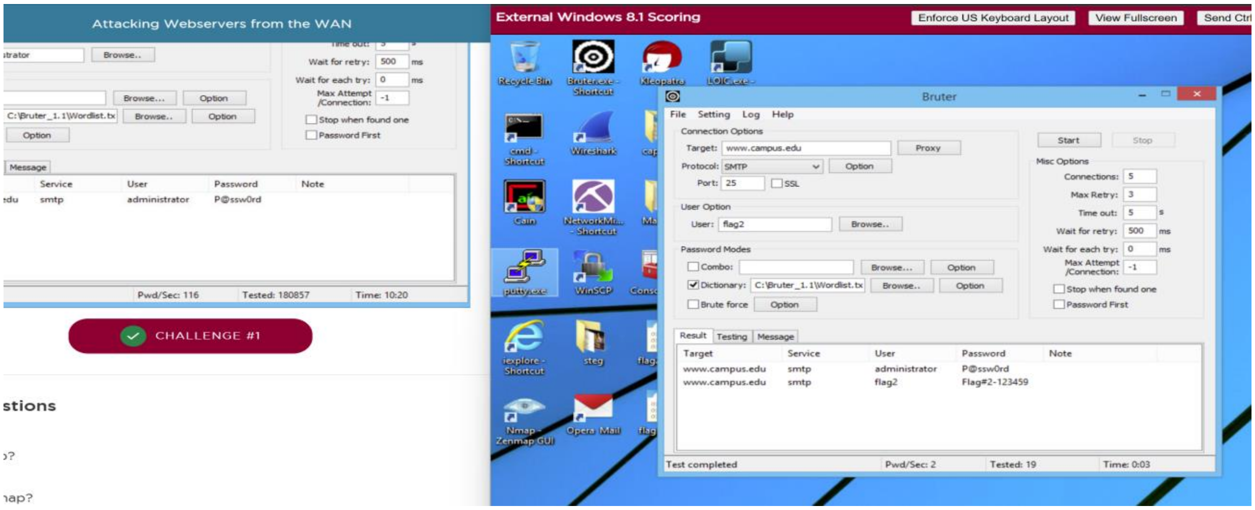


Hacked Web Server

This screenshot shows that the site is hacked

Supporting Evidence

The challenge tasks I had during the lab.



Connection Options

Target: www.campus.edu

Protocol: SMTP

Port: 25 □ SSL

User Option

User: flag2

Password Modes

□ Combo:

☑ Dictionary: C:\Bruter_1.1\Wordlist.tx

□ Brute force

Misc Options

Connections: 5

Max Retry: 3

Time out: 5 s

Wait for retry: 500 ms

Wait for each try: 0 ms

Max Attempt /Connection: -1

□ Stop when found one

□ Password First

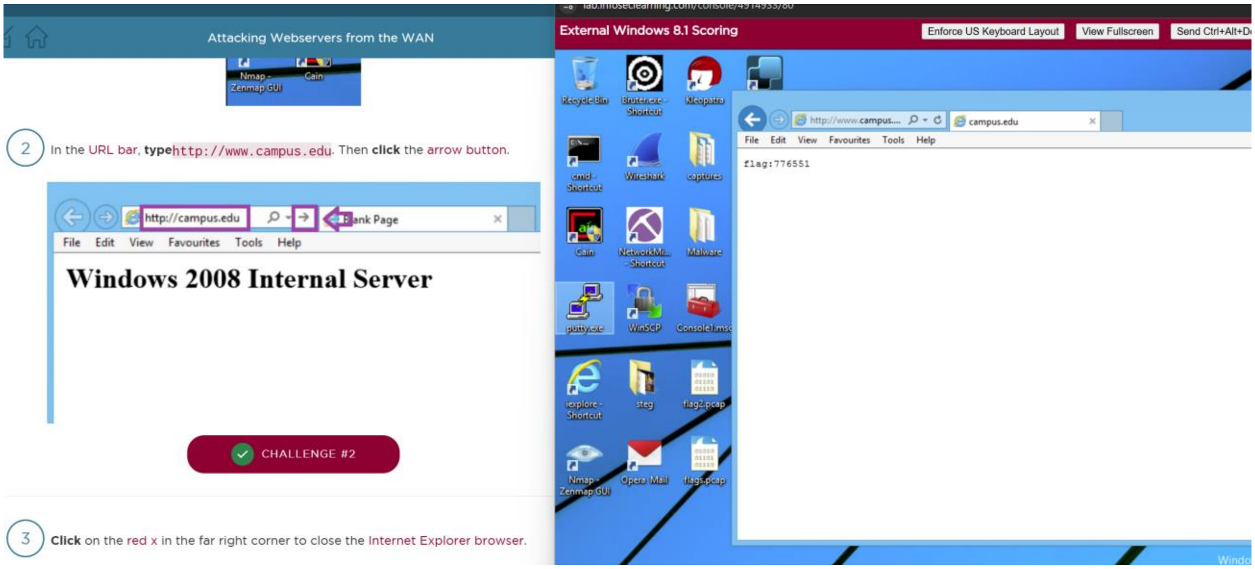
Target	Service	User	Password	Note
www.campus.edu	smtp	administrator	P@ssw0rd	
www.campus.edu	smtp	flag2	Flag#2-123459	

Test completed   Pwd/Sec: 2   Tested: 19   Time: 0:03

Service	User	Password	Note
smtp	administrator	P@ssw0rd	

Pwd/Sec: 116   Tested: 180857   Time: 10:20

This Screenshot shows the password displayed in result for the target



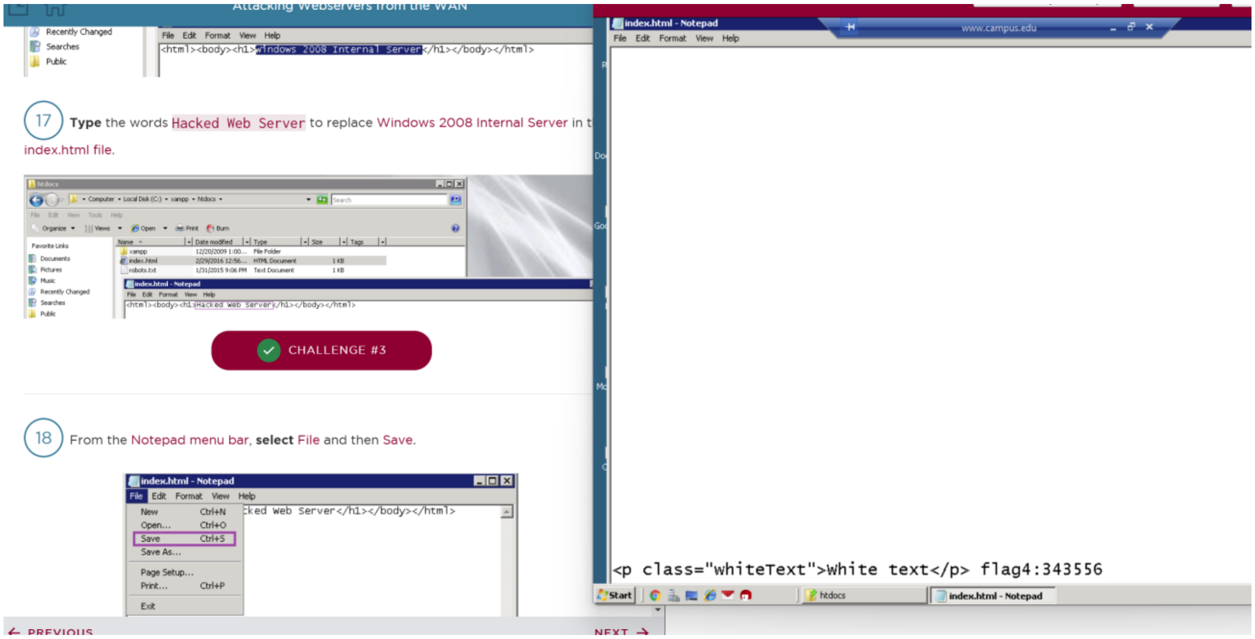
2 In the URL bar, typehttp://www.campus.edu. Then click the arrow button.

Windows 2008 Internal Server

3 Click on the red x in the far right corner to close the Internet Explorer browser.

```
flag:776551
```

This screenshot shows the flag displayed in the "http://www.campus.edu" URL



Attacking Webservers from the WAN

```
<html><body><h1>Windows 2008 Internal Server</h1></body></html>
```

17 **Type** the words `Hacked Web Server` to replace Windows 2008 Internal Server in t index.html file.

Name	Date modified	Type	Size
xampp	12/20/2009 1:00...	File Folder	
index.html	2/29/2016 12:56...	HTML Document	1 KB
robots.txt	1/31/2015 9:06 PM	Text Document	1 KB

```
<html><body><h1>Hacked Web Server</h1></body></html>
```

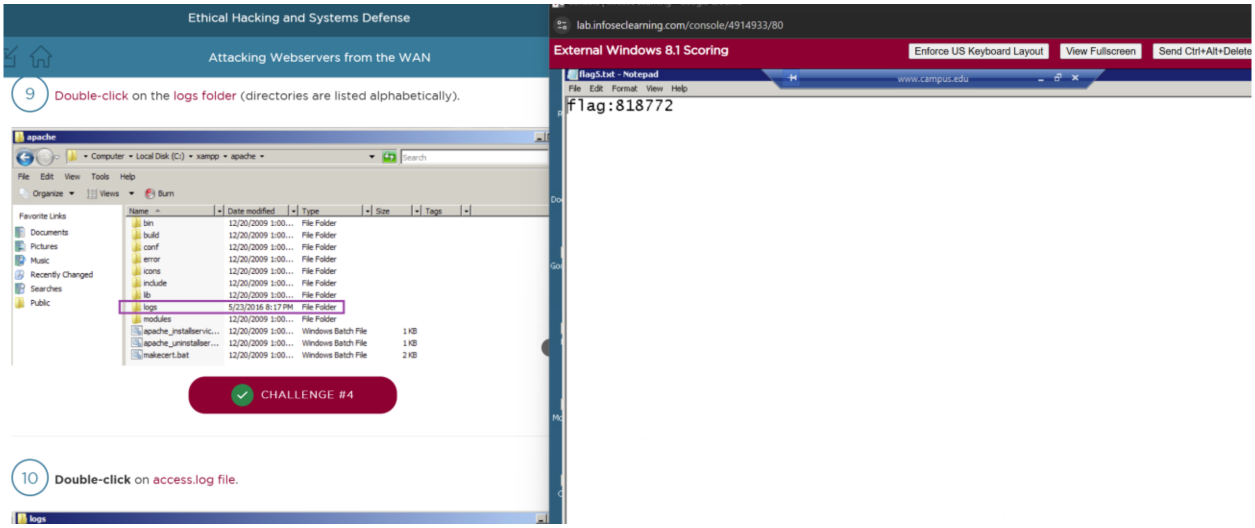
CHALLENGE #3

18 From the Notepad menu bar, **select** File and then Save.

```
cked Web Server</h1></body></html>
```

```
<p class="whiteText">White text</p> flag4:343556
```

This screenshot shows Flag found in the Html file



Ethical Hacking and Systems Defense

Attacking Webservers from the WAN

9 Double-click on the logs folder (directories are listed alphabetically).

Name	Date modified	Type	Size
bin	12/20/2009 1:00...	File Folder	
build	12/20/2009 1:00...	File Folder	
conf	12/20/2009 1:00...	File Folder	
error	12/20/2009 1:00...	File Folder	
icons	12/20/2009 1:00...	File Folder	
include	12/20/2009 1:00...	File Folder	
lib	12/20/2009 1:00...	File Folder	
logs	5/23/2016 8:17 PM	File Folder	
modules	12/20/2009 1:00...	File Folder	
apache_installservic...	12/20/2009 1:00...	Windows Batch File	1 KB
apache_uninstallser...	12/20/2009 1:00...	Windows Batch File	1 KB
makecert.bat	12/20/2009 1:00...	Windows Batch File	2 KB

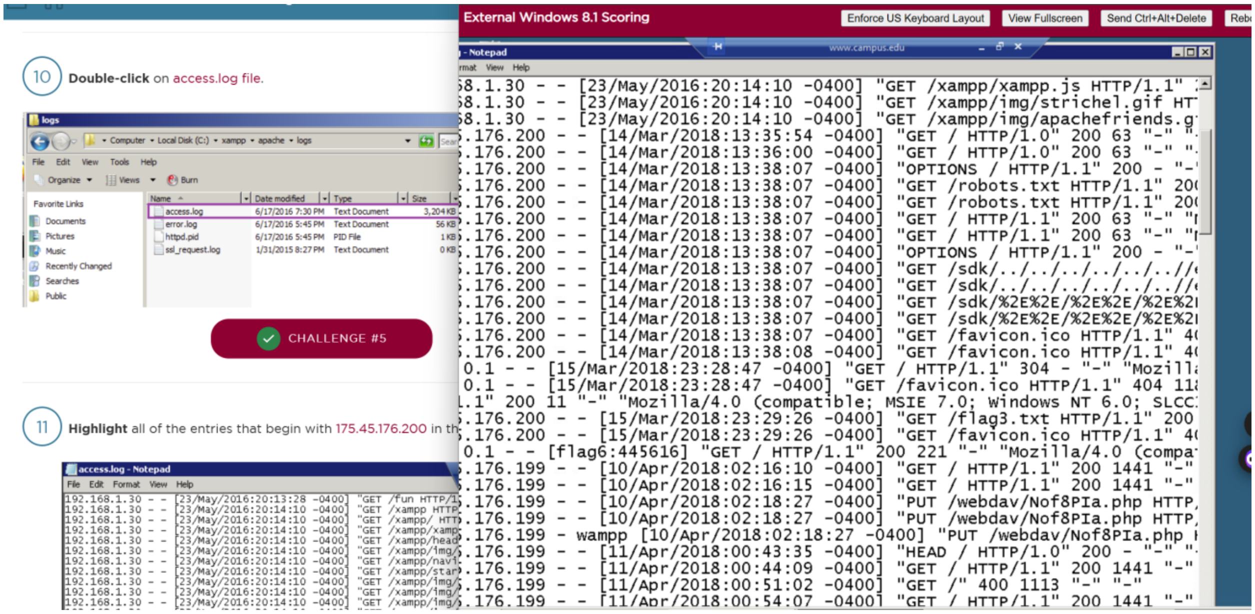
CHALLENGE #4

10 **Double-click** on access.log file.

```
flag:818772
```

lab.infoseclearning.com/console/4914933/80
External Windows 8.1 Scoring
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
flag5.txt - Notepad
www.campus.edu
File Edit Format View Help
apache
Computer ▸ Local Disk (C:) ▸ xampp ▸ apache
logs

This screenshot shows that the flag found in the apache folder



10 **Double-click** on access.log file.

Name	Date modified	Type	Size
access.log	6/17/2016 7:30 PM	Text Document	3,204 KB
error.log	6/17/2016 5:45 PM	Text Document	56 KB
httpd.pid	6/17/2016 5:45 PM	PID File	1 KB
ssl_request.log	1/31/2015 8:27 PM	Text Document	0 KB

11 **Highlight** all of the entries that begin with 175.45.176.200 in th

```
192.168.1.30 - - [23/May/2016:20:13:28 -0400] "GET /fun HTTP/1
192.168.1.30 - - [23/May/2016:20:14:10 -0400] "GET /xampp HTTP
192.168.1.30 - - [23/May/2016:20:14:10 -0400] "GET /xampp/ HTT
192.168.1.30 - - [23/May/2016:20:14:10 -0400] "GET /xampp/xamp
192.168.1.30 - - [23/May/2016:20:14:10 -0400] "GET /xampp/head
192.168.1.30 - - [23/May/2016:20:14:10 -0400] "GET /xampp/img/
192.168.1.30 - - [23/May/2016:20:14:10 -0400] "GET /xampp/navi
192.168.1.30 - - [23/May/2016:20:14:10 -0400] "GET /xampp/star
192.168.1.30 - - [23/May/2016:20:14:10 -0400] "GET /xampp/img/
192.168.1.30 - - [23/May/2016:20:14:10 -0400] "GET /xampp/img/
192.168.1.30 - - [23/May/2016:20:14:10 -0400] "GET /xampp/img/
```

```
68.1.30 - - [23/May/2016:20:14:10 -0400] "GET /xampp/xampp.js HTTP/1.1"
68.1.30 - - [23/May/2016:20:14:10 -0400] "GET /xampp/img/strichel.gif HT
68.1.30 - - [23/May/2016:20:14:10 -0400] "GET /xampp/img/apachefriends.g
5.176.200 - - [14/Mar/2018:13:35:54 -0400] "GET / HTTP/1.0" 200 63 "-" "
5.176.200 - - [14/Mar/2018:13:36:00 -0400] "GET / HTTP/1.0" 200 63 "-" "
5.176.200 - - [14/Mar/2018:13:38:07 -0400] "OPTIONS / HTTP/1.1" 200 - "-
5.176.200 - - [14/Mar/2018:13:38:07 -0400] "GET /robots.txt HTTP/1.1" 20
5.176.200 - - [14/Mar/2018:13:38:07 -0400] "GET /robots.txt HTTP/1.1" 20
5.176.200 - - [14/Mar/2018:13:38:07 -0400] "GET / HTTP/1.1" 200 63 "-" "
5.176.200 - - [14/Mar/2018:13:38:07 -0400] "GET / HTTP/1.1" 200 63 "-" "
5.176.200 - - [14/Mar/2018:13:38:07 -0400] "OPTIONS / HTTP/1.1" 200 - "-
5.176.200 - - [14/Mar/2018:13:38:07 -0400] "GET /sdk/../../../../../../
5.176.200 - - [14/Mar/2018:13:38:07 -0400] "GET /sdk/../../../../../../
5.176.200 - - [14/Mar/2018:13:38:07 -0400] "GET /sdk/%2E%2E/%2E%2E/%2E%2
5.176.200 - - [14/Mar/2018:13:38:07 -0400] "GET /sdk/%2E%2E/%2E%2E/%2E%2
5.176.200 - - [14/Mar/2018:13:38:07 -0400] "GET /favicon.ico HTTP/1.1" 4
5.176.200 - - [14/Mar/2018:13:38:08 -0400] "GET /favicon.ico HTTP/1.1" 4
 0.1 - - [15/Mar/2018:23:28:47 -0400] "GET / HTTP/1.1" 304 - "-" "Mozill
 0.1 - - [15/Mar/2018:23:28:47 -0400] "GET /favicon.ico HTTP/1.1" 404 11
1.1" 200 11 "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; SLCC
5.176.200 - - [15/Mar/2018:23:29:26 -0400] "GET /flag3.txt HTTP/1.1" 200
5.176.200 - - [15/Mar/2018:23:29:26 -0400] "GET /favicon.ico HTTP/1.1" 4
 0.1 - - [flag6:445616] "GET / HTTP/1.1" 200 221 "-" "Mozilla/4.0 (compa
5.176.199 - - [10/Apr/2018:02:16:10 -0400] "GET / HTTP/1.1" 200 1441 "-"
5.176.199 - - [10/Apr/2018:02:16:15 -0400] "GET / HTTP/1.1" 200 1441 "-"
5.176.199 - - [10/Apr/2018:02:18:27 -0400] "PUT /webdav/Nof8PIa.php HTTP
5.176.199 - - [10/Apr/2018:02:18:27 -0400] "PUT /webdav/Nof8PIa.php HTTP
5.176.199 - wampp [10/Apr/2018:02:18:27 -0400] "PUT /webdav/Nof8PIa.php
5.176.199 - - [11/Apr/2018:00:43:35 -0400] "HEAD / HTTP/1.0" 200 - "-" "
5.176.199 - - [11/Apr/2018:00:44:09 -0400] "GET / HTTP/1.1" 200 1441 "-"
5.176.199 - - [11/Apr/2018:00:51:02 -0400] "GET /" 400 1113 "-" "-"
5.176.199 - - [11/Apr/2018:00:54:07 -0400] "GET / HTTP/1.1" 200 1441 "-"
```

The screenshot shows that the file found in the access.log file

Conclusion & Wrap-Up

Summary with:

Observations

In this lab, I attacked a web server from the WAN using Kali Linux. I started by scanning the network with nmap to find open ports. I found that the SMTP port was open, so I used Bruter to perform a dictionary attack and captured the administrator credentials. After gaining access, I used RDP to log into the victim machine, defaced the website, and then covered my tracks by removing log entries that showed my actions.

Identified risks

One major risk is the exposure of the SMTP service to the WAN. If critical services like SMTP are left open to the internet, attackers can easily target them using tools like Bruter to perform brute-force password attacks. Another risk is the use of weak passwords for administrative accounts. When passwords are easy to guess or not complex enough, they become a target for brute-force attacks. Additionally, allowing attackers to deface the website and remove logs means they can cause damage and hide their actions, making it harder to detect and respond to the attack.

Suggested recommendations

To reduce risks, I recommend restricting access to critical services like SMTP by using firewalls to block unauthorized traffic. Additionally, enforce the use of strong passwords and consider using multi-factor authentication (MFA) to protect admin accounts. Regularly monitor and analyze logs to detect suspicious activity and maintain a secure logging system that can't be easily tampered with. Lastly, ensure that all software and systems are regularly updated to patch known vulnerabilities.

Successes & failures

I successfully performed a dictionary attack, captured the credentials, accessed the system via RDP, defaced the website, and removed my traces. However, the lab environment was controlled, so it didn't include real-world security measures like intrusion detection systems (IDS), which would have made the attack more challenging.

Challenges

The main challenge was performing the dictionary attack using Bruter, as I had to choose the right wordlist to crack the password. After gaining access, it was tricky to completely cover my tracks in the logs, as doing this without detection would be more difficult in a real-world environment with advanced monitoring systems.

Table outlining the identified risks, their priority, and suggested remediation

Risk	Priority	Remediation	**What & Why**
Exposing SMTP service to the WAN	High	Use firewalls to restrict access to SMTP and other critical services, allowing access only from trusted internal networks.	Exposing SMTP makes it vulnerable to brute-force attacks, allowing unauthorized access to email systems.
Weak or easily guessable passwords	High	Enforce strong password policies, requiring complex and unique passwords for all admin accounts. Implement multi-factor authentication (MFA).	Weak passwords can be easily cracked, giving attackers access to critical systems and data.
Allowing attackers to deface the website	Medium	Regularly back up website content and implement web application firewalls (WAFs) to detect and block unauthorized change	Attackers can modify or deface a website, causing reputational and financial damage.
Ability to cover tracks in log files	Medium	Enable detailed logging and ensure that logs are stored securely and monitored to detect tampering or unauthorized activities.	Attackers can erase logs, hiding their actions and making detection difficult.