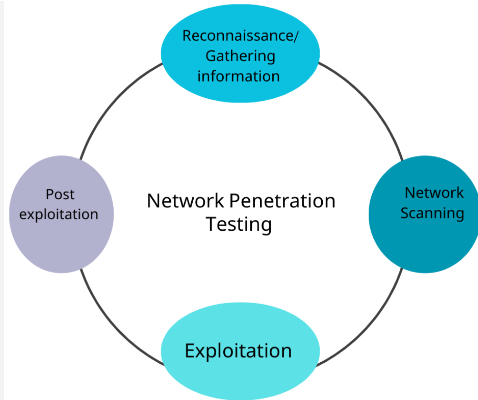


**NAME : GUJJULA SAILAJA**

**REG.NO. : 21B91A5459**

**4/4 AIDS – A**

**The steps involved in a network penetration test on Kali Linux:**

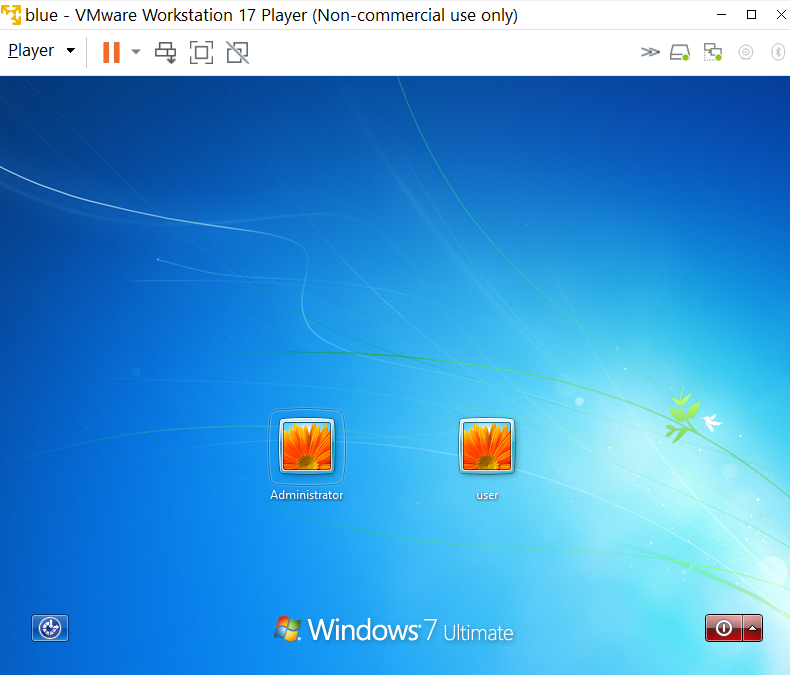


Step 1: planning and preparation.

* Define the scope of the test, including the networks, systems, and data to be tested.
* Identify the goals and objectives of the test.
* Gather necessary information about the target network, such as IP addresses, network ranges, and system details.
* Choose  the tools and techniques to be used during the test.
* Obtain necessary permissions and legal agreements before conducting the test.

VICTIM MACHINE :

 A Target Machine refers to a computer system or device that is being tested or attacked to identify vulnerabilities, weaknesses, or security flaws. The target machine is the system that the penetration tester or hacker is trying to compromise, gain unauthorized access to, or exploit.



**REASONS BEHIND TO DO PENTESTING ON WINDOWS 7 :**

Windows 7  is still widely used in many organizations, making it a target for attackers. Penetration testing helps identify vulnerabilities and weaknesses in Windows 7 systems. Testing on Windows 7 simulates real-world scenarios, allowing testers to identify potential entry points for attackers. It helps organizations comply with regulatory requirements and industry standards. Penetration testing on Windows 7 improves overall security posture and reduces the risk of a successful attack.

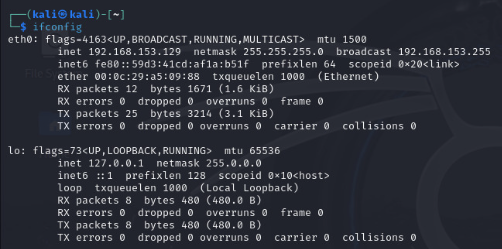
Step 2 : information gathering.

ABOUT KALI LINUX :

Kali Linux is a popular open-source OS for digital forensics, penetration testing, and ethical hacking. It comes with over 600 pre-installed tools for security testing and analysis. Kali Linux is customizable, lightweight, and free, making it accessible to anyone. It's ideal for penetration testing, digital forensics, and ethical hacking. Kali Linux is used in training and educational programs for security professionals. Regular updates ensure users have access to the latest tools and features. Kali Linux is a must-have for security professionals, providing a comprehensive platform for security testing and analysis.

ifconfig :

The *ifconfig* command is a powerful tool in Kali Linux (and other Linux distributions) that allows you to configure and manage network interfaces. This will display information about all network interfaces, including their IP addresses, subnet masks, and MTU.



Kali linux ip address : 192.168.153.129

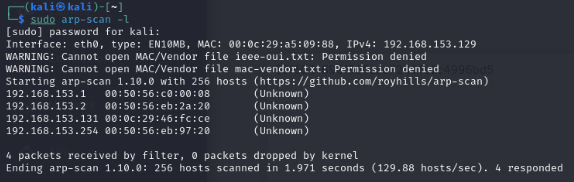
MAC address : 00:0c:29:46:FC:CE (VMware)

arp-scan :

The *arp-scan* command is a powerful tool in Kali Linux (and other Linux distributions) that allows you to scan for devices on a local network using the Address Resolution Protocol (ARP).

arp-scan -l :

The *-l*option tells *arp-scan* to display the list of interfaces on the system that can be used for scanning. This option is useful when you want to specify a particular interface to use for scanning.



nmap command :

*nmap* is a powerful network scanning tool used for network exploration, security scanning, and host discovery. It can scan for open ports, operating systems, and versions of services running on a network*. nmap* can also be used to identify vulnerabilities and detect malware on a network. The command offers various scan types, including TCP SYN scan, UDP scan, and OS detection. *nmap* is a popular tool among security professionals and is widely used for penetration testing and network security assessments.

OS Detection :

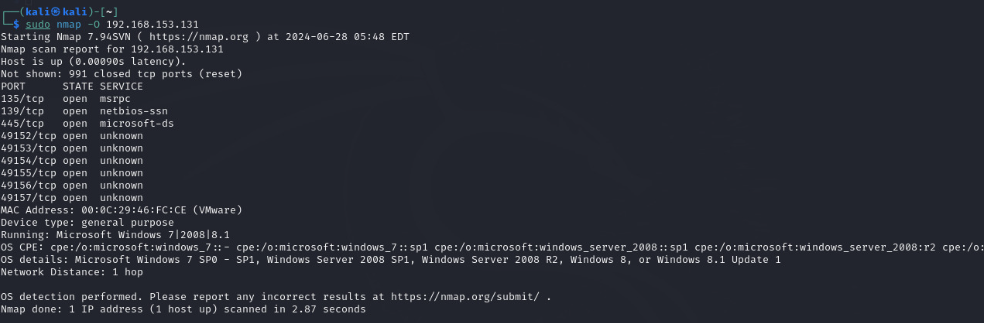
OS detection is crucial for vulnerability assessment and patch management. It helps identify potential security risks and weaknesses. Accurate OS detection enables effective security auditing and compliance. It aids in network inventory and asset management. OS detection helps prioritize security efforts and resource allocation. It facilitates incident response and threat hunting. Ultimately, OS detection is essential for maintaining a secure and resilient network.

nmap -O :

The *-O* option is used to enable OS detection, which allows *nmap* to try to identify the operating system (OS) running on the target machine.

Syntax :

*nmap -O <target***>**



Running : Microsoft Windows 7 |2008|8.1

MAC address : 00:0c:29:46:FC:CE (VMware)

Our Target Machine is Microsoft Windows 7 |2008|8.1.

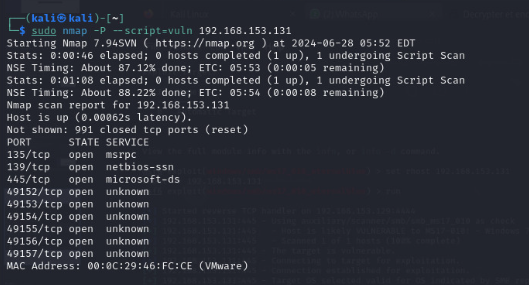
Step 3 : vulnerability identification.

Vulnerability identification is the process of discovering potential vulnerabilities. It's a critical step in the vulnerability management lifecycle. Identifying vulnerabilities helps prevent attacks and reduces risk. It's required for compliance with regulations like PCI-DSS and HIPAA. Vulnerabilities can be found in networks, systems, applications, and human behavior. Techniques for identification include network scanning, vulnerability scanning, and penetration testing. Tools like Nessus, OpenVAS, Nmap, and Burp Suite are used for identification. Vulnerability identification helps improve an organization's security posture. It's an ongoing process, as new vulnerabilities are constantly emerging. By identifying vulnerabilities, organizations can take proactive steps to remediate them.

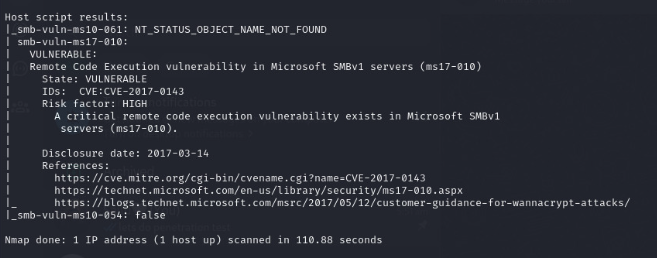
Command : *nmap -P –script=vuln*

The command we provided, *nmap -P –script=vuln <target ip address>*, is using Nmap's scripting engine to scan for vulnerabilities.

* ‘-P’ : This option tells Nmap to only perform a ping scan, which is a quick way to determine if a host is up or down. It doesn't perform a full port scan.
* ‘--script=vuln’ : This option tells Nmap to run the vulnerability detection scripts. The’vuln’ script category includes scripts that check for various vulnerabilities, such as buffer overflows, SQL injection, and cross-site scripting (XSS).



LOOPHOLE : Attackers often exploit various loopholes to gain unauthorized access to systems and data. One common vulnerability is unpatched software or operating systems, which can leave systems open to known exploits. Weak passwords or poor password management can also provide an easy entry point for attackers. Misconfigured networks or unsecured protocols can further compromise security, while unvalidated user input can lead to SQL injection or cross-site scripting (XSS) attacks. Outdated software or plugins, such as Adobe Flash or Java, can also be exploited. Additionally, unsecured services like open SSH or FTP ports, social engineering tactics like phishing or pretexting, and insecure file permissions can all provide opportunities for attackers to gain access. Furthermore, a lack of encryption can expose sensitive data, and unmonitored systems can make it easier for attackers to remain undetected.



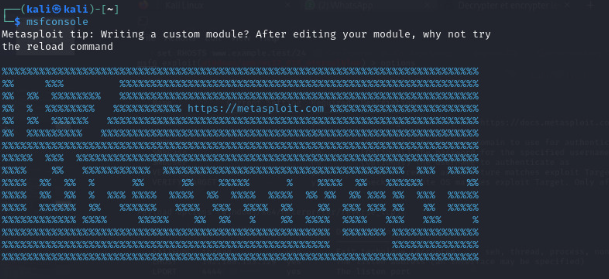
Loophole : ms17-010

Step 4 : exploitation.

Exploitation is the process of taking advantage of a vulnerability to compromise a system, network, or application. It's the next step after vulnerability identification, where an attacker uses the identified vulnerability to gain unauthorized access. There are two types of exploitation: remote and local. Remote exploitation occurs without physical access to the system. Local exploitation requires physical access to the system. Privilege escalation is a type of exploitation where an attacker gains higher privileges. Exploitation techniques include buffer overflow, SQL injection, cross-site scripting (XSS), and social engineering. Exploitation tools include Metasploit, Exploit-DB, and Burp Suite. Defense against exploitation includes patch management and vulnerability scanning. Regularly applying security patches and scanning for vulnerabilities can help prevent exploitation.

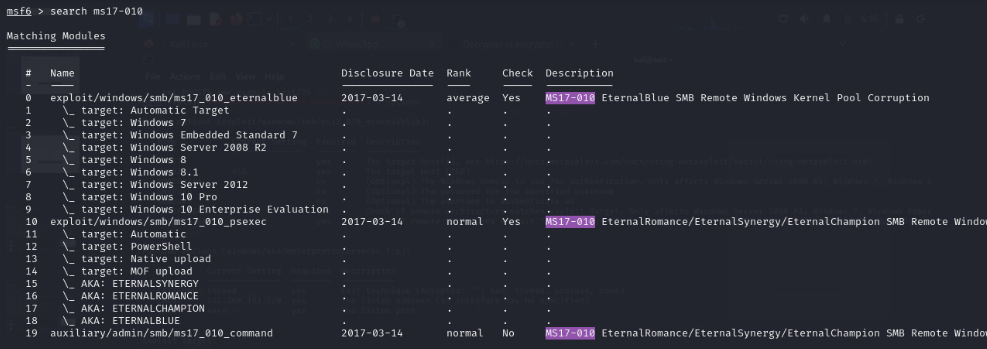
msfconsole :

Use tools like metasploit ( msfconsole ) to exploit identified vulnerabilities. MSFconsole is the command-line interface to the Metasploit Framework, a popular open-source penetration testing and exploitation tool. It provides a powerful and flexible way to interact with the Metasploit Framework, allowing users to launch exploits, scan for vulnerabilities, and interact with compromised systems.



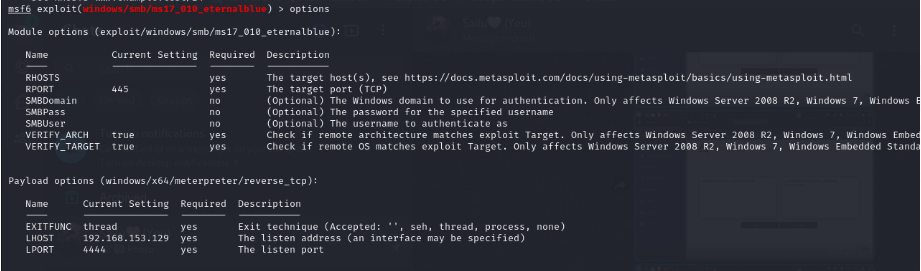
Searchsploit :

Use exploit-db ( serarchsploit) to search for exploits for identified vulnerabilities. Searchsploit is a command-line search tool for the Exploit-DB database, which is a comprehensive collection of exploits, shellcode, and security papers. It allows you to search for exploits, vulnerabilities, and other security-related information using various criteria.



Step 5 : post exploitation.

Check the Rhost :



Rhost :

rhost is a Kali Linux command that manages the .rhosts file which specifies trusted remote hosts for rsh access. Use rhost + hostname to add a remote host, rhost - hostname to remove one, and rhost to display the list. The .rhosts file is considered insecure and has been largely replaced by SSH. It's not recommended to use rhost or .rhosts for remote access due to security risks. Instead, use SSH for secure remote access.

Lhost :

This variable contains the IP address of the attacker's system that is the IP address of the system from where we are initiating the exploit.

To insert rhost:

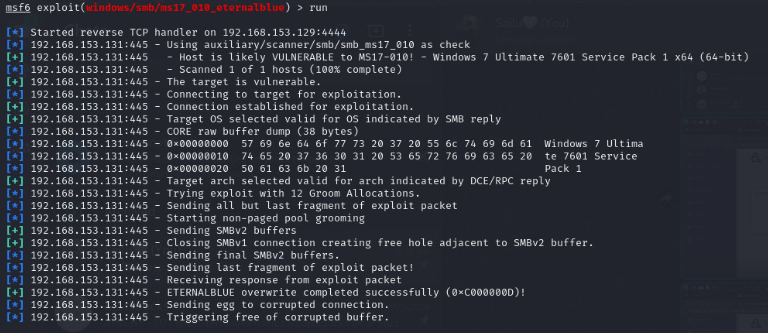
Syntax : rhost + hostname



To Run:

Command : run

The run command is used to execute an exploit or auxiliary module in Metasploit. It's a crucial command that initiates the attack or scan against a target system.



Hashdump :

The hashdump command in Metasploit extracts password hashes from a target system's SAM database or Active Directory database. It requires system-level access to the target system. The command outputs a list of usernames and their corresponding password hashes. The output can be used to crack the passwords using tools like John the Ripper or Hashcat. Use hashdump carefully, as it can be detected by security software and may trigger alarms.

Administrator: aad3b435b51404eeaad3b435b51404ee:58f5081696f366cdc72491a2c4996bd5::: User: aad3b435b51404eeaad3b435b51404ee:2b576acbe6bcfda7294d6bd18041b8fe:::

For Administrator :

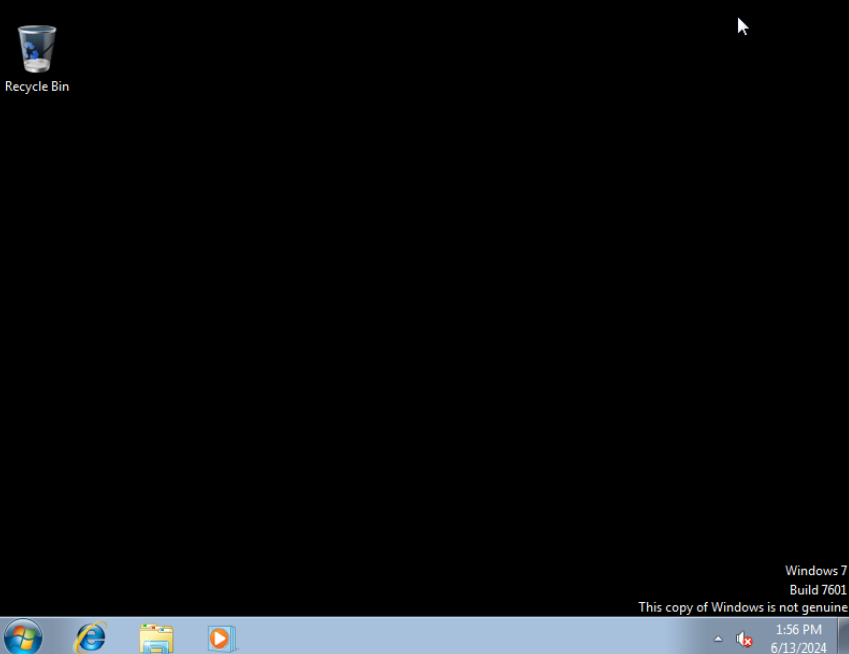


The Password for Administrator is **Password456!**

**For User :**

****

For user : the password is **Password123!**

****

I got logged in to the system as an **Administrator and User**. As you can see the tester got into your server with in that particular vulnerability called SMBv1(ms17-010) you have to update the server to cure that patch as software update and you have to use some defenders and firewalls.to protect yourself from malware and viruses.