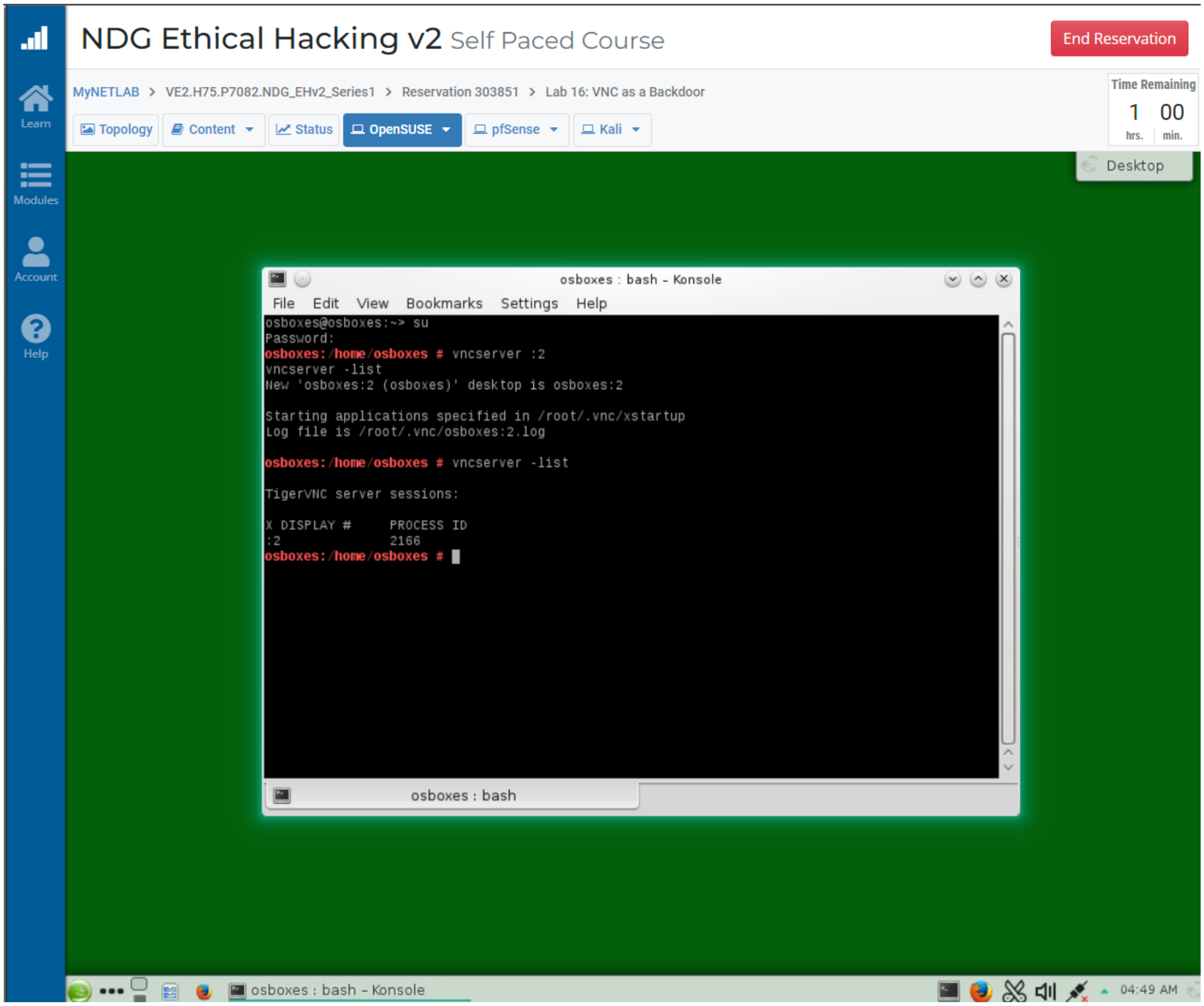
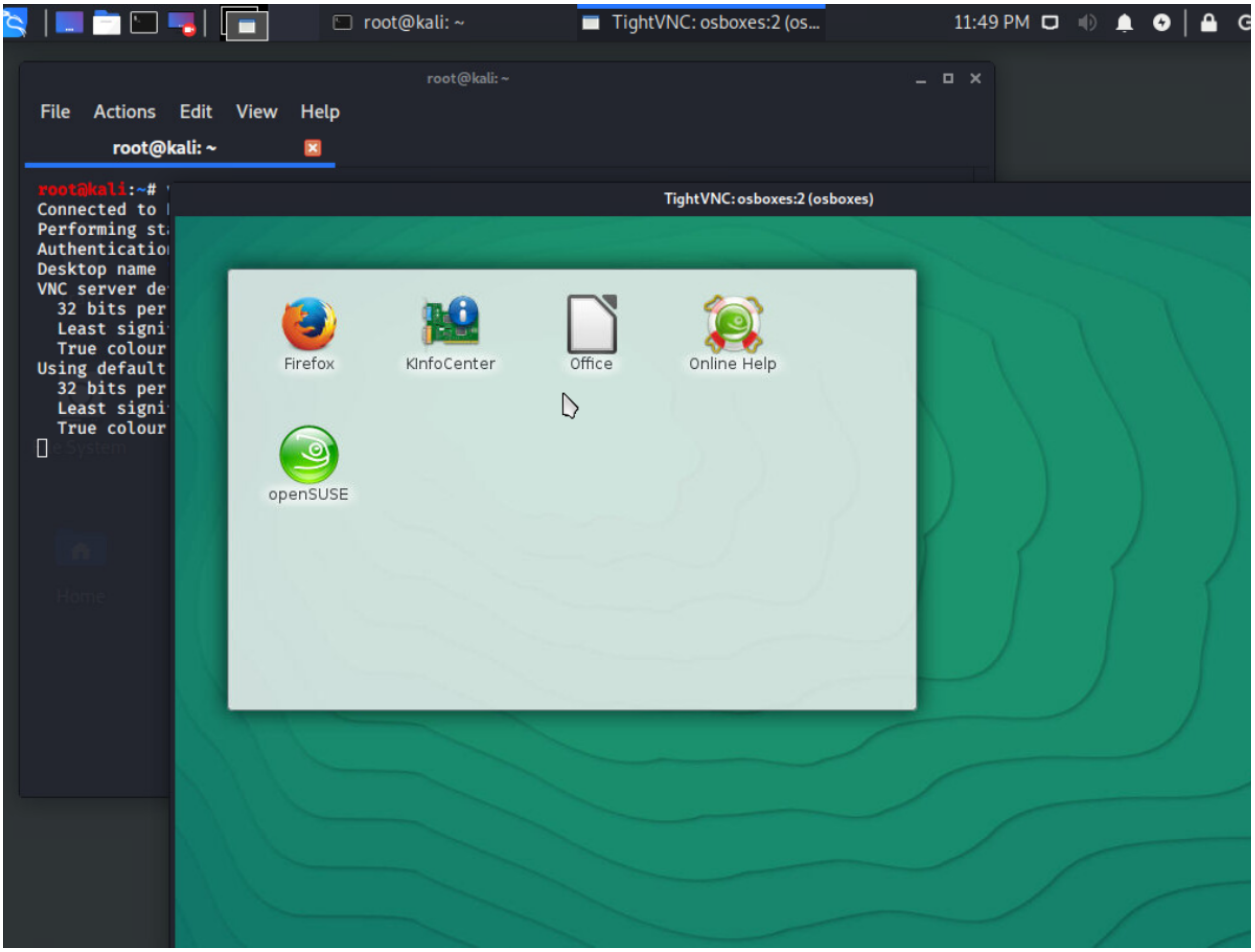
JasoJason Palmeri
CS53C
Lab 16
Timothy Ryan

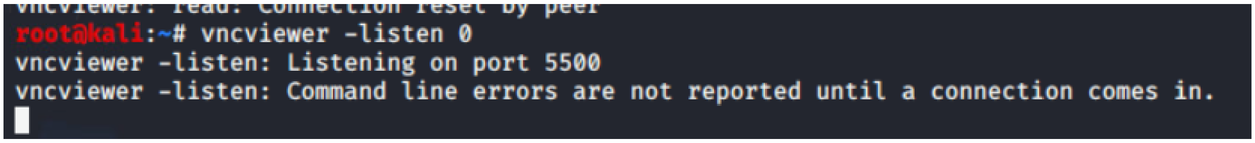
Lab #16: VNC Backdoor


NDG Ethical Hacking v2 Self Paced Course
End Reservation
MyNETLAB > VE2.H75.P7082.NDG_EHv2_Series1 > Reservation 303851 > Lab 16: VNC as a Backdoor
Topology
Content
Status
OpenSUSE
pfSense
Kali
Time Remaining 1 hrs. 00 min.
Learn
Modules
Account
Help
Desktop
osboxes : bash – Konsole
File Edit View Bookmarks Settings Help
osboxes : bash
osboxes : bash – Konsole
04:49 AM

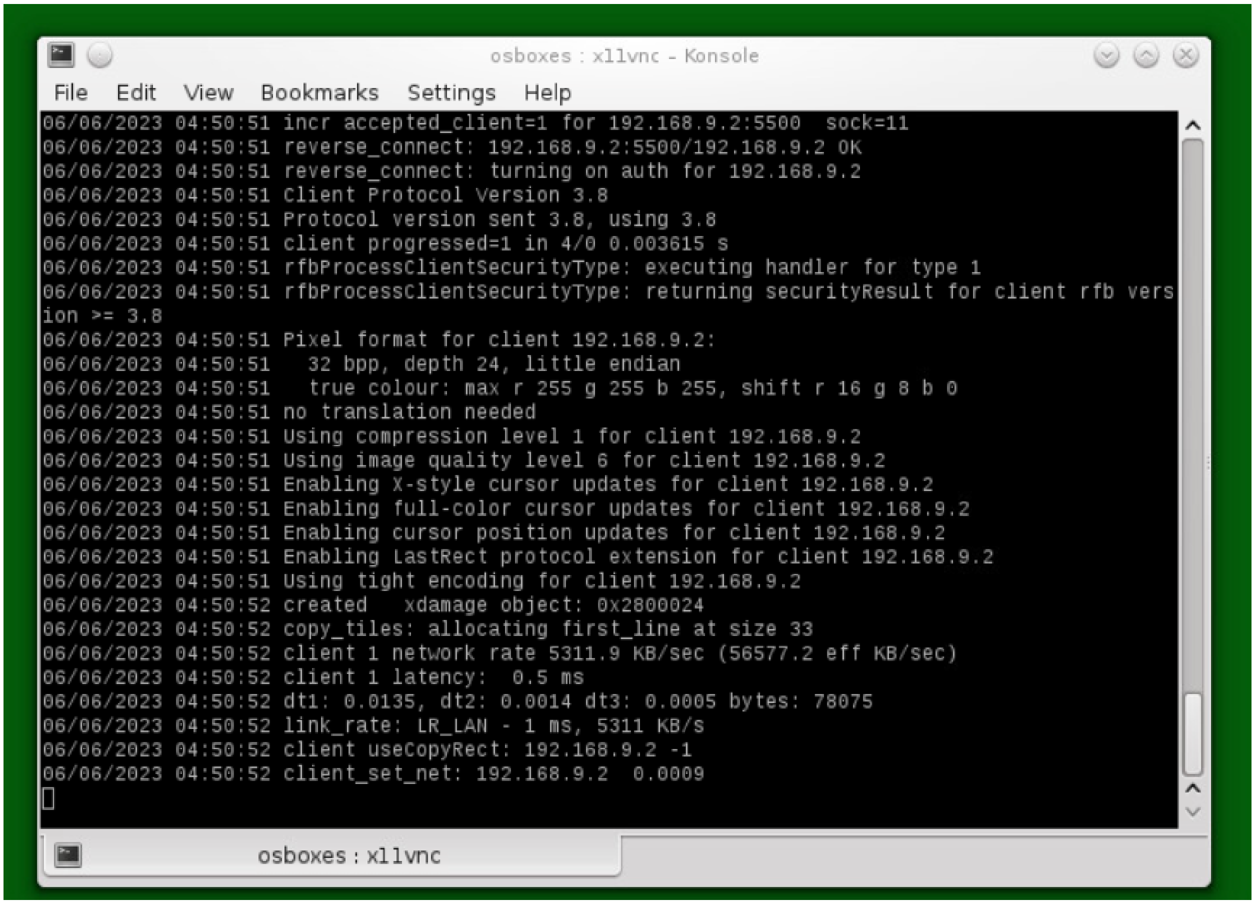
```
osboxes@osboxes:~> su
Password:
osboxes:/home/osboxes # vncserver :2
vncserver -list
New 'osboxes:2 (osboxes)' desktop is osboxes:2

Starting applications specified in /root/.vnc/xstartup
Log file is /root/.vnc/osboxes:2.log

osboxes:/home/osboxes # vncserver -list

TigerVNC server sessions:

X DISPLAY #     PROCESS ID
:2              2166
osboxes:/home/osboxes #
```



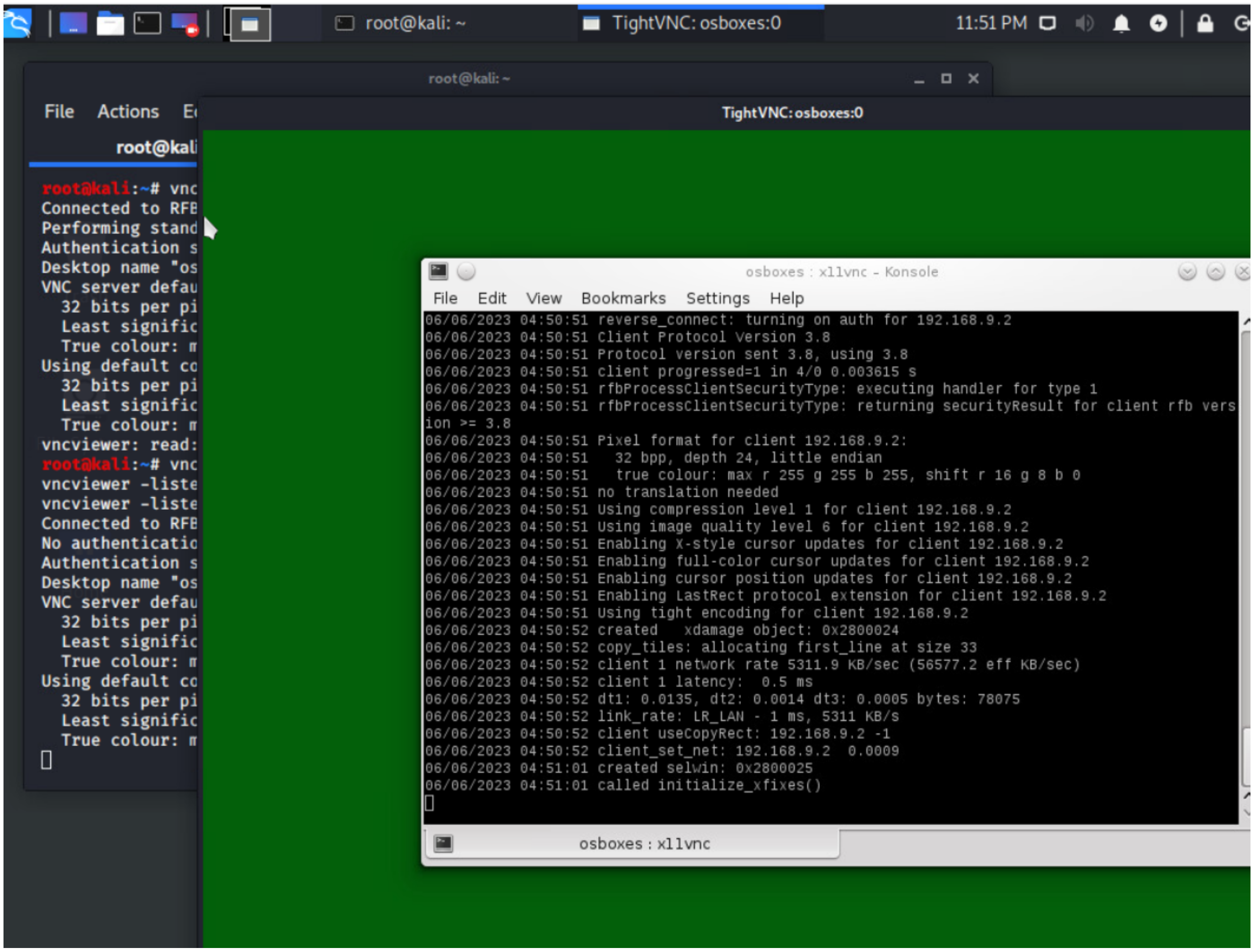
```
root@kali:~# 
Connected to 
Performing st
Authenticatio
Desktop name 
VNC server de
  32 bits per
  Least signi
  True colour
Using default
  32 bits per
  Least signi
  True colour
```



```
vncviewer: read: Connection reset by peer
root@kali:~# vncviewer -listen 0
vncviewer -listen: Listening on port 5500
vncviewer -listen: Command line errors are not reported until a connection comes in.
█
```



```
06/06/2023 04:50:51 incr accepted_client=1 for 192.168.9.2:5500  sock=11
06/06/2023 04:50:51 reverse_connect: 192.168.9.2:5500/192.168.9.2 OK
06/06/2023 04:50:51 reverse_connect: turning on auth for 192.168.9.2
06/06/2023 04:50:51 Client Protocol Version 3.8
06/06/2023 04:50:51 Protocol version sent 3.8, using 3.8
06/06/2023 04:50:51 client progressed=1 in 4/0 0.003615 s
06/06/2023 04:50:51 rfbProcessClientSecurityType: executing handler for type 1
06/06/2023 04:50:51 rfbProcessClientSecurityType: returning securityResult for client rfb vers
ion >= 3.8
06/06/2023 04:50:51 Pixel format for client 192.168.9.2:
06/06/2023 04:50:51   32 bpp, depth 24, little endian
06/06/2023 04:50:51   true colour: max r 255 g 255 b 255, shift r 16 g 8 b 0
06/06/2023 04:50:51 no translation needed
06/06/2023 04:50:51 Using compression level 1 for client 192.168.9.2
06/06/2023 04:50:51 Using image quality level 6 for client 192.168.9.2
06/06/2023 04:50:51 Enabling X-style cursor updates for client 192.168.9.2
06/06/2023 04:50:51 Enabling full-color cursor updates for client 192.168.9.2
06/06/2023 04:50:51 Enabling cursor position updates for client 192.168.9.2
06/06/2023 04:50:51 Enabling LastRect protocol extension for client 192.168.9.2
06/06/2023 04:50:51 Using tight encoding for client 192.168.9.2
06/06/2023 04:50:52 created   xdamage object: 0x2800024
06/06/2023 04:50:52 copy_tiles: allocating first_line at size 33
06/06/2023 04:50:52 client 1 network rate 5311.9 KB/sec (56577.2 eff KB/sec)
06/06/2023 04:50:52 client 1 latency:  0.5 ms
06/06/2023 04:50:52 dt1: 0.0135, dt2: 0.0014 dt3: 0.0005 bytes: 78075
06/06/2023 04:50:52 link_rate: LR_LAN - 1 ms, 5311 KB/s
06/06/2023 04:50:52 client useCopyRect: 192.168.9.2 -1
06/06/2023 04:50:52 client_set_net: 192.168.9.2  0.0009
```



```
root@kali:~# vnc
Connected to RFB
Performing stand
Authentication s
Desktop name "os
VNC server defau
  32 bits per pi
  Least signific
  True colour: m
Using default co
  32 bits per pi
  Least signific
  True colour: m
vncviewer: read:
root@kali:~# vnc
vncviewer -liste
vncviewer -liste
Connected to RFB
No authenticatio
Authentication s
Desktop name "os
VNC server defau
  32 bits per pi
  Least signific
  True colour: m
Using default co
  32 bits per pi
  Least signific
  True colour: m
▯
```

```
06/06/2023 04:50:51 reverse_connect: turning on auth for 192.168.9.2
06/06/2023 04:50:51 Client Protocol Version 3.8
06/06/2023 04:50:51 Protocol version sent 3.8, using 3.8
06/06/2023 04:50:51 client progressed=1 in 4/0 0.003615 s
06/06/2023 04:50:51 rfbProcessClientSecurityType: executing handler for type 1
06/06/2023 04:50:51 rfbProcessClientSecurityType: returning securityResult for client rfb vers
ion >= 3.8
06/06/2023 04:50:51 Pixel format for client 192.168.9.2:
06/06/2023 04:50:51   32 bpp, depth 24, little endian
06/06/2023 04:50:51   true colour: max r 255 g 255 b 255, shift r 16 g 8 b 0
06/06/2023 04:50:51 no translation needed
06/06/2023 04:50:51 Using compression level 1 for client 192.168.9.2
06/06/2023 04:50:51 Using image quality level 6 for client 192.168.9.2
06/06/2023 04:50:51 Enabling X-style cursor updates for client 192.168.9.2
06/06/2023 04:50:51 Enabling full-color cursor updates for client 192.168.9.2
06/06/2023 04:50:51 Enabling cursor position updates for client 192.168.9.2
06/06/2023 04:50:51 Enabling LastRect protocol extension for client 192.168.9.2
06/06/2023 04:50:51 Using tight encoding for client 192.168.9.2
06/06/2023 04:50:52 created   xdamage object: 0x2800024
06/06/2023 04:50:52 copy_tiles: allocating first_line at size 33
06/06/2023 04:50:52 client 1 network rate 5311.9 KB/sec (56577.2 eff KB/sec)
06/06/2023 04:50:52 client 1 latency:  0.5 ms
06/06/2023 04:50:52 dt1: 0.0135, dt2: 0.0014 dt3: 0.0005 bytes: 78075
06/06/2023 04:50:52 link_rate: LR_LAN - 1 ms, 5311 KB/s
06/06/2023 04:50:52 client useCopyRect: 192.168.9.2 -1
06/06/2023 04:50:52 client_set_net: 192.168.9.2  0.0009
06/06/2023 04:51:01 created selwin: 0x2800025
06/06/2023 04:51:01 called initialize_xfixes()
▯
```