##### **Assignment\_1 (Module 7)**

Topic: Running an Exploit Using the Metasploit Tool

#### **Introduction:**

This report details the process of running an exploit using the Metasploit tool on Kali Linux. The focus was on identifying and testing the EternalBlue exploit (MS17-010) as part of the assignment requirements.

**Steps Followed:**

Step 1: Launch Metasploit

* The msfconsole command was executed in the Kali Linux terminal to start the Metasploit framework.

Step 2: Search for an Exploit

* The search eternalblue command was used to locate the EternalBlue exploit in the Metasploit database.

Step 3: Analyze and Report on the Exploit

* The info exploit/windows/smb/ms17\_010\_psexec command was used to select the exploit.
* The info command provided detailed information about the exploit for reporting.

#### **Exploit Details:**

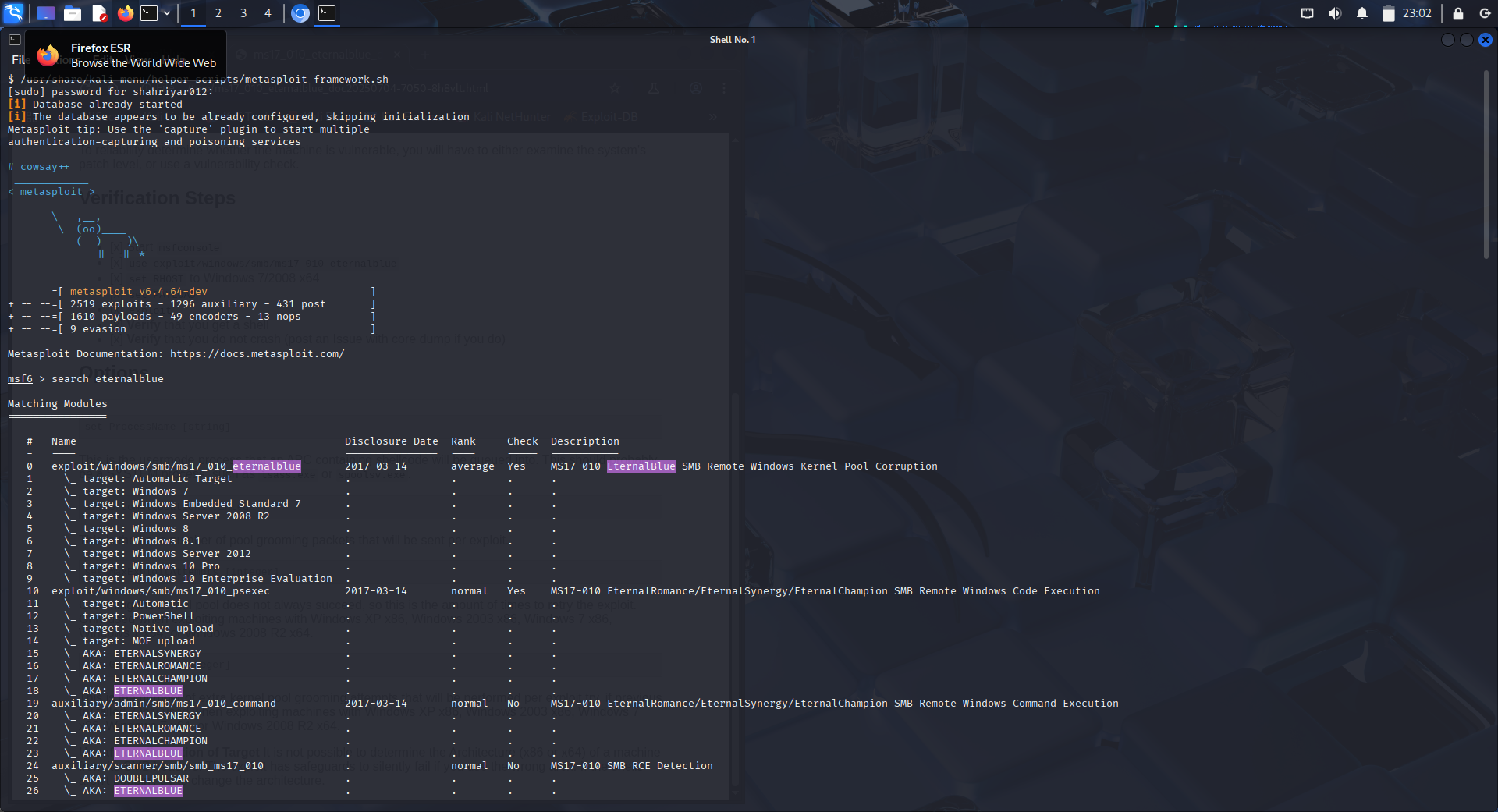
* Name: MS17-010 EternalRomance
* Description: This exploit targets a vulnerability in the Windows SMB (Server Message Block) protocol (CVE-2017-0144), enabling remote code execution.
* How It Works: It creates a kernel pool corruption, allowing an attacker to gain control of the target system.
* Affected Systems: Windows 7, Windows Server 2008 R2, Windows 8.1, etc.
* Disclosure Date: 2017-03-14

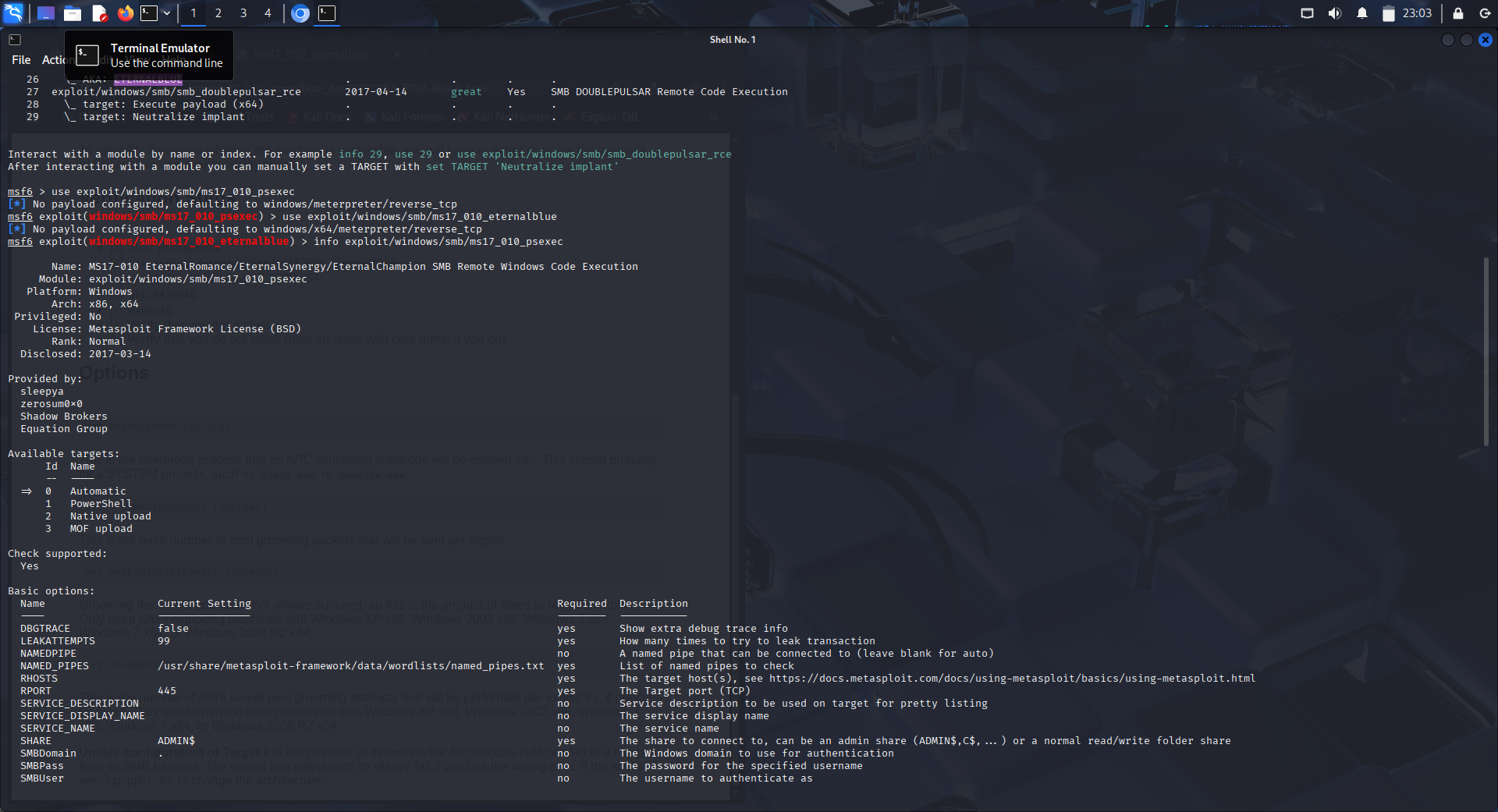
**Attempt and Results:**

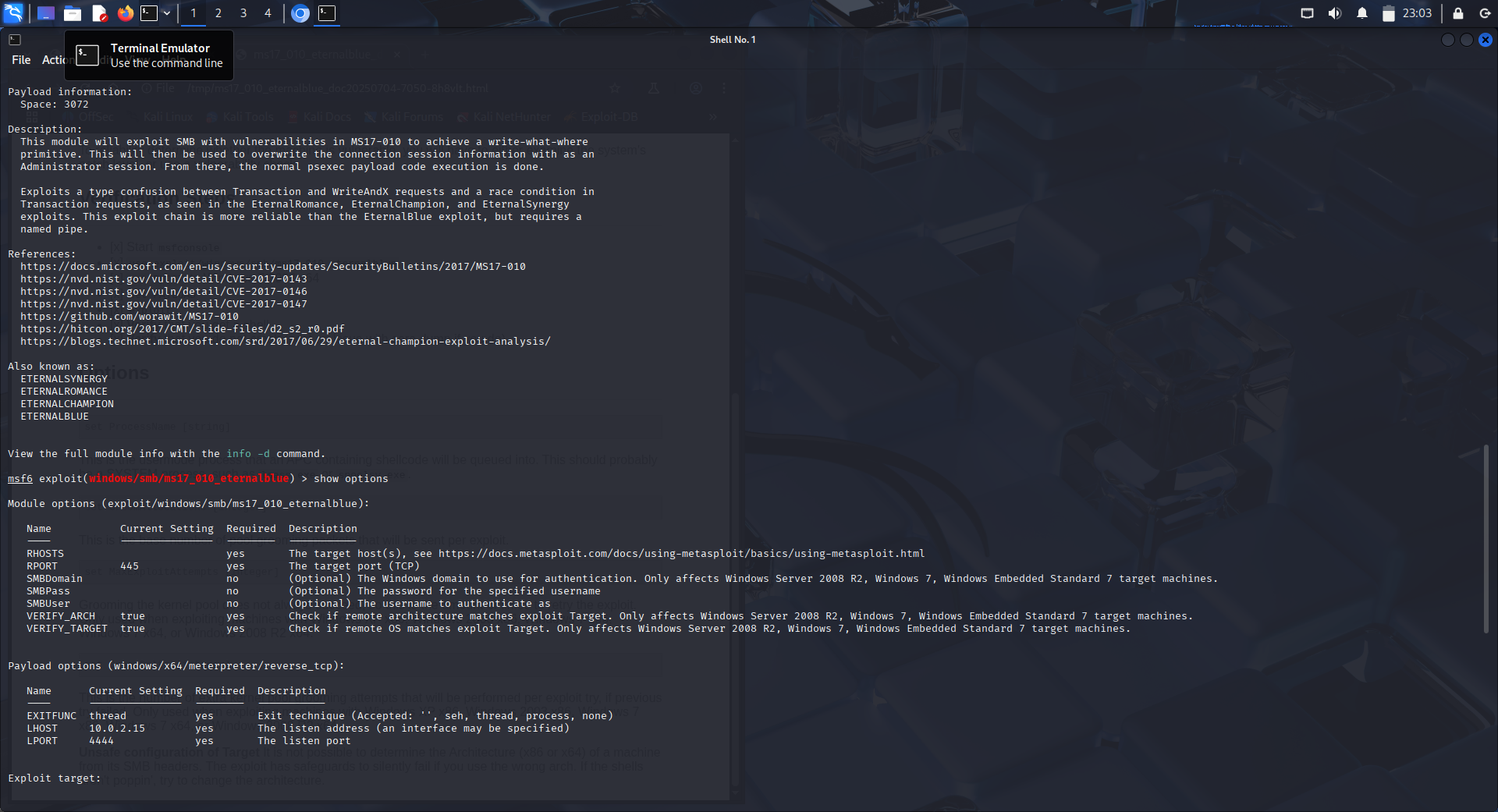
**Configuration:**

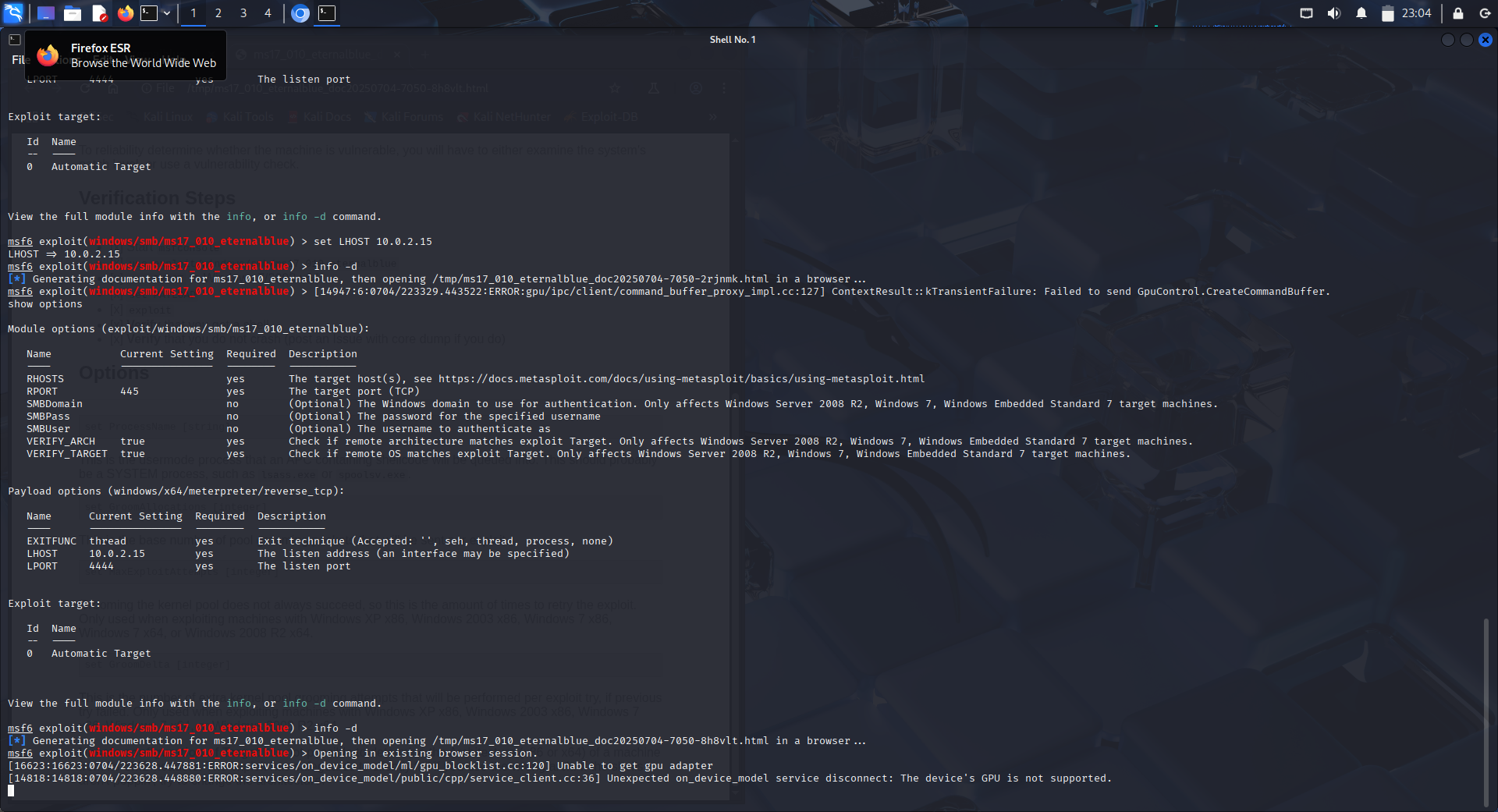
* LHOST was set to the attacker's IP (e.g., 10.0.2.15).
* PAYLOAD was set to windows/x64/meterpreter/reverse\_tcp.
* LPORT was set to 4444.

**Some screenshots of this exploit:**

****

****

****

****

#### **Conclusion:**

The exploration of the EternalBlue exploit using Metasploit has provided a solid understanding of vulnerability assessment and exploit configuration. The process highlighted the importance of proper target setup and the use of appropriate tools for vulnerability scanning. For optimal results, utilizing a controlled environment with a vulnerable system, such as an unpatched Windows 7 virtual machine, is recommended. This experience enhances skills in penetration testing and prepares for advanced security analysis in future tasks.