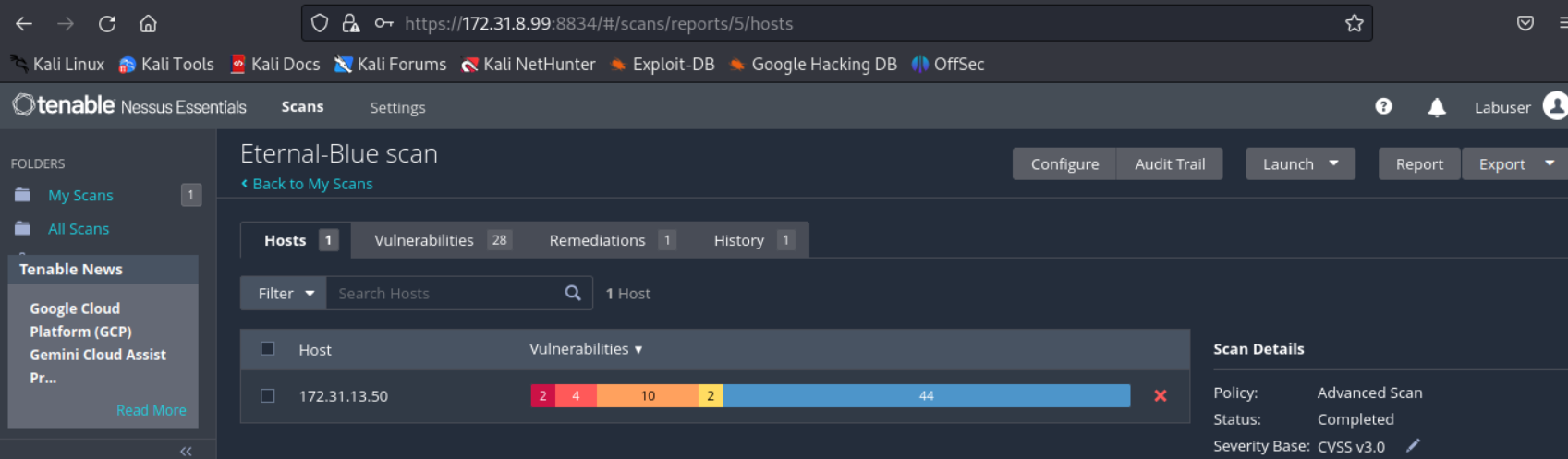
**Vulnerability Assessment**

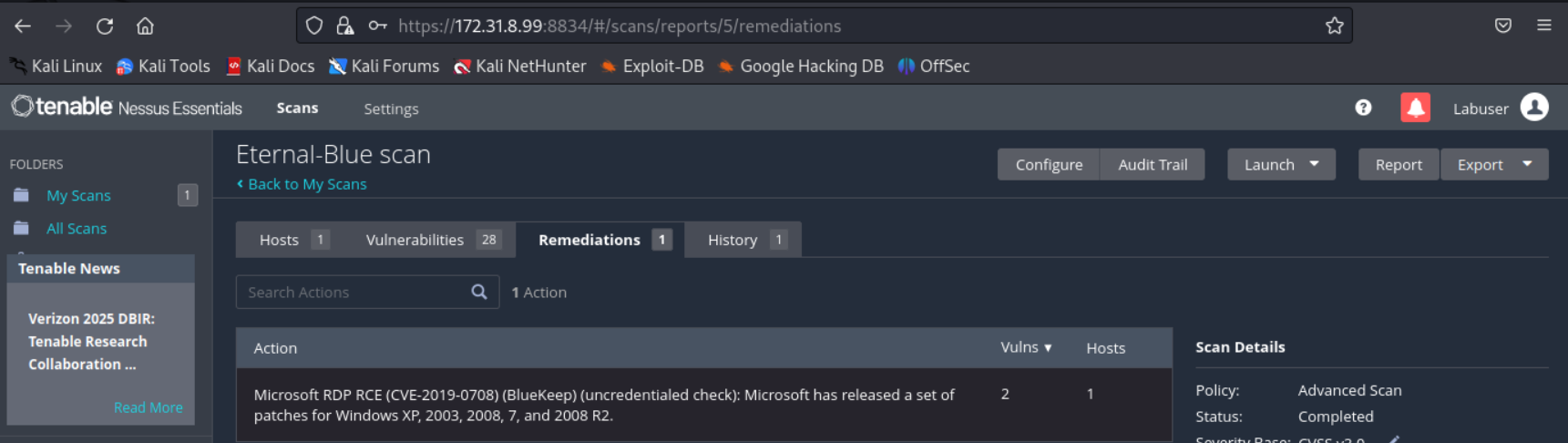
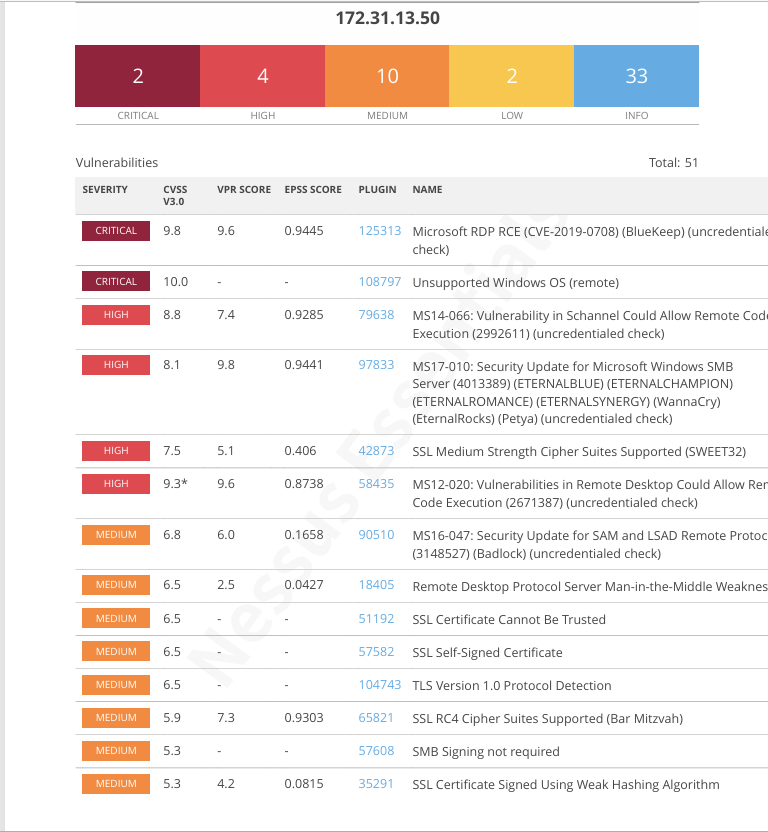
Downloaded the Nessus in Kali Linux.

<https://www.tenable.com/products/nessus/nessus-essentials>

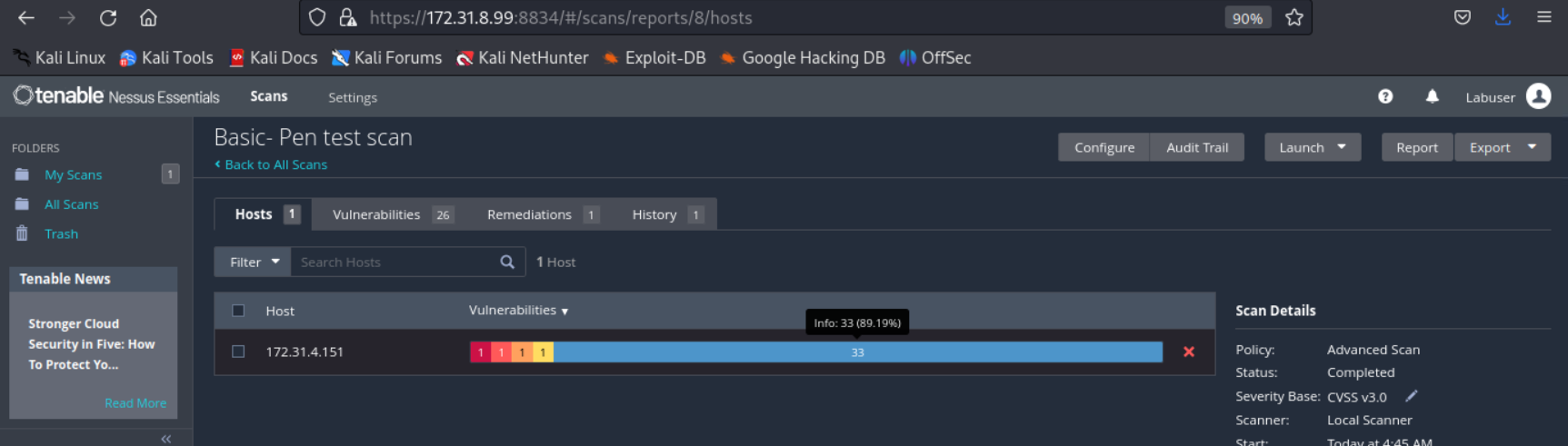
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Hostname** | **IP (public)** | **IP (private)** | **Port** | **Access** |
| kali | 34.221.33.132 | 172.31.8.99 | 8443 | <https://34.221.33.132:8443> |
| ubuntu-desktop | 35.90.121.28 | 172.31.1.92 | 8443 | <https://35.90.121.28:8443> |
| eternal-blue | 35.166.97.160 | 172.31.13.50 | 8443 | <https://35.166.97.160:8443> |
| basic-pen test | 52.26.25.69 | 172.31.4.151 | 8443 | <https://52.26.25.69:8443> |

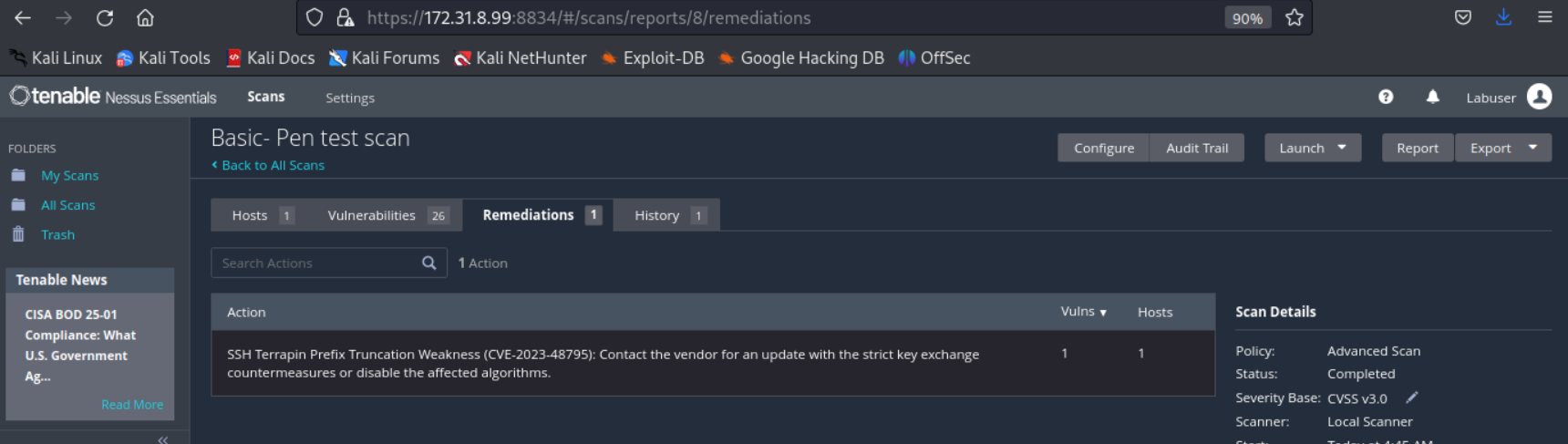
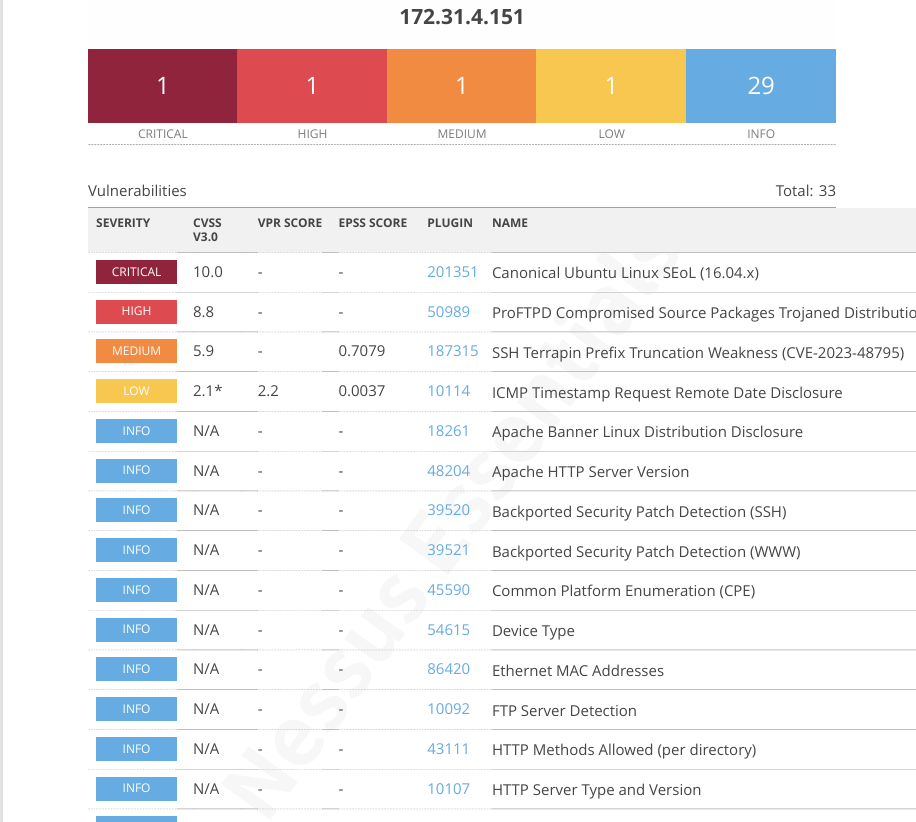
* Performed Nessus scan for Eternal Blue(windows) and below is the scan report for the same.



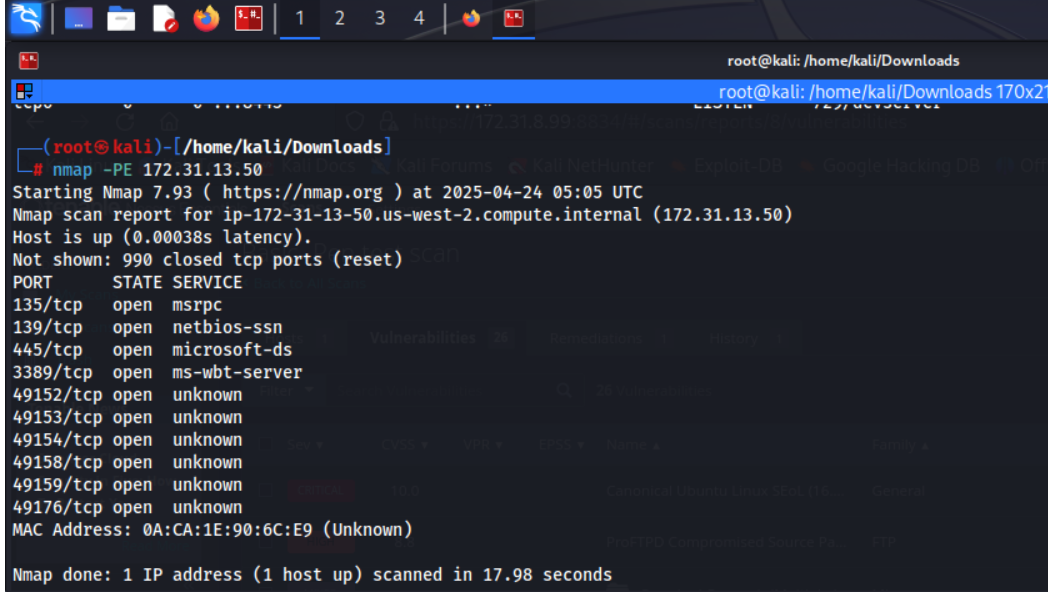
* Performed Nessus scan for Basic Pen Test (Linux) and below is the scan report for the same.

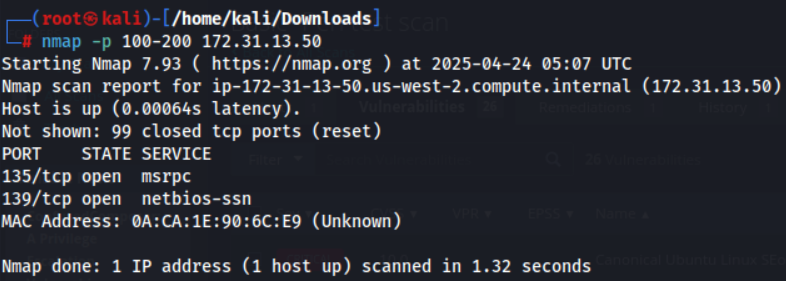


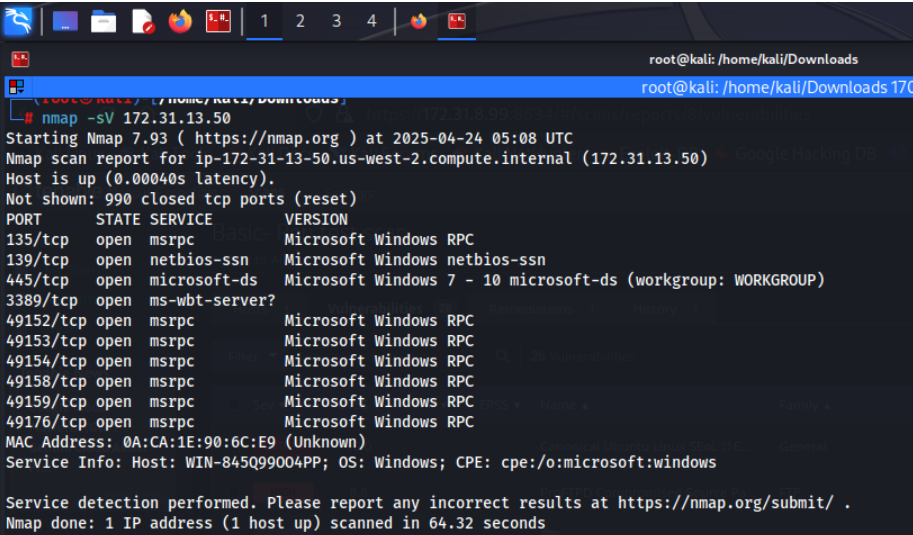
**Information Gathering**

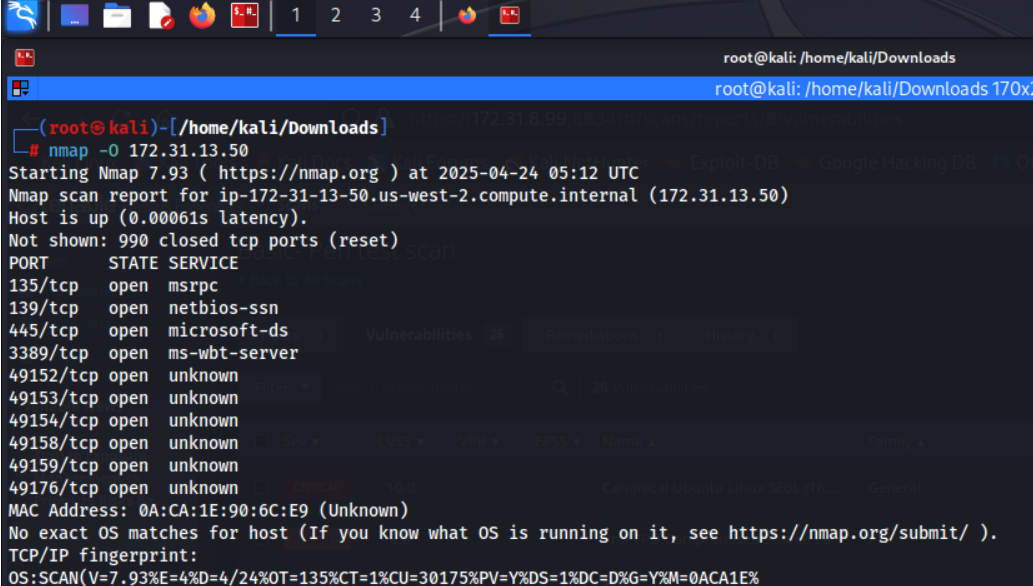
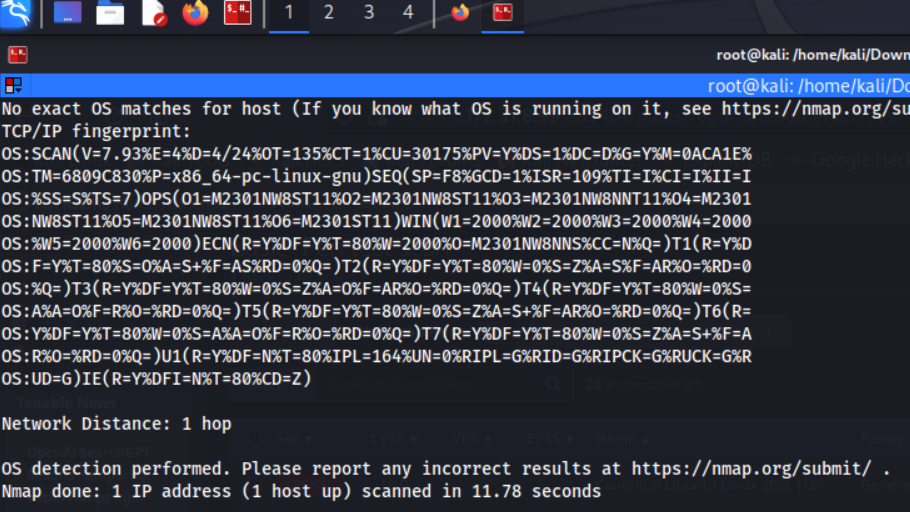
* Nmap Port scan for Eternal Blue (Windows).

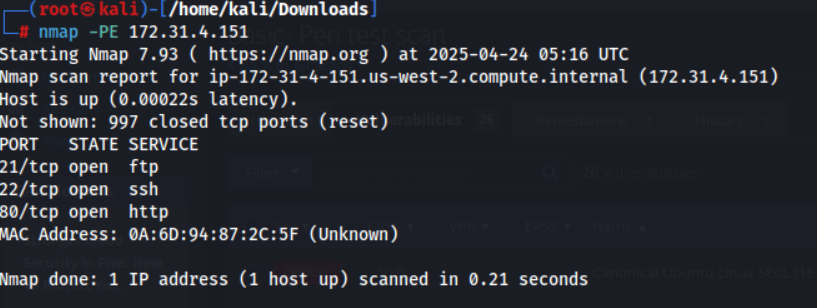




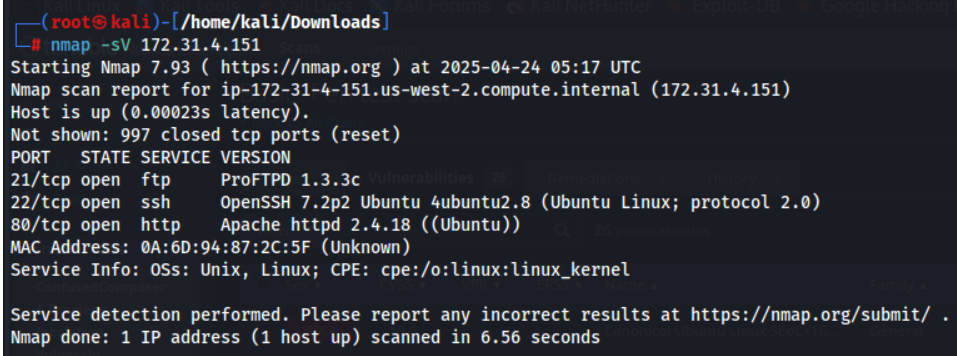
* Nmap Service scan for Eternal Blue (Windows).



* Nmap OS scan for Eternal Blue (Windows). 
* Nmap Port scan for Basic Pen Test (Linux).

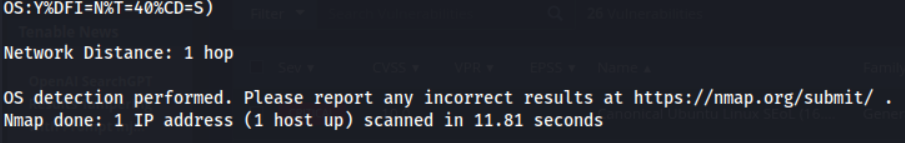


* Nmap Service scan for Basic Pen Test (Linux).



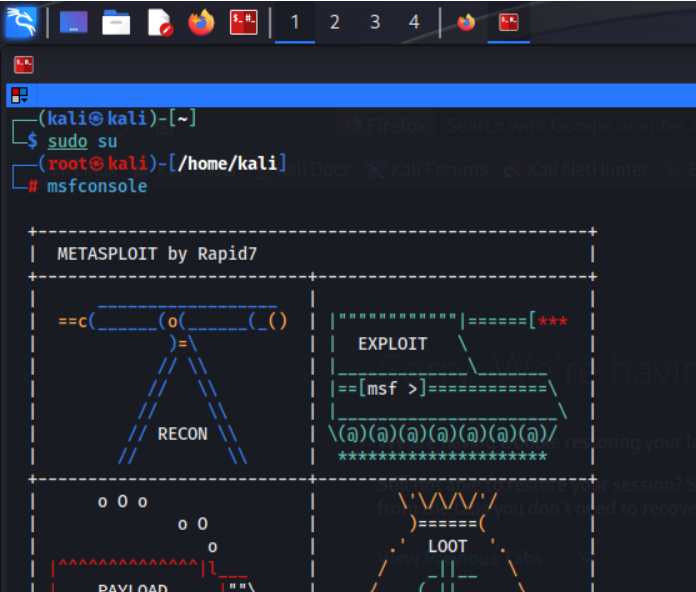
* Nmap OS scan for Basic Pen Test (Linux).

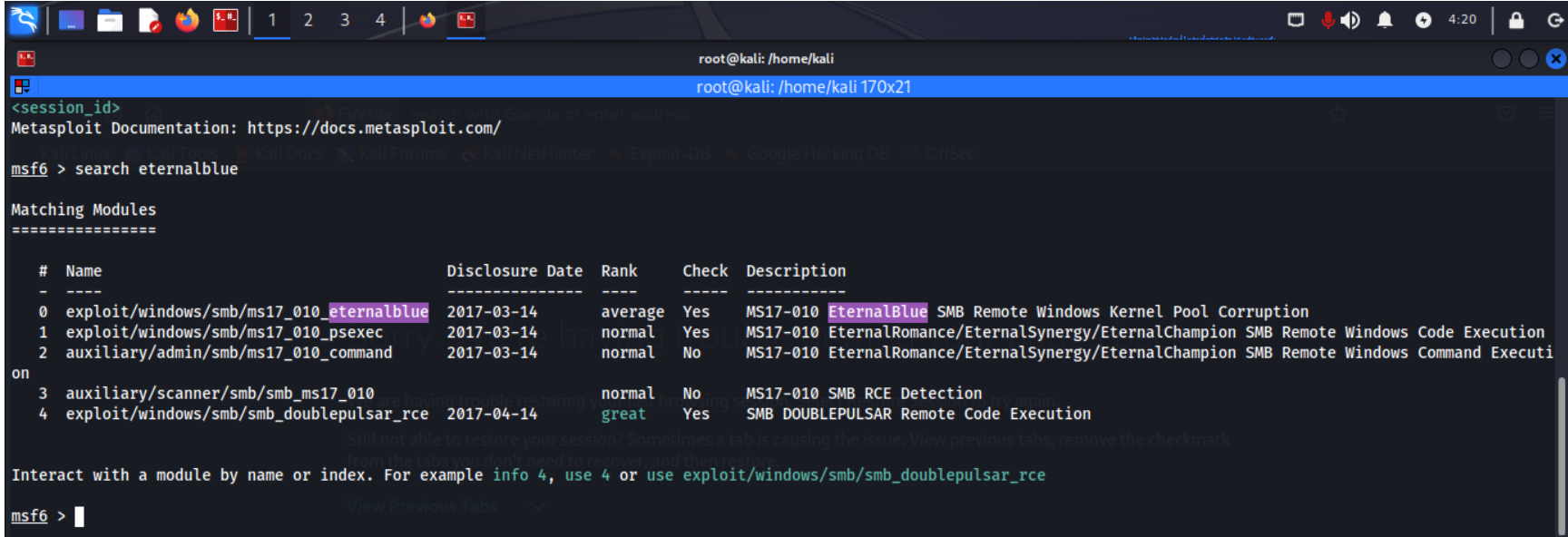


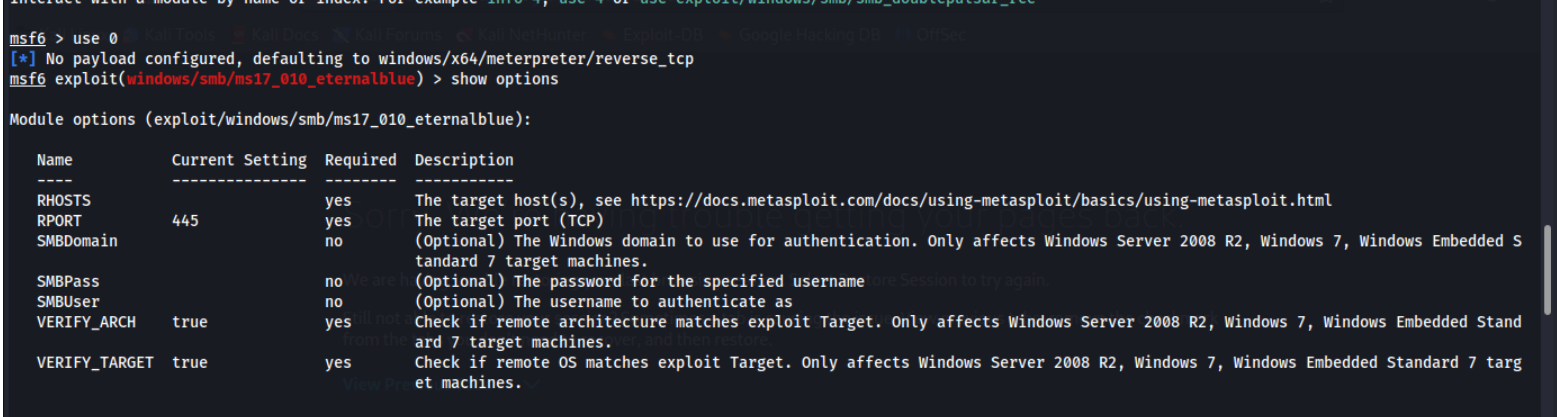


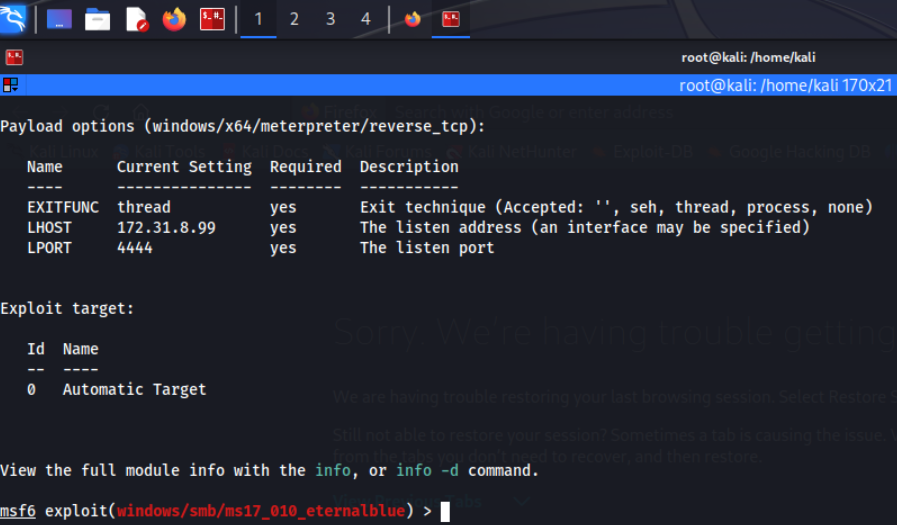
**Exploitation**

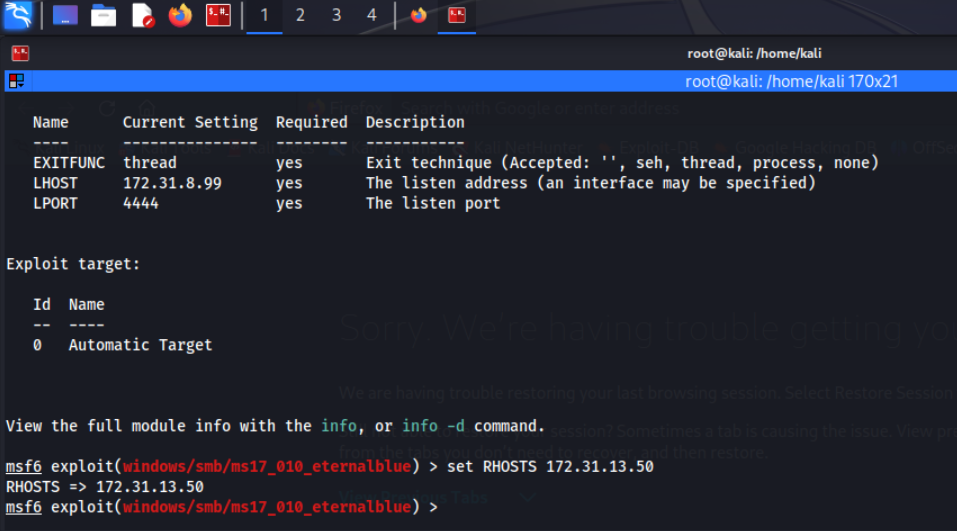
* Exploiting the Eternal Blue (windows).

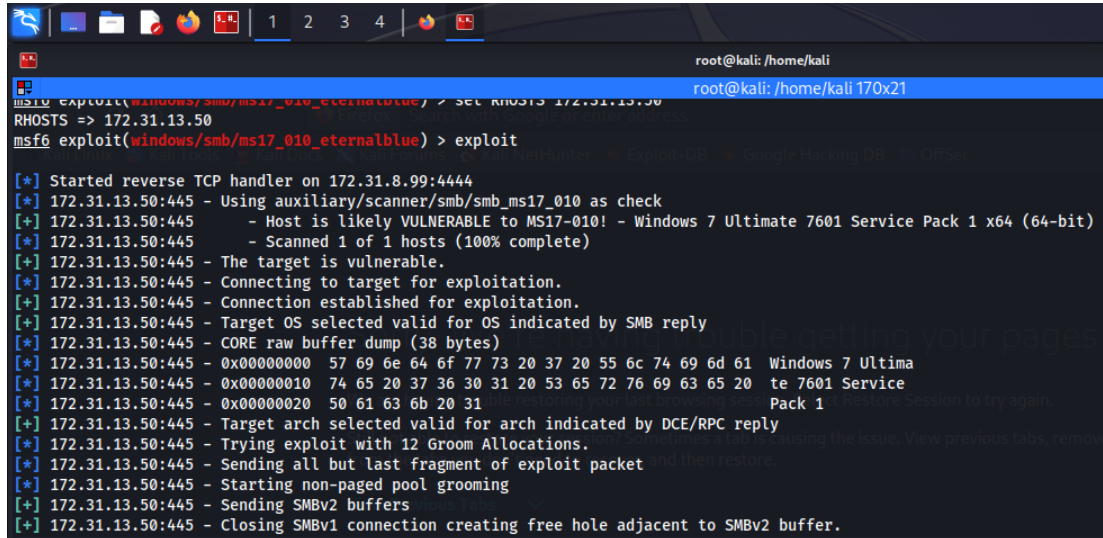


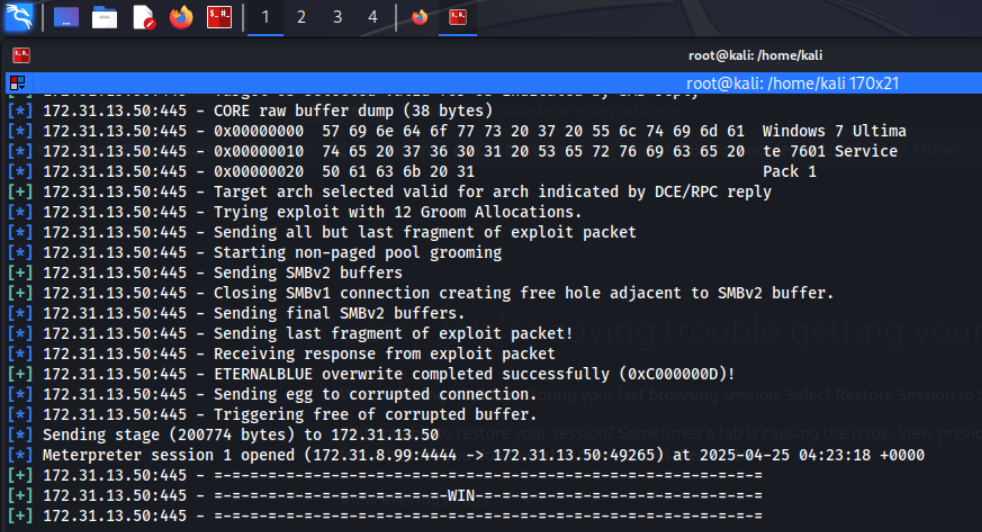








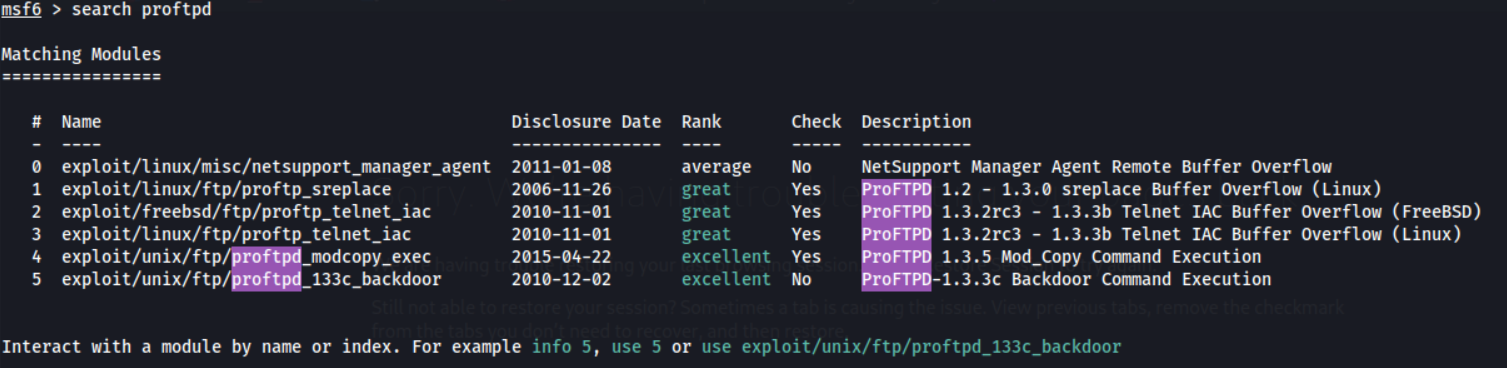


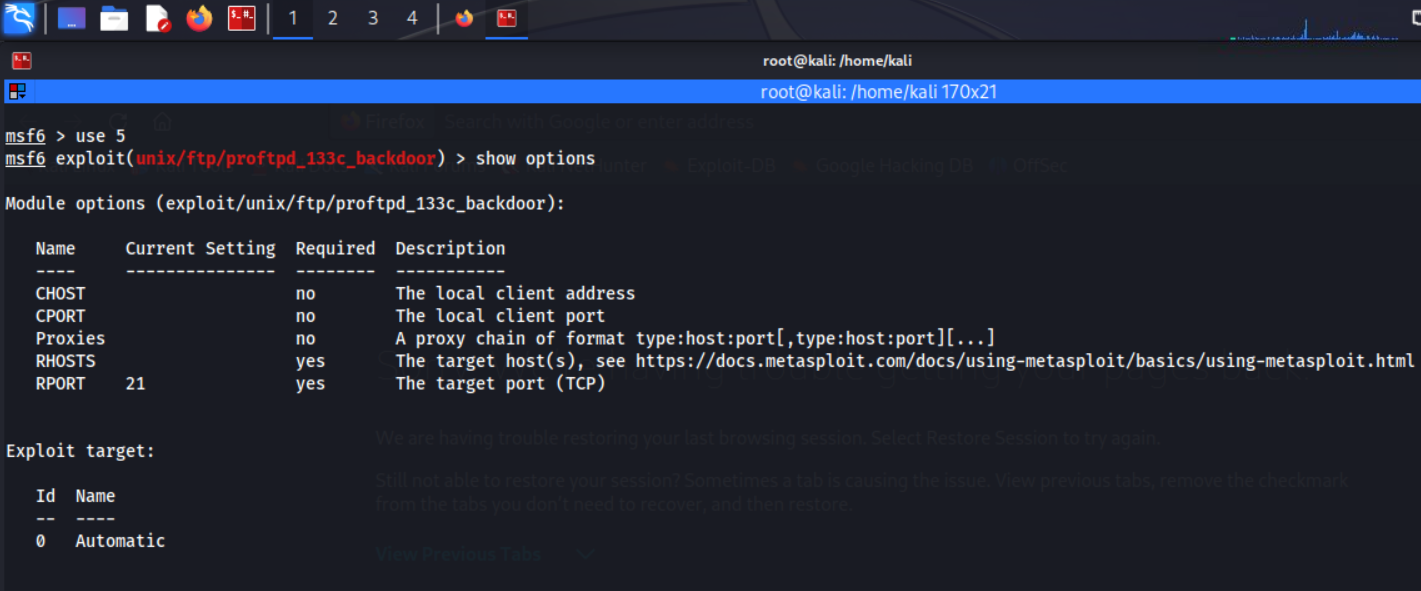


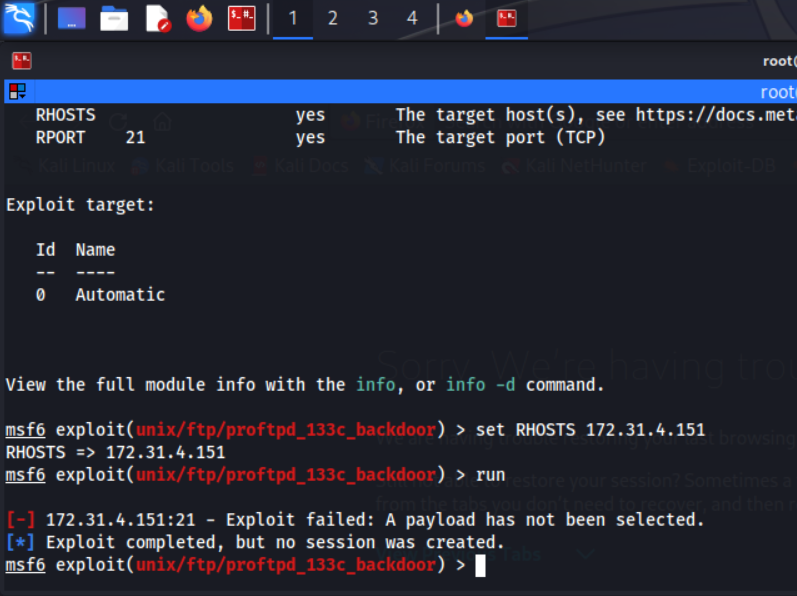
EternalBlue is both the given name to a series of **Microsoft software vulnerabilities and the exploit created by the NSA as a cyberattack tool.** Although the EternalBlue exploit — officially named MS17-010 by Microsoft — affects only Windows operating systems, anything that uses the SMBv1 (Server Message Block version 1) file-sharing protocol is technically at risk of being targeted for ransomware and other cyberattacks.

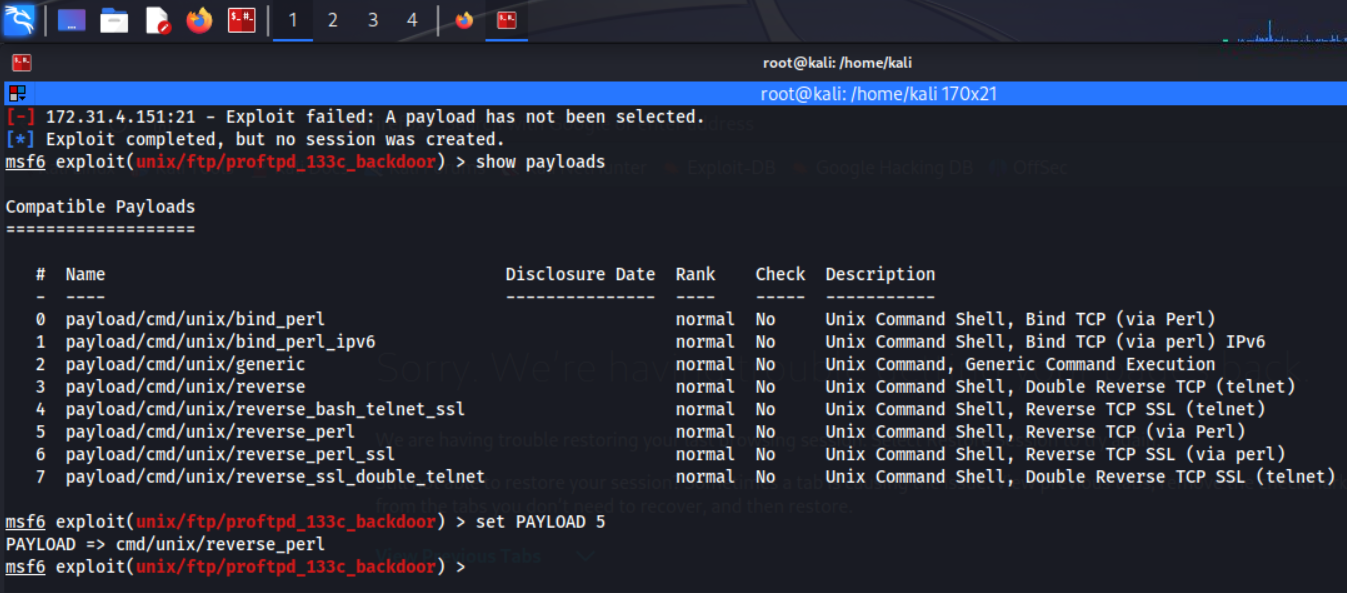
The MS17-010 patch was designed to fix the SMBv1 software flaws for all supported Windows operating systems, including **Windows Vista, Windows 7, Windows 8.1, Windows 10, Windows Server 2008, Windows Server 2012, and Windows Server 2016**. Microsoft also automatically disabled SMBv1 in the latest versions of Windows 10 and Windows Servers 2012 and 2016 by default.

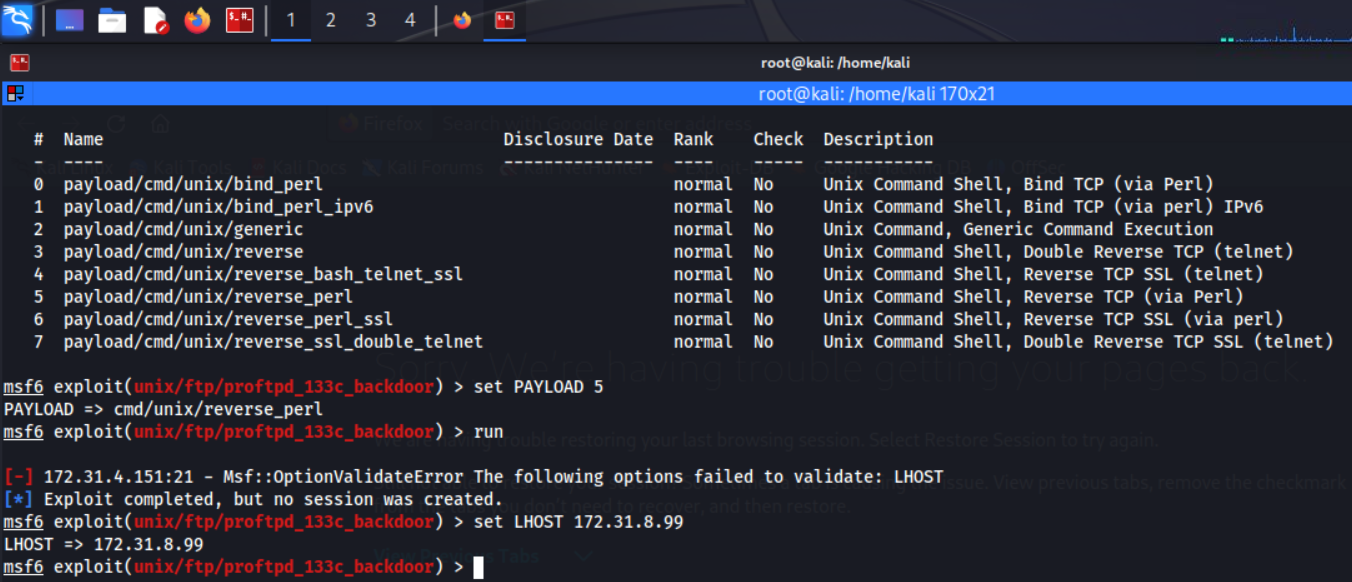
* Exploiting the Basic Pen Test (Linux).

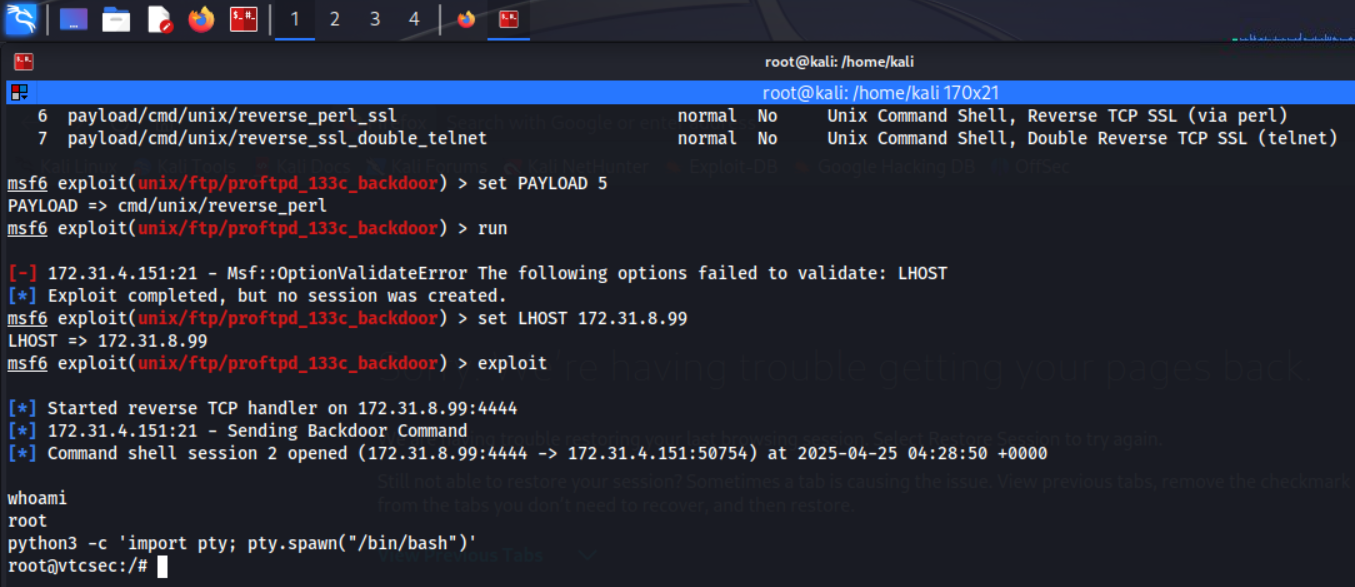












**Executive Report**

**Objective:** To assess the security posture of a Windows 10 and Linux environment by simulating real-world attacks and identifying vulnerabilities that could be exploited by malicious actors.

**Methodology:** Utilizes a combination of automated tools and manual techniques to probe for weaknesses in the operating system, applications, network configurations, and user behavior

**Areas of Focus:** Information gathering , Vulnerability scanning, privilege escalation, password cracking, network exploitation, application security testing, social engineering assessments, and overall system hardening recommendations.

**Deliverables:** Detailed report outlining discovered vulnerabilities, their severity levels, exploitation scenarios, recommendations for remediation, and best practices for improving the security posture of Windows 10 and Linux OS.

**Overall Findings :**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Asset Details** | **Critical** | **High** | **Medium** | **Low** | **Nessus Scan Report** |
| 172.31.13.50 | 2 | 4 | 10 | 2 |  |
| 172.31.4.151 | 1 | 1 | 1 | 1 |  |

**Summary of Findings :**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sno** | **Asset Details** | **Vulnerability Title** | **Description** | **Severity** | **Exploitable** |
| 1 | 172.31.13.50 | Eternal Blue | SMB-MS17-010-Eternal blue | Critical | Yes |
| 2 | 172.31.4.151 | Basic Pen Test | PROFPTD 1.3.3c backdoor execution | Critical | Yes |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sno** | **Asset Details** | **Severity** | **CVSS V3.0** | **Description** |
| 1 | 172.31.13.50 | Critical | 10 | Unsupported Windows OS (remote) |
| 2 | 172.31.13.50 | Critical | 9.8 | Microsoft RDP RCE (CVE-2019-0708)  (BlueKeep) (uncredentialed check) |
| 3 | 172.31.13.50 | High | 8.8 | MS14-066: Vulnerability in Schannel Could  Allow Remote Code Execution (2992611) (uncredentialed check) |
| 4 | 172.31.13.50 | High | 8.1 | MS17-010: Security Update for Microsoft Windows SMB Server  (4013389) (ETERNALBLUE) (ETERNALCHAMPION)  (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry)  (EternalRocks) (Petya) (uncredentialed check) |
| 5 | 172.31.13.50 | High | 9.3 | MS12-020: Vulnerabilities in Remote Desktop Could Allow Rem  Code Execution (2671387) (uncredentialed check) |
| 6 | 172.31.4.151 | Critical | 10 | Canonical Ubuntu Linux SEoL (16.04.x) |
| 7 | 172.31.4.151 | High | 8.8 | ProFTPD Compromised Source Packages Trojaned Distribution |
| 8 | 172.31.4.151 | Medium | 59 | SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795) |

**Technical Report**

|  |  |
| --- | --- |
| **Vulnerability** | Remote Desktop Services Remote Code Execution Vulnerability |
| **Reference** | CVE 2019-0708 |
| **Vulnerability Description** | A remote code execution vulnerability exists in Remote Desktop Services formerly known as Terminal Services when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Remote Desktop Services Remote Code Execution Vulnerability'. |
| **CVSS 3.x Severity and Metrics:** | **9.8 (Critical)** |
| **NVD Reference** | [NVD - CVE-2019-0708](https://nvd.nist.gov/vuln/detail/CVE-2019-0708) |
| **Known Exploits** | exploit/windows/rdp/cve\_2019\_0708\_bluekeep\_rce, Kaspersky Lab’s Custom BlueKeep Exploit |
| **Impact** | An attacker can execute arbitrary code on the target system **without authentication** and **without user interaction**. |
| **Remediation** | * Apply Official Patches. * Enable Network Level Authentication (NLA). * Disable Remote Desktop Services (if not needed). * Block Port 3389 (RDP) at Perimeter. |

|  |  |
| --- | --- |
| **Vulnerability** | ProFTPD Source Code Backdoor (Trojaned Distribution) |
| **Reference** | CVE-2010-4221 |
| **Vulnerability Description** | A **backdoor was intentionally inserted** into the source code of **ProFTPD version 1.3.3c** after the project's main distribution server (ftp.proftpd.org) was **compromised by attackers**. This malicious version was **distributed via official download channels** from **November 28 to December 2, 2010**.  The trojaned code introduced a backdoor that allowed a remote attacker to **execute arbitrary commands with root privileges** by sending specially crafted input to the FTP server on **TCP port 21**. |
| **CVSS 3.x Severity and Metrics:** | **8.8 (High)** |
| **NVD Reference** | [NVD - CVE-2010-4221](https://nvd.nist.gov/vuln/detail/CVE-2010-4221) |
| **Known Exploits** | Backdoor Command Injection (Built-In Exploit) |
| **Impact** | * Unauthenticated Remote Root Access. * Full System Compromise. |
| **Remediation** | * Identify Affected Systems. * Verify Source Code Integrity. * Immediately Remove Compromised Installations. * Reinstall a Clean Version. * Harden FTP Security. |