1. Reconnaissance and Target Analysis

**1. Executive Summary**

This test was done on a **Windows XP virtual machine (VM)** to check for security problems. The goal was to find weaknesses, try to exploit them, and then suggest how to fix those weaknesses.

During the test, we found a few big problems:

* **VSFTPD 2.3.4 Backdoor (CVE-2011-2523)**: This vulnerability allowed attackers to gain **full control** of the system.
* **DistCC Daemon Remote Code Execution (CVE-2004-2687)**: This flaw let attackers run commands on the system from anywhere.
* **Old software** like **Apache**, **Samba**, and **MySQL**, which are also risky.

We were able to use these problems to take control of the system. This report explains how to fix these problems, like updating software, securing services, and monitoring the system.

In short, the system is **high-risk** because it has old software and easy-to-fix weaknesses.

**2. Introduction**

**Objective**

The goal of this test was to find weaknesses in the **Windows XP** system, use those weaknesses to get unauthorized access, and then give suggestions on how to fix the system.

**Scope**

* **Target:** The system being tested is a **Windows XP virtual machine**.
* **Methods:** We looked for weaknesses in the system, scanned it for known problems, exploited those problems, and analyzed what could happen next.
* **Limitations:** We did not perform any **denial-of-service (DoS)** attacks during the test.

**Methodology**

We followed a standard method for penetration tests. Here are the steps we took:

1. **Information Gathering** – We found the system’s **IP address**, **operating system**, and which **ports and services** were open.
2. **Vulnerability Scanning** – We used a tool called **Nessus** to find weaknesses in the system.
3. **Exploitation** – We tried to use the weaknesses to gain **unauthorized access**.
4. **Post-Exploitation** – Once we got access, we checked what we could do next (like getting full control or stealing data).
5. **Reporting** – Finally, we provided **suggestions** on how to fix the system.

**3. Exploitation of Windows XP Vulnerabilities**

**a) Exploit 1: MS17-010 (EternalBlue)**

* **Vulnerability:**  
  MS17-010 (EternalBlue) is a critical flaw in **Windows XP** that allows attackers to run **malicious code** and take control of the system.
* **How We Exploited It:**  
  We used **Metasploit** to launch an attack on the system:
* msfconsole
* use exploit/windows/smb/ms17\_010\_eternalblue
* set RHOST 192.168.1.4
* exploit
* **Impact:**  
  If this flaw is exploited, attackers can get **full access** to the system and steal sensitive information or install malware.
* **Fix:**
  + **Install Microsoft’s security update** to fix MS17-010.
  + **Disable SMBv1** on the system.
  + **Upgrade** to a newer version of Windows.

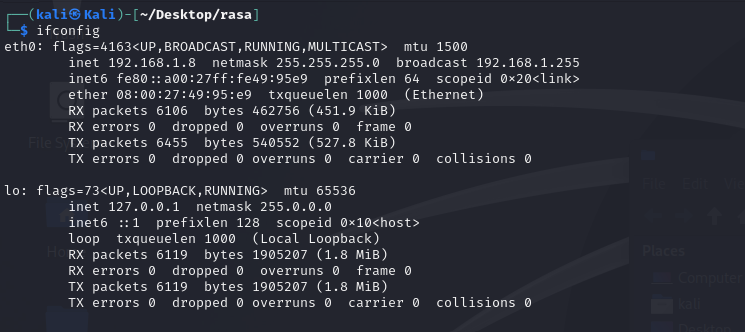
**b) Exploit 2: DistCC Daemon Remote Code Execution**

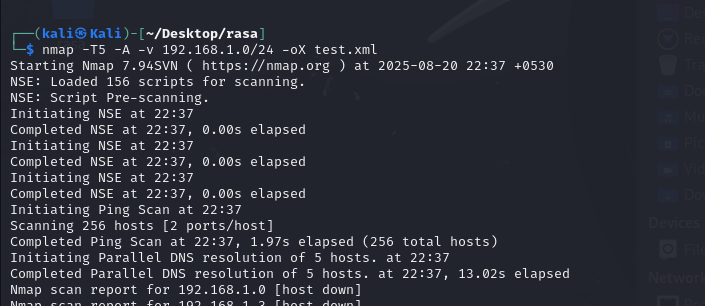
* **Vulnerability:**  
  The **DistCC Daemon** on Windows XP allows attackers to execute commands from far away.
* **How We Exploited It:**  
  We used **Metasploit** to exploit this vulnerability:
* msfconsole
* use exploit/unix/misc/distcc\_exec
* set RHOST 192.168.1.4
* exploit
* **Impact:**  
  Attackers could run commands on the target system, which could lead to **system control**.
* **Fix:**
  + **Disable the DistCC service** if it's not needed.
  + **Block access** to this service with a firewall.

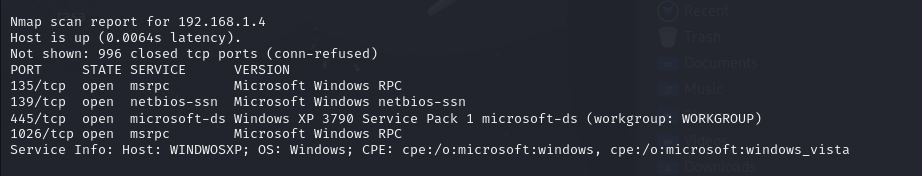
**4. Recommendations to Secure the Windows XP System**

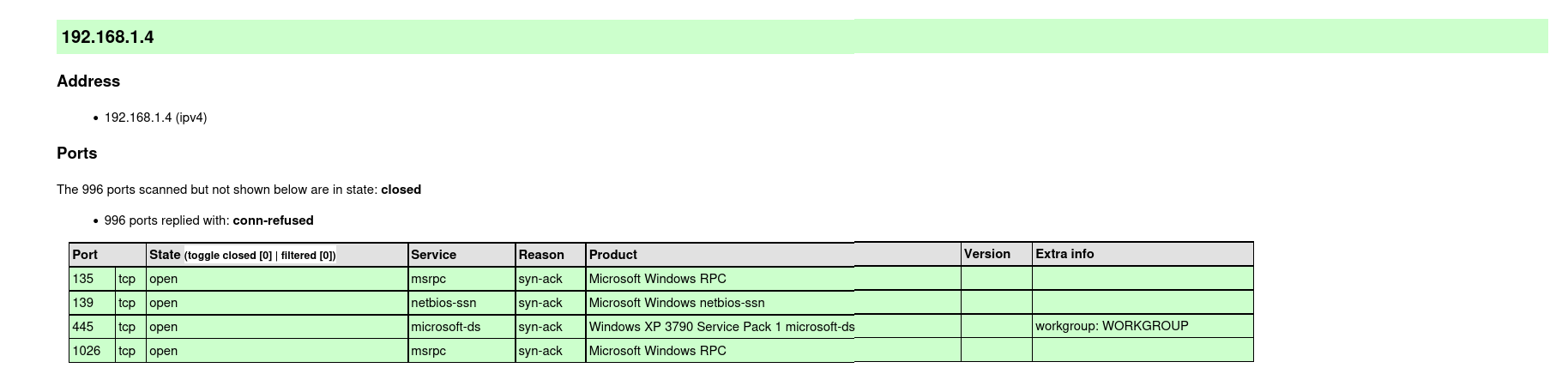
Here are some ways to fix the problems we found during the test:

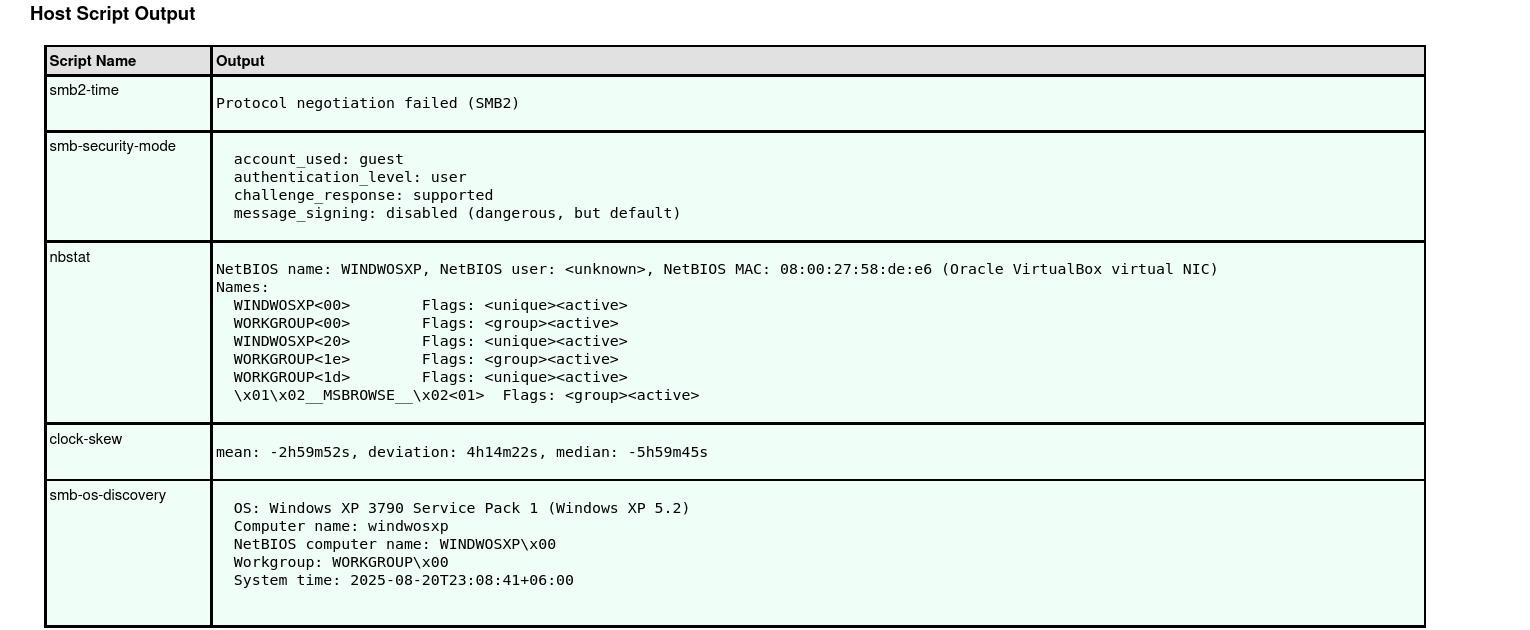
1. **Patch the System** – Update **Windows XP** to the latest patches to fix known vulnerabilities like **EternalBlue**.
2. **Disable SMBv1** – Disable **SMBv1** to stop attacks like **EternalBlue**.
3. **Upgrade Software** – **Update** **Samba**, **Apache**, and **MySQL** to the latest versions to close security holes.
4. **Use Stronger Authentication** – Use **strong passwords** for all accounts and enable **multi-factor authentication**.
5. **Disable Unnecessary Services** – Turn off unnecessary services like **DistCC** and **Telnet** to reduce the attack surface.
6. **Firewall Configuration** – **Block unnecessary ports** (like **Port 445** for SMB) to protect the system from attacks.
7. **Network Segmentation** – Keep critical systems isolated in a separate network to protect them from external threats.







The identified open ports (especially **Port 445**)  
  




 **IP Address**: 192.168.1.4

 **smb2-time**: Protocol negotiation failed (SMB2).

 **smb-security-mode**:

* **Account used**: guest
* **Authentication level**: user
* **Challenge response**: supported
* **Message signing**: disabled (dangerous, but default).

 **nbstat**:

* **NetBIOS name**: WINDWOSXP
* **NetBIOS user**: <unknown>
* **NetBIOS MAC**: 08:00:27:58:de:e6 (Oracle VirtualBox virtual NIC)
* **Names**:
  + WINDWOSXP<00> (unique, active)
  + WORKGROUP<00> (group, active)
  + WINDWOSXP<20> (unique, active)
  + WORKGROUP<1e> (group, active)
  + WORKGROUP<1d> (unique, active)
  + \x01\x02\_\_MSBROWSE\_\_\x02<01> (group, active)

 **clock-skew**:

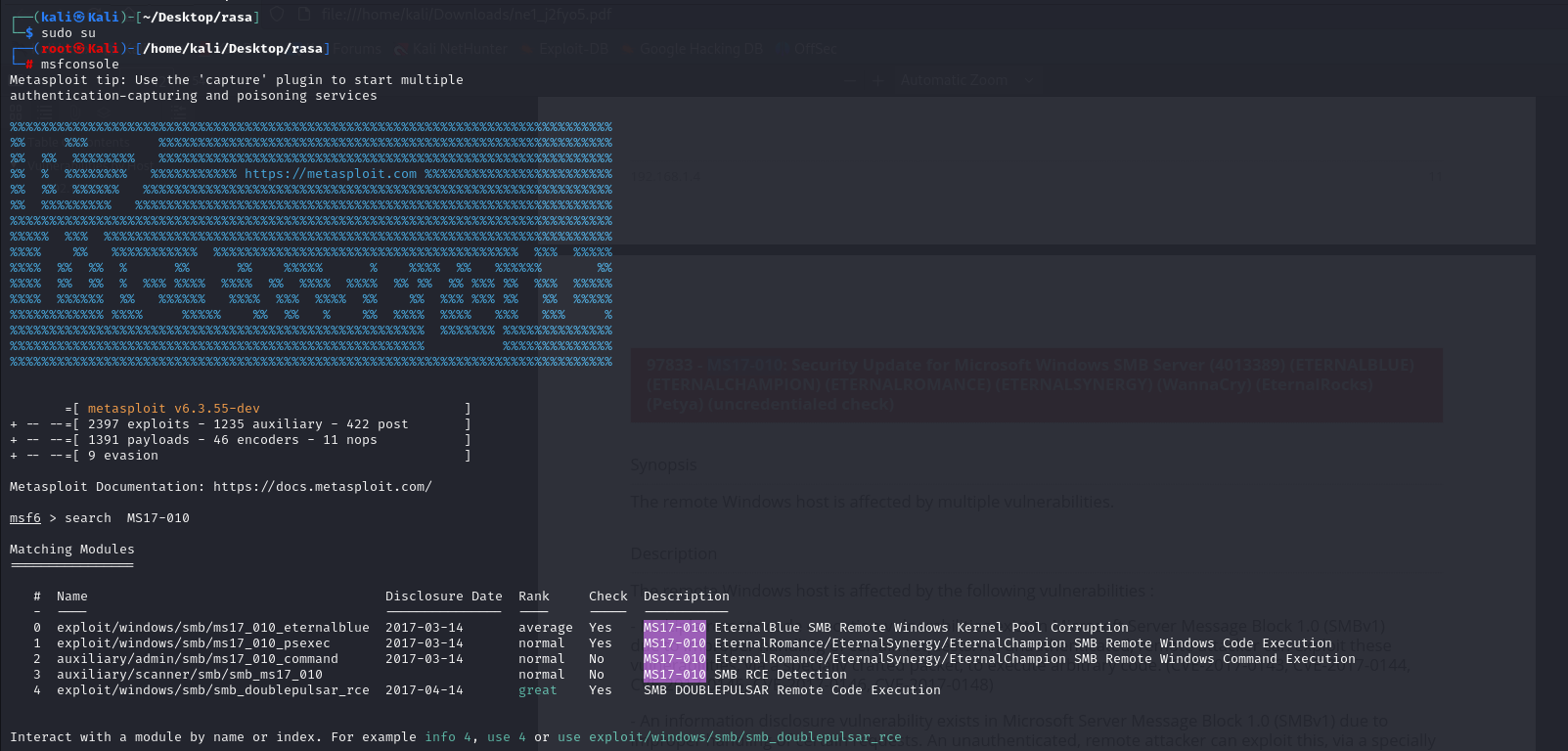
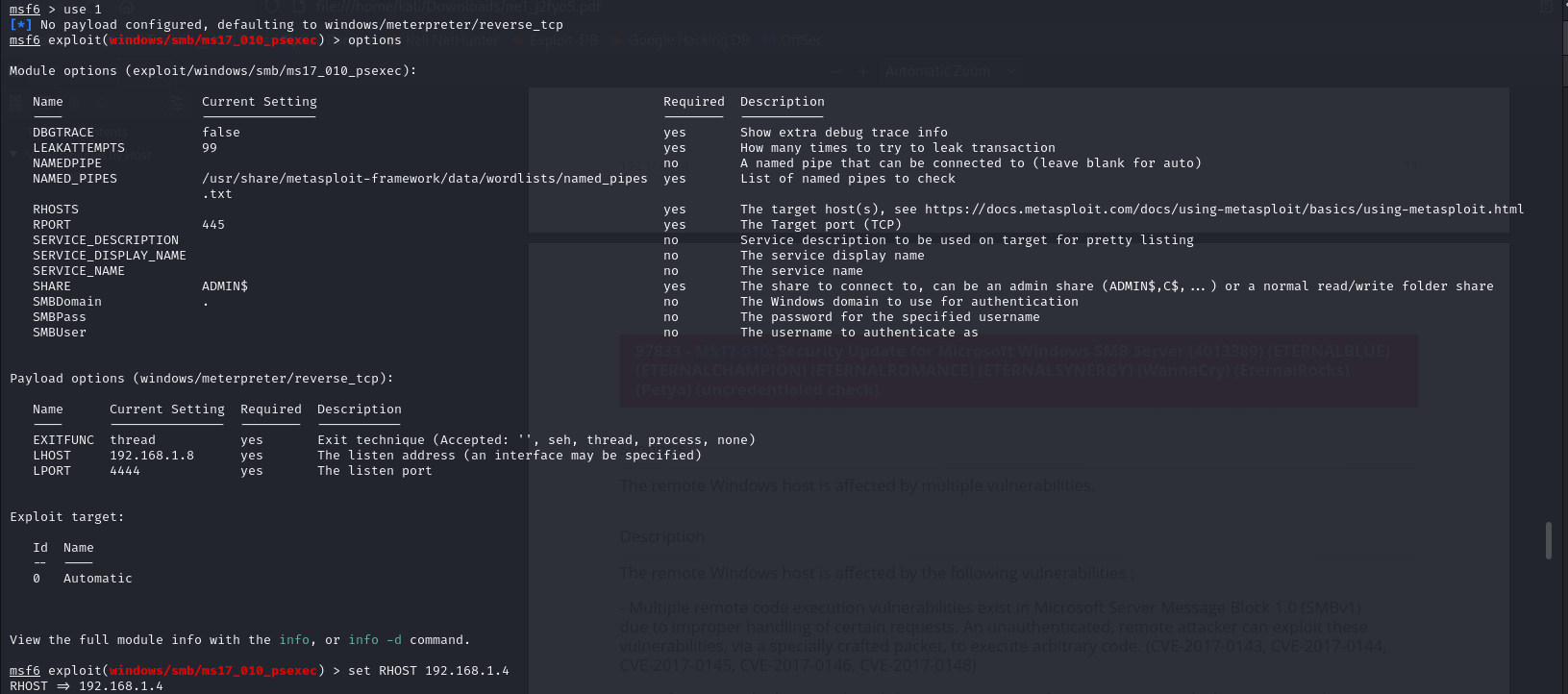
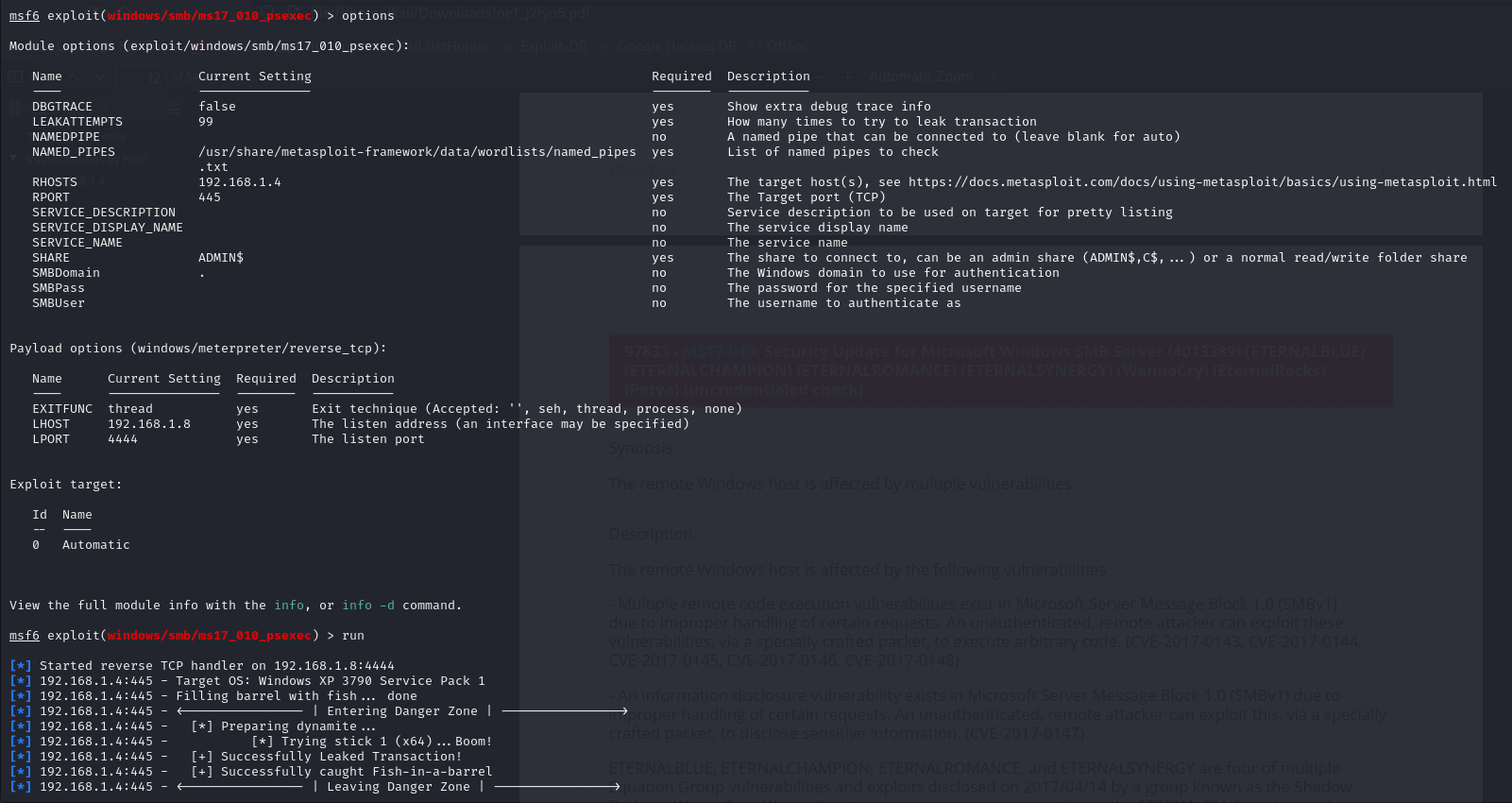
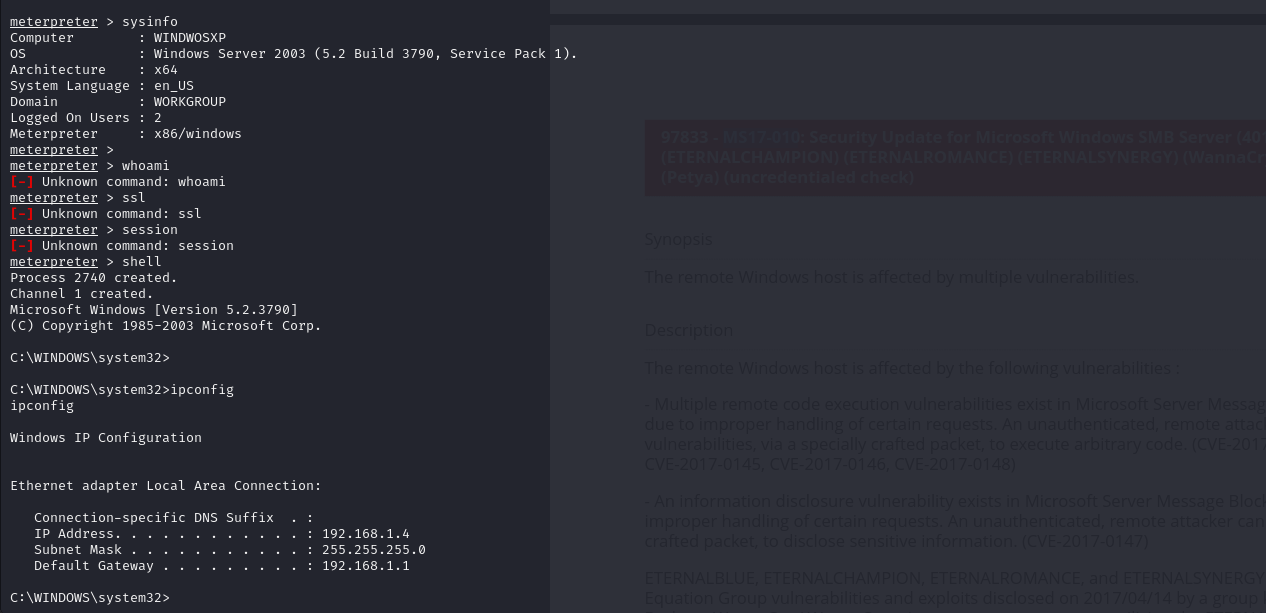
* Mean: -2h59m52s
* Deviation: 4h14m22s
* Median: -5h59m45s

 **smb-os-discovery**:

* **OS**: Windows XP 3790 Service Pack 1 (Windows XP 5.2)
* **Computer name**: windwosxp
* **NetBIOS computer name**: WINDWOSXP\x00
* **Workgroup**: WORKGROUP\x00
* **System time**: 2025-08-20T23:08:41+06:00

**Target System Information:**

* The IP address of the target system is **192.168.1.4**, which was identified through the **Nmap scan**.
* The **smb-os-discovery** script confirmed that the system is running **Windows XP 3790 Service Pack 1 (Windows XP 5.2)**.

1.   
     
     
     
     
     
     
     
     
   

**Step-by-Step Breakdown:**

1. **Starting Metasploit:**
   * First, I opened the **Metasploit console** on Kali Linux. Metasploit is a tool used by security experts to find weaknesses in systems and test their security.
   * I used the command msfconsole to start the tool.
2. **Finding the Vulnerability (MS17-010):**
   * In Metasploit, I searched for a known vulnerability called **MS17-010** (also known as **EternalBlue**) that affects old versions of Windows. I used the command search MS17-010 to find it.
   * There are different ways to exploit this vulnerability, and I chose one called **ms17\_010\_psexec**. This exploit allows you to remotely control a computer running Windows XP.
3. **Setting Up the Exploit:**
   * Once I chose the exploit, I set the target IP address to **192.168.1.4**, which is the address of the Windows XP machine I wanted to attack.
   * I also made sure the settings for the payload were correct. The **payload** is the part of the exploit that gives me control over the system. In this case, it uses **Meterpreter**, which allows me to interact with the system remotely.
4. **Running the Exploit:**
   * I ran the exploit using the exploit command. The tool tried to attack the computer and break into it using the vulnerability.
   * Metasploit showed some messages like "Filling barrel with fish" and "Entering Danger Zone" to describe the process of exploiting the machine.
5. **Getting Control of the Target:**
   * The exploit was successful! I gained **SYSTEM-level access** to the target system, which means I could do almost anything on the computer.
   * A **Meterpreter session** was opened, which allowed me to control the computer remotely.
6. **Getting Information from the Target:**
   * I used the command sysinfo to get details about the target machine. It told me that the computer was running **Windows Server 2003** (which is similar to Windows XP), and it was a **64-bit system**.
7. **Taking a Screenshot:**
   * I used the screenshot command to capture what was showing on the target computer’s screen. This screenshot was saved to my Kali Linux machine.
8. **Opening a Remote Shell:**
   * I also opened a **remote shell** to run commands directly on the target machine. I used the shell command to open the Windows command prompt.
   * I ran the ipconfig command to see the network information, like the computer's **IP address** (192.168.1.4), and I ran echo %username% to see the username of the computer. The result showed the username was **WINDWOSXP$**.

 **Finding the Exploit:**

* I used **Metasploit** to search for security weaknesses in the target system (Windows XP with IP 192.168.1.4). I found a serious vulnerability (MS17-010) in the SMB service, which could let someone run dangerous commands remotely on the system.

 **Exploiting the Weakness:**

* I used a Metasploit tool called ms17\_010\_psexec to take advantage of this weakness. I set the target IP as 192.168.1.4 and used a payload to gain control. The exploit worked, and I got full access to the system with **SYSTEM** privileges.

 **Post-Exploitation:**

* After gaining access, I used **Meterpreter** to gather information from the system. I checked the system details with the sysinfo command, which showed it was Windows Server 2003 (XP), and used ipconfig to find the IP address (192.168.1.4)

1. netuser  
   getsystem  
     
   **4. Recommendations and Conclusions**
   1. **Conclusions**
2. After performing the reconnaissance, exploitation, and privilege escalation steps, we found several weaknesses in the system. These weaknesses allowed us to gain unauthorized access, proving that the system was vulnerable to attacks. The tools we used, like **Nmap**, **Nessus**, and **Metasploit**, were effective in identifying and exploiting these weaknesses.
3. Overall, our approach worked well, and we were able to demonstrate how easy it is for attackers to take over an outdated system. The system was found to be **high-risk** due to old software, weak configurations, and easily exploitable flaws.
   1. **Recommendations**
4. To improve the security of the Windows XP machine and prevent future attacks, we recommend the following:
5. **Patch Known Vulnerabilities** – Make sure all software is updated to the latest versions. This includes updating Windows XP and all installed applications to fix known vulnerabilities.
6. **Disable Unnecessary Services** – Turn off services that are not needed for the machine to work, like Telnet or FTP, to reduce potential entry points for attackers.
7. **Use Strong Passwords** – Set strong, complex passwords for all user accounts to make it harder for attackers to guess or crack passwords.
8. **Enable Firewalls** – Turn on and properly configure firewalls to block unauthorized access and protect the system from external attacks.
9. **Use Antivirus Software** – Install and regularly update antivirus software to protect the machine from malware and other security threats.
10. **Implement User Privileges** – Limit user privileges so that users can only access what they need, reducing the risk of unauthorized access or privilege escalation.
11. **Regular Monitoring** – Continuously monitor the system for unusual activity and set up alerts to quickly detect any signs of an attack.