***Individual Assignment***

1. There was a Known Windows 7 Exploit called “EternalBlue” that can be exploited by Metasploit.
2. What is it?
3. Which vulnerability is exploited by this exploit
4. How does it work
5. How can we exploit it using Metasploit – show with screenshots.

**Answer**

***What is EternalBlue?***

EternalBlue is a software vulnerability in Microsoft’s Windows operating system. It targets the Windows Server Message Block (SMB) protocol, a network protocol that enables shared access to files, printers, and other resources within a network.

The United States National Security Agency (NSA) discovered this vulnerability, and it was a part of their secret toolkit. It became public when a hacker group called the Shadow Brokers leaked the NSA’s tools in April 2017.

***Understanding the Vulnerability***

To grasp the core of the EternalBlue vulnerability, we must understand the SMB protocol. It relies on port 445 to enable network communications, and this is where the flaw resides.

1. **The Bug in SMBv1**: The main issue lies in the handling of specially crafted packets by the SMBv1 protocol. By sending specific requests to a Windows Server running SMBv1, a remote attacker can execute random code on the target system.
2. **DoublePulsar:** Accompanying EternalBlue is DoublePulsar, a backdoor implant tool. Once EternalBlue opens the way, DoublePulsar helps in injecting and running malicious code on a target system.
3. **Lack of Segmentation**: The nature of SMB allows for lateral movement within the network. It allows an attacker to spread the malware from one system to another. It means that once inside, the malicious software could travel through an entire network if not properly segmented.

***How does EternalBlue work***

The EternalBlue 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.

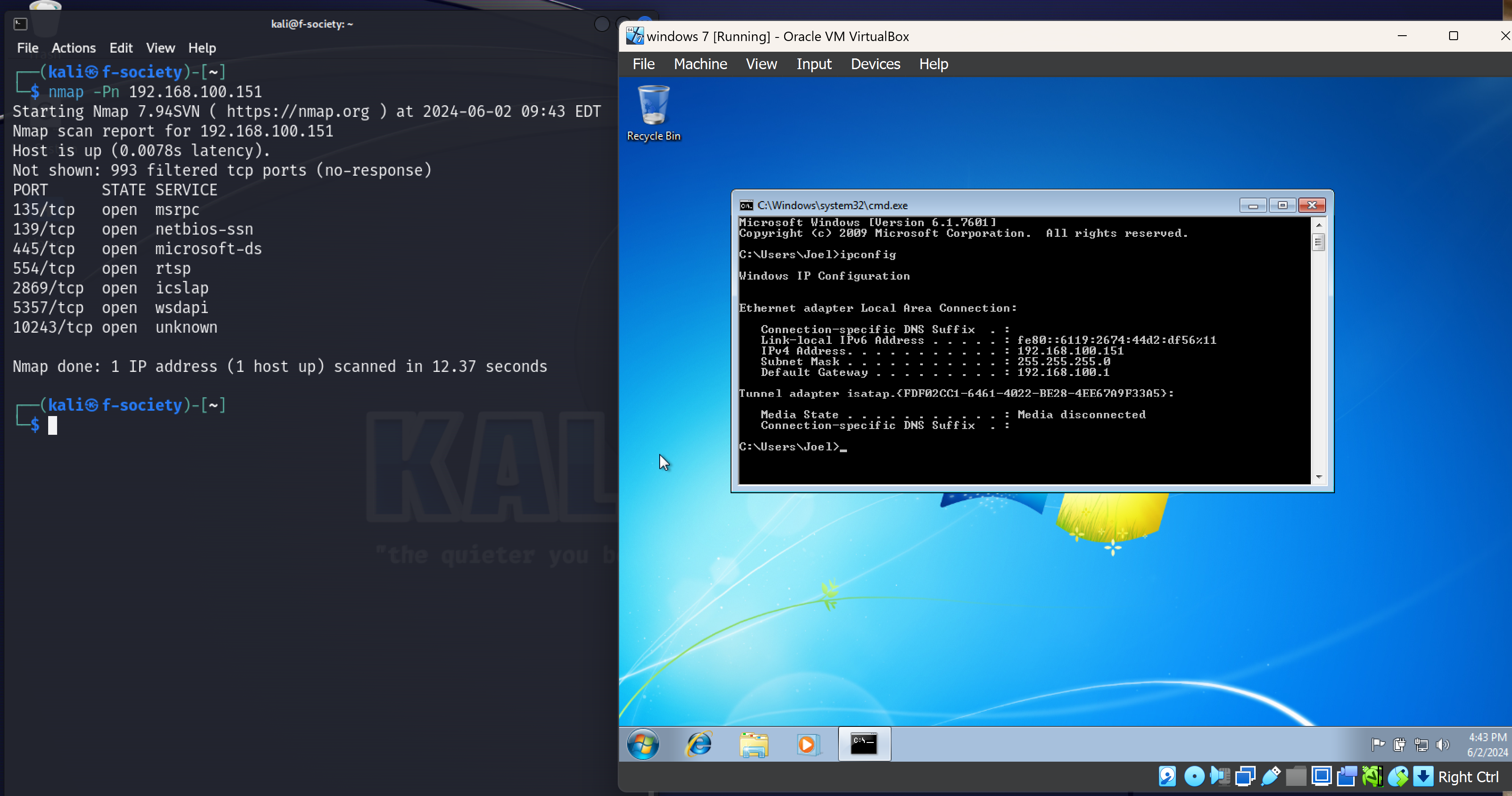
The exploit makes use of the way Microsoft Windows handles, or rather mishandles, specially crafted packets from malicious attackers. All the attacker needs to do is send a maliciously crafted packet to the target server, and, boom, the malware propagates and a cyberattack ensues.

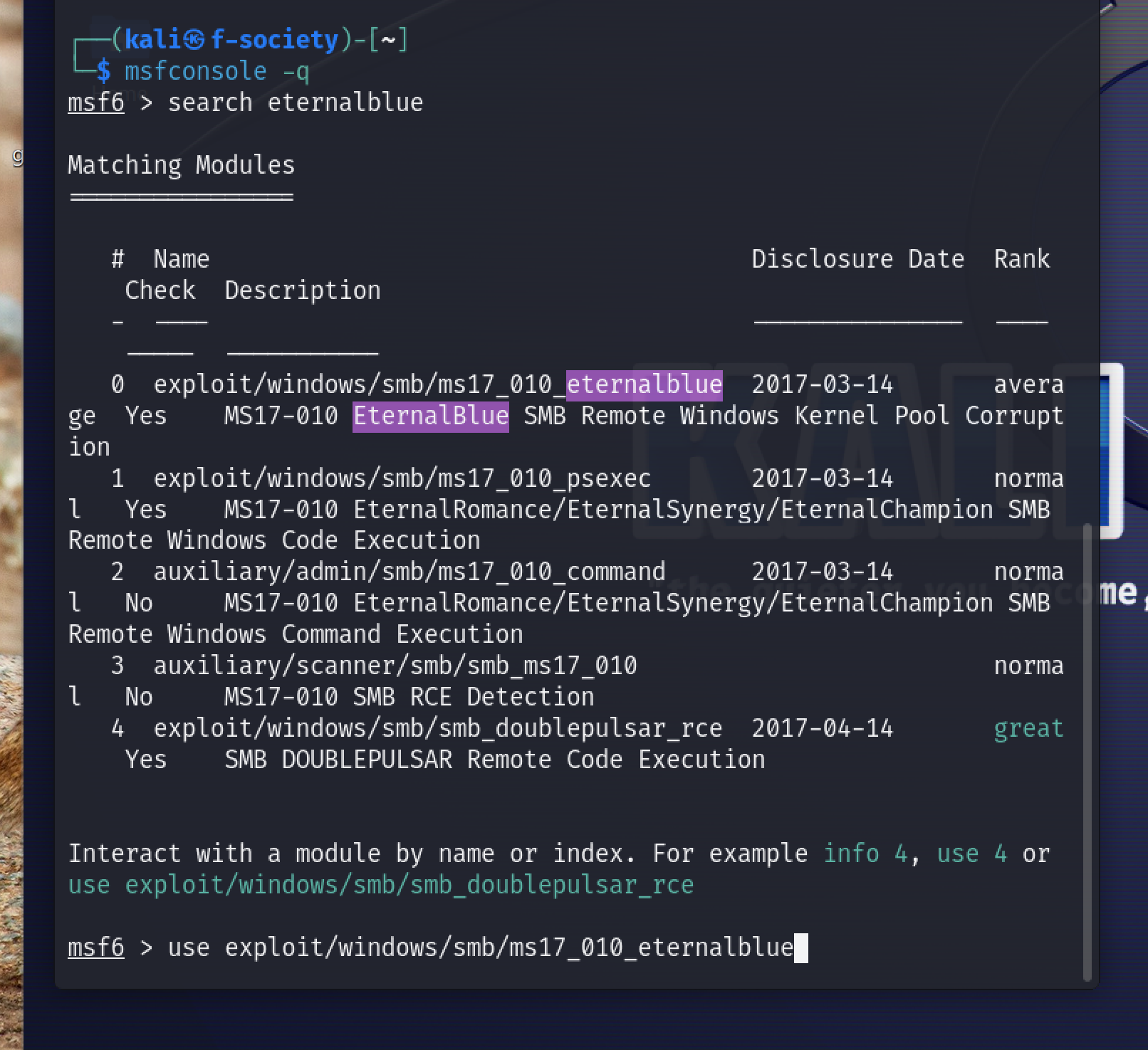
The **WannaCry ransomware** attack was the most notorious one, affecting more than 200,000 computers across 150 countries. It was the first to showcase the full destructive potential of EternalBlue.

Moreover, other malware like **NotPetya** and **Bad Rabbit** also leveraged EternalBlue, causing substantial damage and financial losses.

**NOTE:** EternalBlue's Common Vulnerabilities and Exposures number is logged in the National Vulnerability Database as ***CVE-2017-0144***.

***Showing how we can exploit it***





A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

A computer screen with a screen on it

Description automatically generated