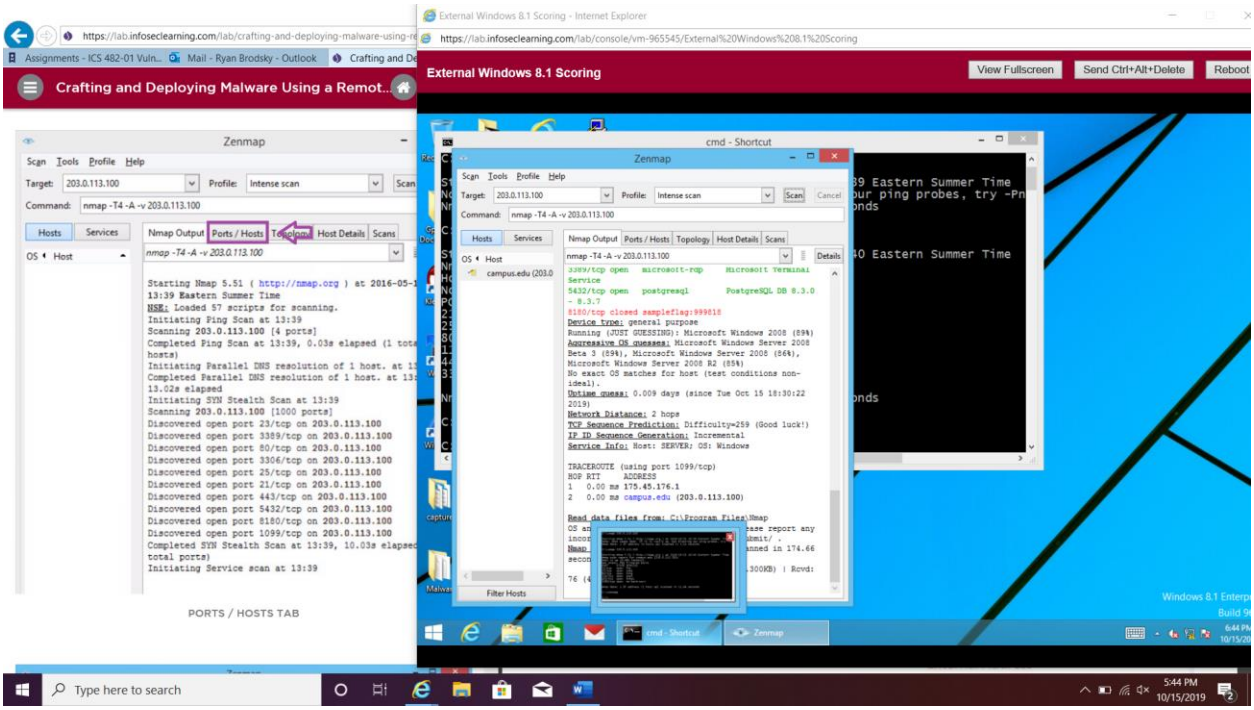
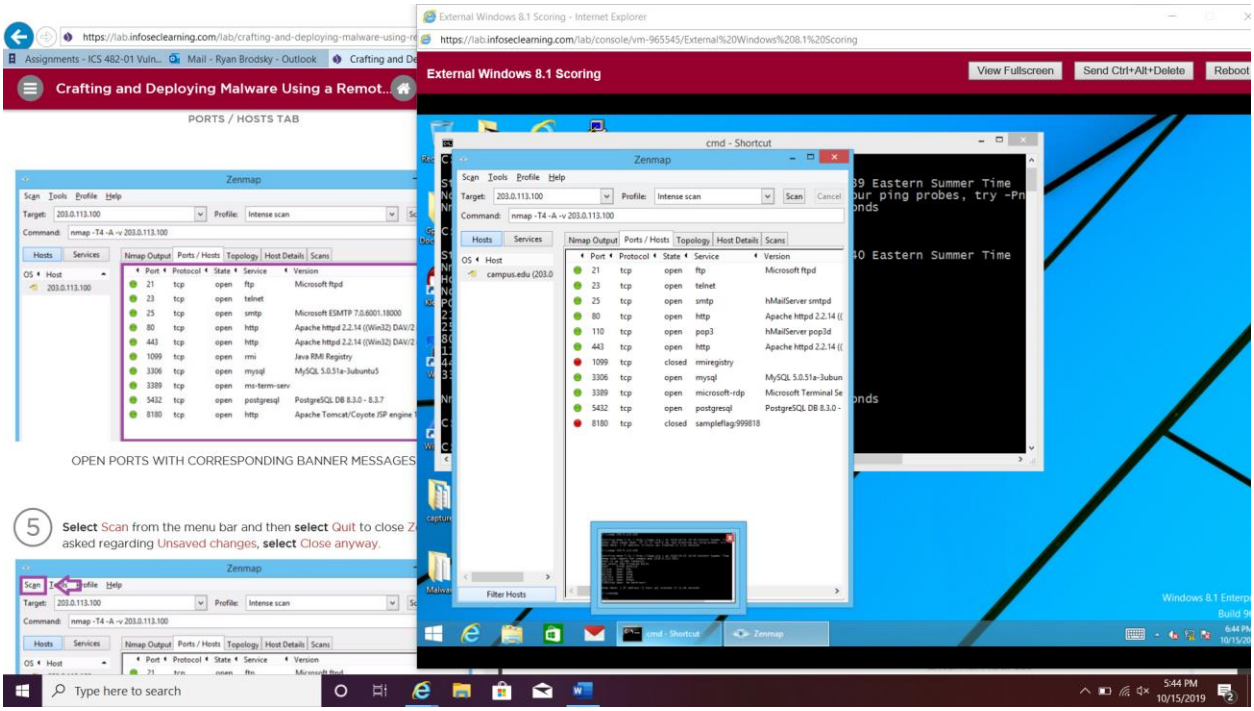
Ryan Brodsky

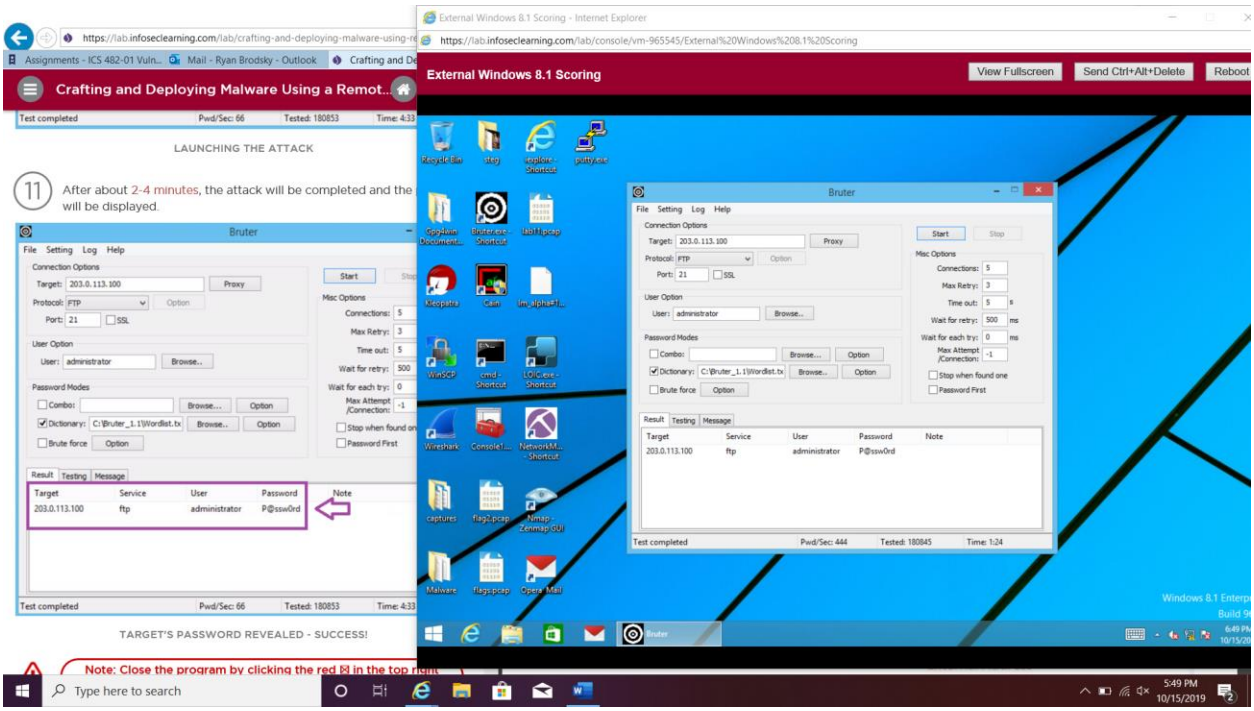
ICS 482

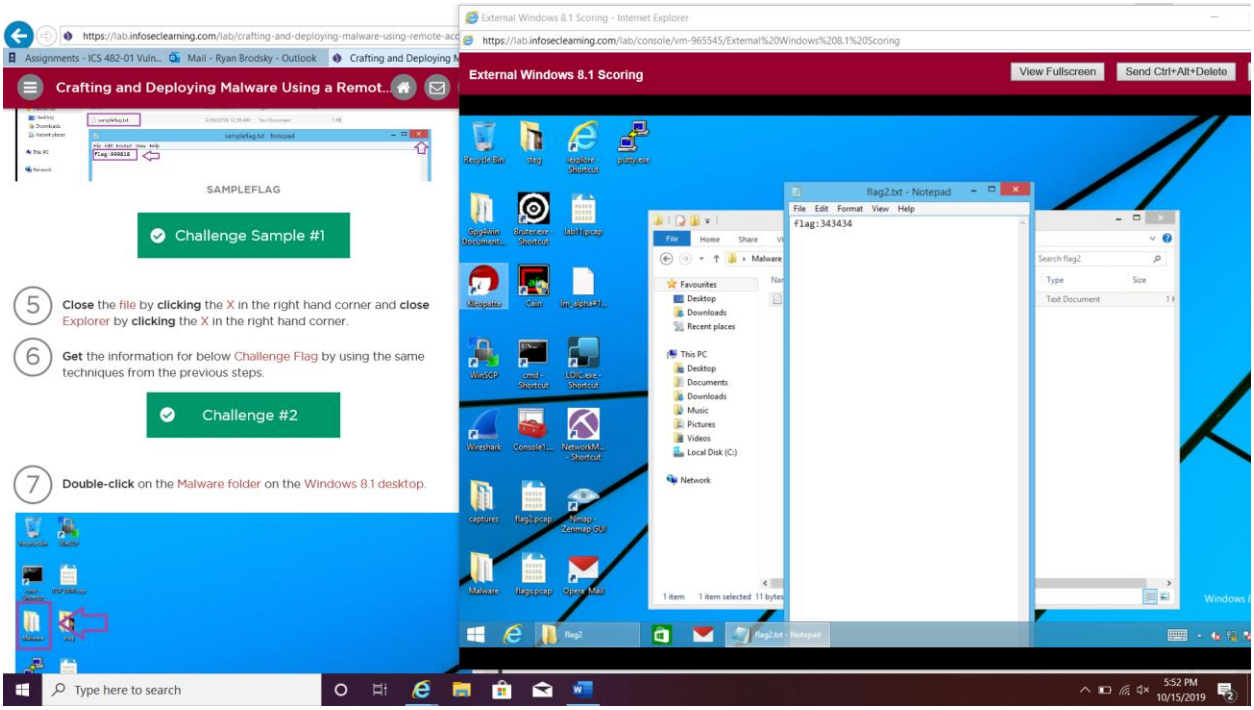
10/15/19

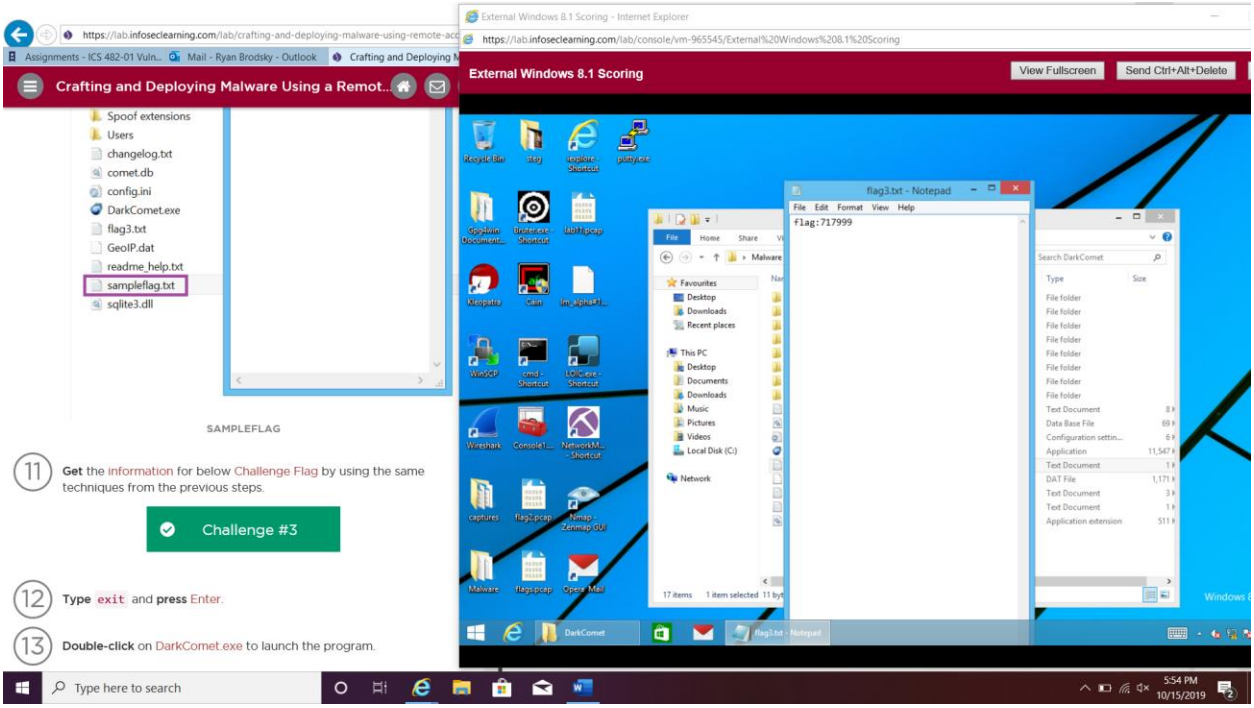
InfoSec Lab: Crafting and Deploying Malware Using a Remote Access Trojan (RAT)






Crafting and Deploying Malware Using a Remot...
LAUNCHING THE ATTACK
11
After about 2-4 minutes, the attack will be completed and the
will be displayed.
Bruter
Target 203.0.113.100
Service ftp
User administrator
Password P@ssw0rd
TARGET'S PASSWORD REVEALED - SUCCESS!
Note: Close the program by clicking the red ☒ in the top right
External Windows 8.1 Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Type here to search
5:49 PM
10/15/2019


Crafting and Deploying Malware Using a Remot...
SAMPLEFLAG
Challenge Sample #1
5
Close the file by clicking the X in the right hand corner and close Explorer by clicking the X in the right hand corner.
6
Get the information for below Challenge Flag by using the same techniques from the previous steps.
Challenge #2
7
Double-click on the Malware folder on the Windows 8.1 desktop.
External Windows 8.1 Scoring
View Fullscreen
Send Ctrl+Alt+Delete
flag2.txt - Notepad
flag:343434
Type here to search
5:52 PM
10/15/2019



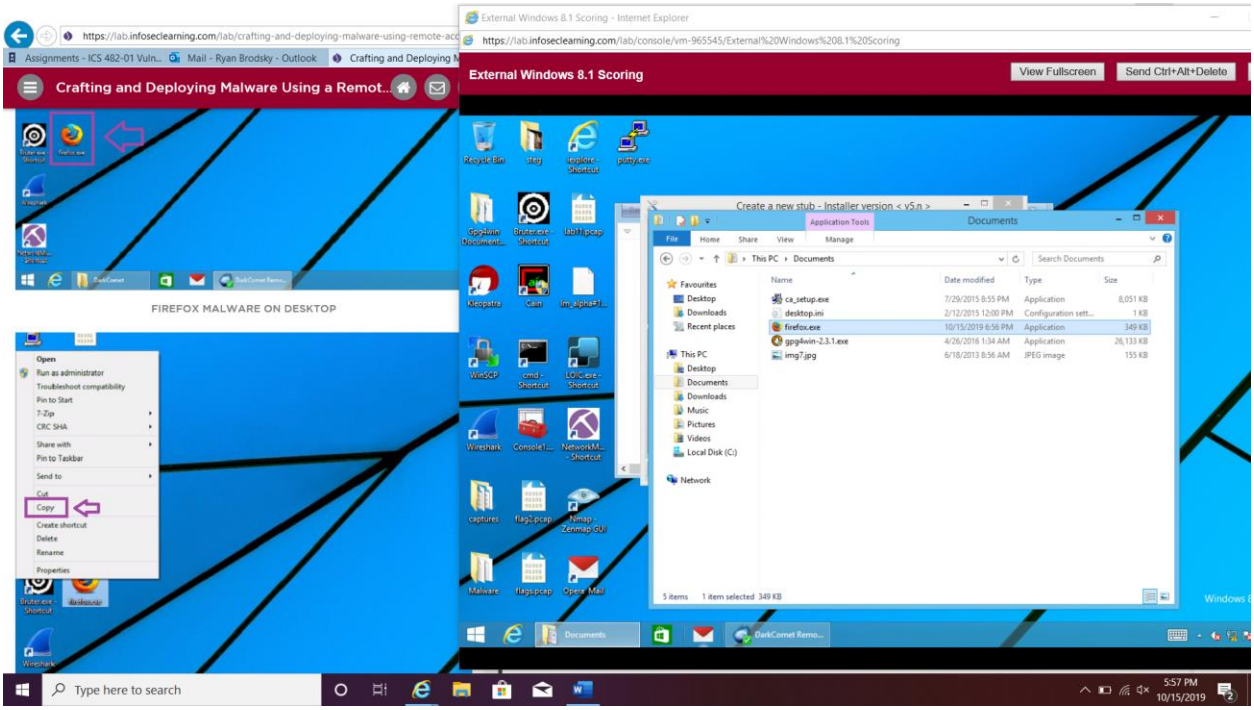
SAMPLEFLAG

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

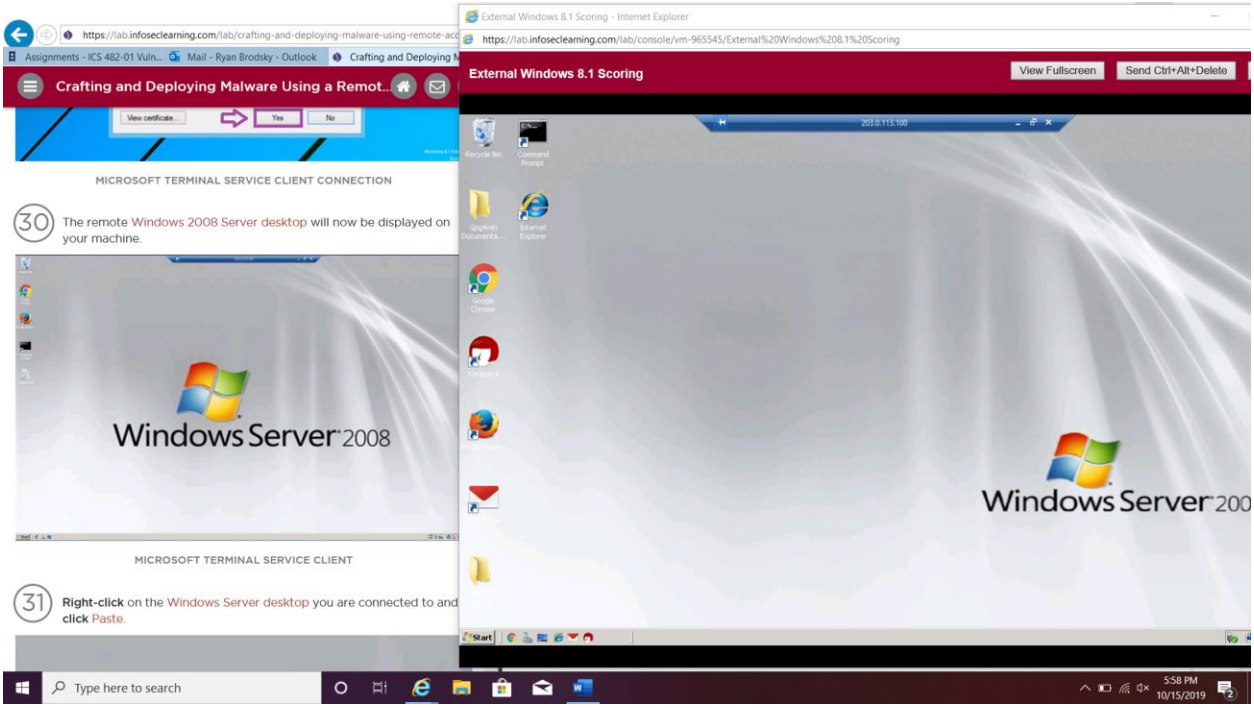
Challenge #3

12 **Type** `exit` and **press** Enter.

13 **Double-click** on DarkComet.exe to launch the program.



FIREFOX MALWARE ON DESKTOP

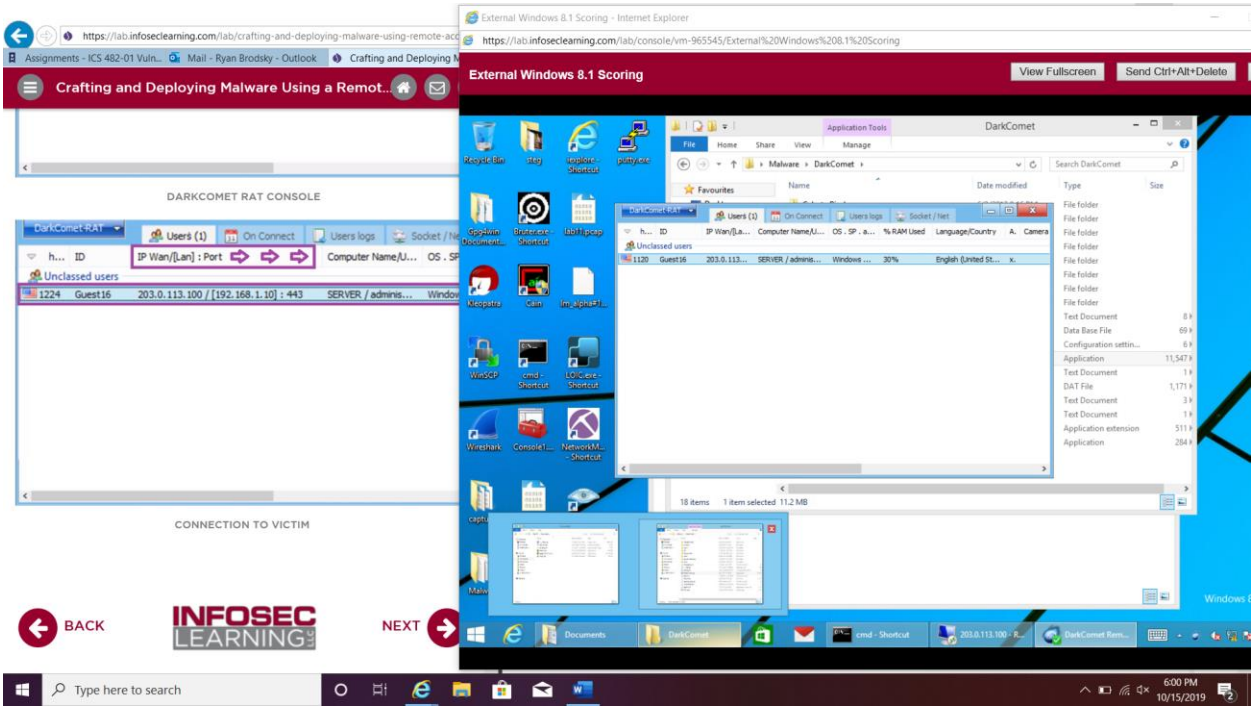


MICROSOFT TERMINAL SERVICE CLIENT CONNECTION

30 The remote Windows 2008 Server desktop will now be displayed on your machine.

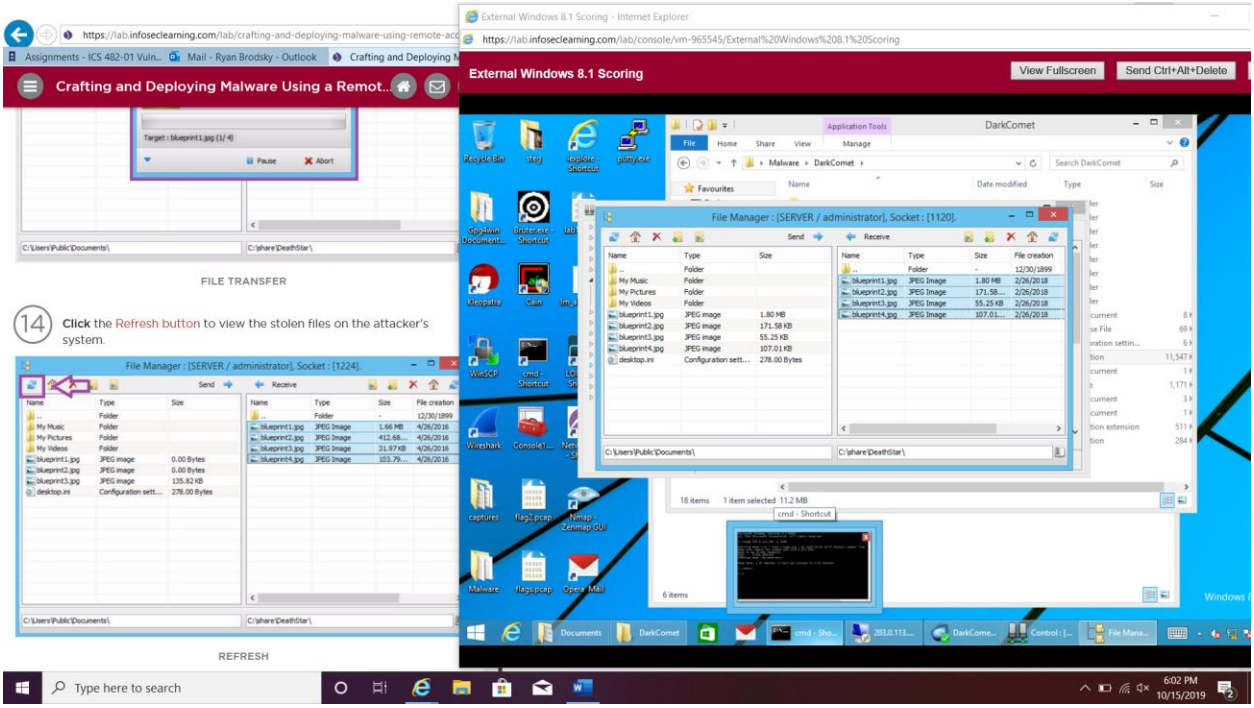
MICROSOFT TERMINAL SERVICE CLIENT

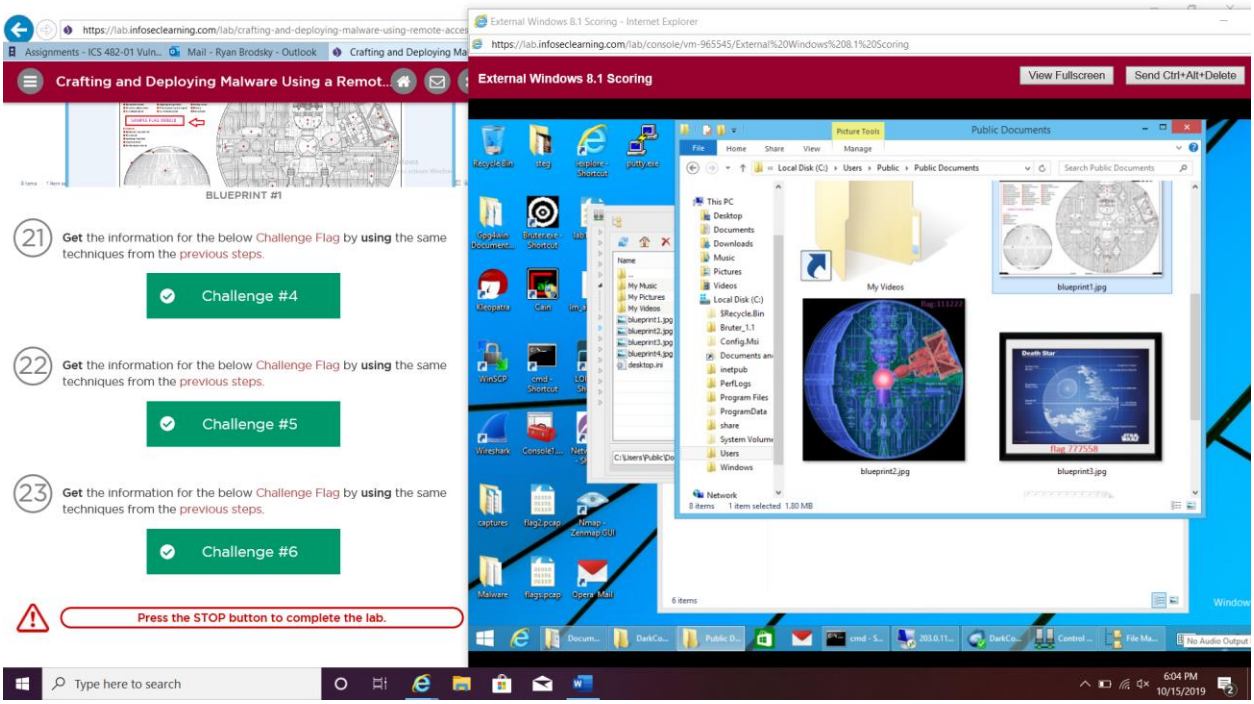
31 **Right-click** on the Windows Server desktop you are connected to and **click** Paste.



DARKCOMET RAT CONSOLE

CONNECTION TO VICTIM


https://lab.infoseclearning.com/lab/crafting-and-deploying-malware-using-remote-acc
Assignments - ICS 482-01 Vuln...
Mail - Ryan Brodsky - Outlook
Crafting and Deploying M
Crafting and Deploying Malware Using a Remot...
External Windows 8.1 Scoring - Internet Explorer
https://lab.infoseclearning.com/lab/console/vm-965545/External%20Windows%208.1%20Scoring
External Windows 8.1 Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Target : blueprint1.jpg (1/ 4)
Pause
Abort
C:\Users\Public\Documents\
C:\share\DeathStar\
FILE TRANSFER
14
Click the Refresh button to view the stolen files on the attacker's system.
File Manager : [SERVER / administrator], Socket : [1224].
Send
Receive
REFRESH
File Manager : [SERVER / administrator], Socket : [1120].
DarkComet
Type here to search
6:02 PM
10/15/2019


https://lab.infoseclearning.com/lab/crafting-and-deploying-malware-using-remote-acces
Assignments - ICS 482-01 Vuln...
Mail - Ryan Brodsky - Outlook
Crafting and Deploying Ma
Crafting and Deploying Malware Using a Remot...
External Windows 8.1 Scoring - Internet Explorer
https://lab.infoseclearning.com/lab/console/vm-965545/External%20Windows%208.1%20Scoring
External Windows 8.1 Scoring
View Fullscreen
Send Ctrl+Alt+Delete
BLUEPRINT #1
21
Get the information for the below Challenge Flag by using the same techniques from the previous steps.
Challenge #4
22
Get the information for the below Challenge Flag by using the same techniques from the previous steps.
Challenge #5
23
Get the information for the below Challenge Flag by using the same techniques from the previous steps.
Challenge #6
Press the STOP button to complete the lab.
Public Documents
My Videos
blueprint1.jpg
blueprint2.jpg
blueprint3.jpg
Type here to search
6:04 PM
10/15/2019