**Step-by-Step Exploitation Process**

**🔹 Step 1: Identify IP Addresses**

Open a terminal on Kali:

* **Ip a or ipconfig**

A computer screen shot of a program

Description automatically generated

Check the Windows 7 IP using:

* **ipconfig**

A computer screen shot of a computer screen

Description automatically generated

**🔹 Step 2: Scan Target with Nmap**

Use Nmap to detect open ports and services:

A screenshot of a computer program

Description automatically generated

Look for port **445 (SMB)** — if it’s open, proceed.

Port 445 open → vulnerable to SMB-based exploits like EternalBlue.

A screenshot of a computer

Description automatically generated

Use this command to check the vulnerability in target machine

**Server Message Block (SMB)** protocol which the SMB creates a connection between the user and the server by sending responses and requests. (Eternal Blue, 2017)

**🔹 Step 3: Launch Metasploit**

Open Metasploit:

* Using **msfconsole**

A screenshot of a computer

Description automatically generated

**🔹 Step 4: Search for EternalBlue or MS17-010**

Search for the exploit:

A screenshot of a computer program

Description automatically generated

You’ll find something like:

* **exploit/windows/smb/ms17\_010\_eternalblue**

**Choose: use 0**

A computer screen shot of a computer code

Description automatically generated

**🔹 Step 6: Configure Exploit Options**

Check current settings:

* **show options**

A screenshot of a computer screen

Description automatically generated

We then select the EternalBlue exploit and type show options to show us all the available setting before we launch the attack, as you can see RHOSTS which is the target system does not have its IP address in there.

Set the **target IP:**

set RHOSTS 10.0.2.4

A screen shot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

This can easily be fixed by using “set RHOSTS 10.0.2.4” which sets the IP to the target system.

**🔹 Step 7: Exploit the Target**

Run the exploit:

A screenshot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated

We then type run and after the process is completed, we gain full access to the system which then we can run any program and could exploit the system in any way that could benefit the unauthorised personnel.