

VAPT REPORT ON WINDOWS7

Varun Hegde | Cybersecurity -June 23 | 24/07/2023

**INTRODUCTION**

The purpose of this report to give an overview of the penetration testing conducted on Window 7 machine. The penetration testing was performed with intention of identifying the vulnerabilities and weakness within the window 7 operating system, assessing the potential impact of these vulnerabilities, and providing recommendations for remediation.

The penetration testing followed a systematic and controlled approach of industry best practices and ethical guidelines**.** The primary objective was to stimulate real-world attack and replicating the techniques and methodologies to find the vulnerabilities that could be exploited by us**.** By conducting the penetration test, we aimed to identify the weakness in the window 7 system, vulnerabilities and potential avenues for unauthorized access. This report will provide detailed information on the methodologies, tools and techniques are used during the testing process.

**TOOL USED: -**

**Arp-Scan: -** The command is used to perform an ARP (Address Resolution Protocol) scan on local network. It allows you to scan to discover the and display all the IP addresses and corresponding MAC (Media Access control) Addresses of connected to the same network. The ARP protocol is used to map IP Addresses to MAC Addresses, which is crucial for data transmission within a local network.

**Nmap: -** Nmap (Network mapper) is a powerful and widely used network scanning tool that has legitimate and ethical applications in network security, system administration and penetration testing. It design to discover hosts on a network, perform service and version detection and provide the valuable information about the devices and version detection, and provide valuable information about the devices and services and services running on those hosts.

Here how Nmap is used in the exploitation of window7:

1.Host Discovery

2.Port Scanning

3. Service and Version Detection

4.Vulnerability scanning

**METASPLOIT: -** Metasploit is widely-used penetration testing and exploitation framework that provides a collection of tools and resources o identify, validate and exploit vulnerabilities in various system and applications including window7.

Here are reasons why Metasploit is used in the exploitation of window 7: -

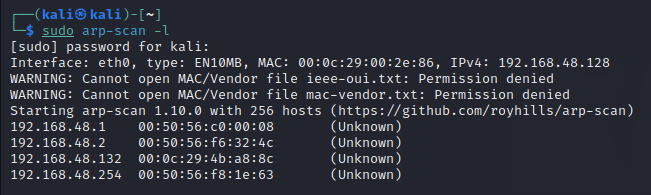
1.Exploit Development

2. Payloads

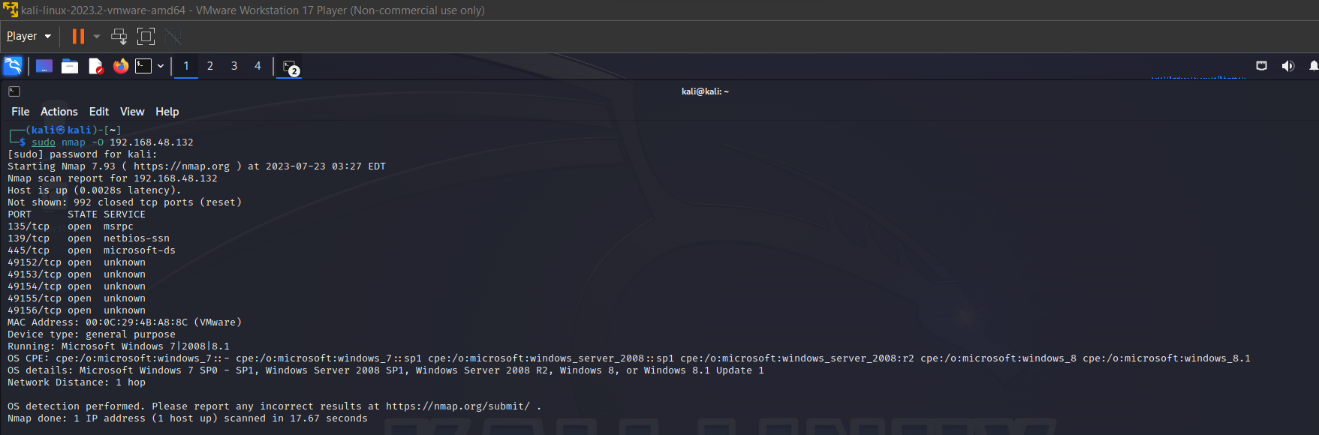
3.post-Exploitation

**Steps Taken to Exploit the vulnerable machine: -**

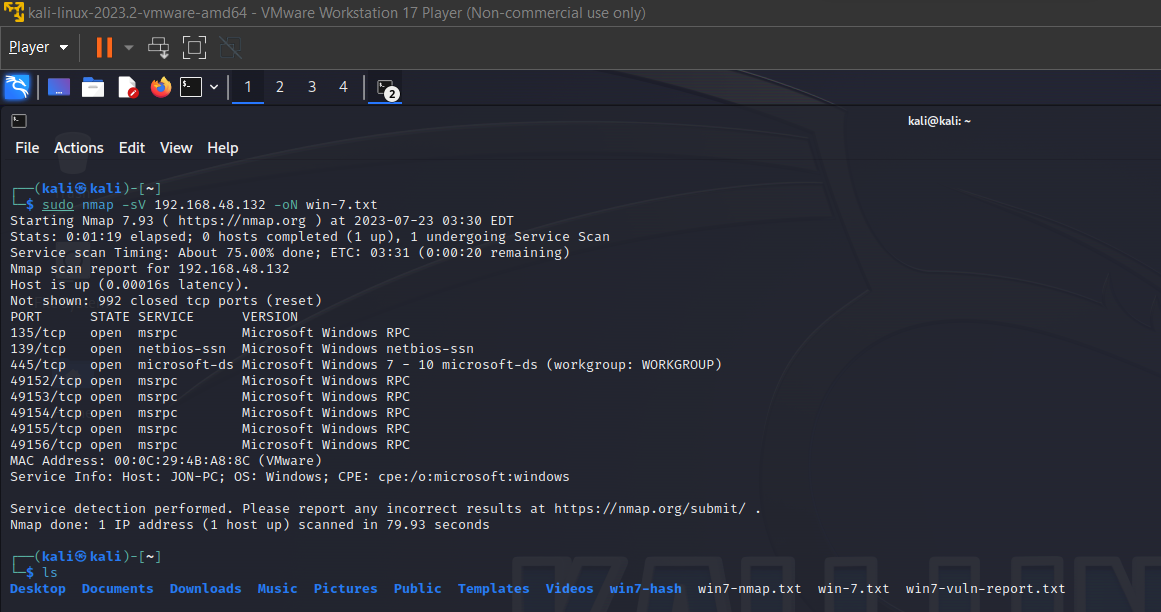
1. **sudo arp-scan -l** :- This is used to scan the the local network arp scan. The scan completion gives us the ip addresses



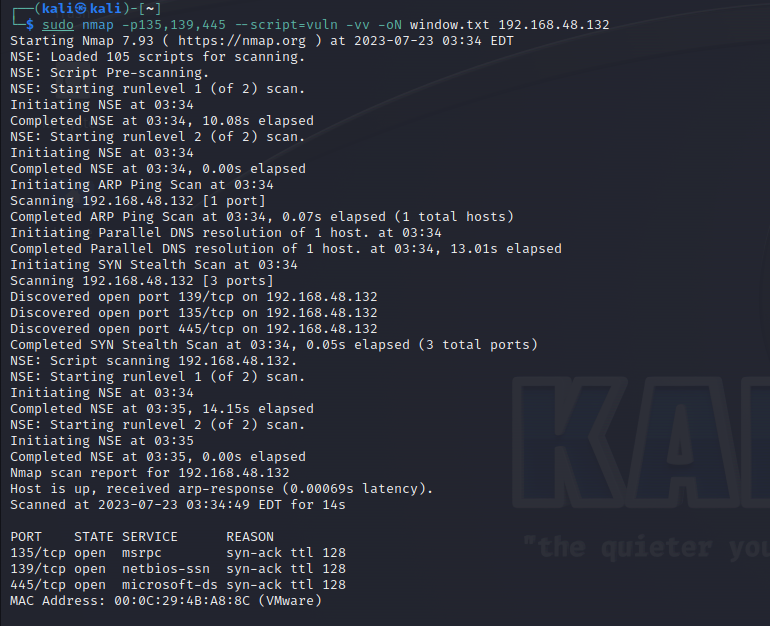
1. **sudo nmap -O 192.168.253.142:** - is used to perform OS (Operating System) detection on specific target IP addresses. By running this command with administrative privileges (using sudo), Nmap attempts to identify the operating system and its version running on the specified IP addresses. In this we have scan the 192.168.253.134 and found that it the IP addresses of our window machine that we want to exploit.

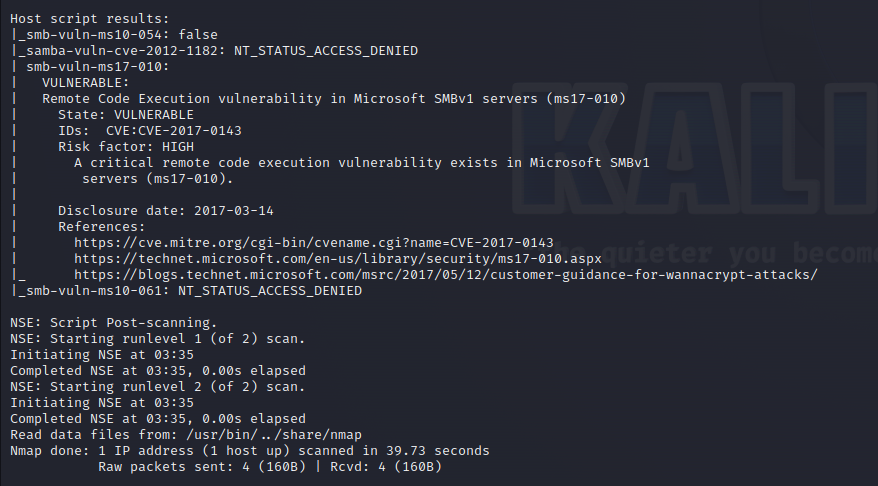


1. **Sudo nmap -sV ip -oN “filename.txt”: -** Command is used to perform a scan on the give IP address and the save the result in the given text file.”-sV” option enables the service detection.**-oN** this option specifies the output format and the file name for the scan result. We run this command and gets report on the directory we are working.



1. **Sudo nmap -p 135,139,445 –script =vuln –vv -oN window.txt 192.168.253.134:-** This command is used to perform the targeted vulnerability scan on the specific IP address . In this we scan the port no 135,139&139 which we get from the report. After scanning report and the ports we get that the machine contain the Vulnerability named **ms17-010(Eternalblue)**

****

****

The Windows 7 lab is running the following services:

SMBv1

HTTP

Telnet

The Windows 7 lab has the following vulnerabilities:

SMBv1 is enabled, which is a known security risk.

The HTTP service is running on port 80, which is a common port for web servers.

The Telnet service is running on port 23, which is a common port for remote administration.

Recommendations:

Disable SMBv1.

Harden the HTTP service.

Disable the Telnet service.

Conclusion:

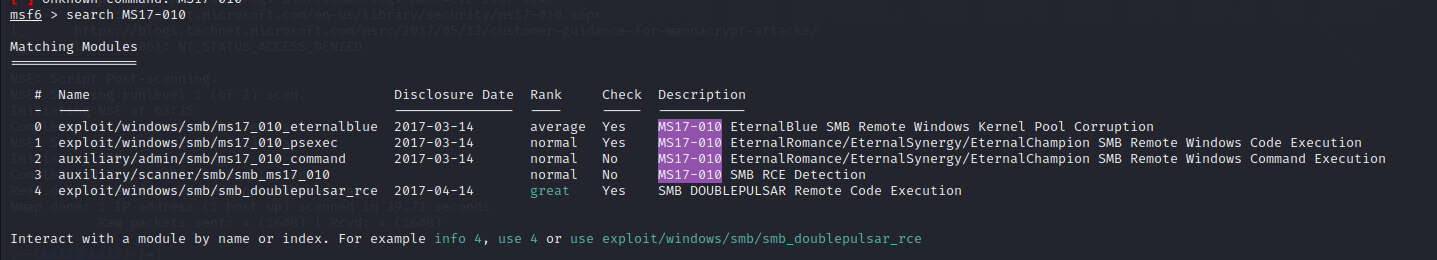
The Windows 7 lab has several vulnerabilities that could be exploited by an attacker. It is recommended that the vulnerabilities be addressed to improve the security of the lab.

**After knowing the vulnerability in machine, we started exploited the machine using Metasploit:**

1. To start the Metasploit we use the command msfconsole.

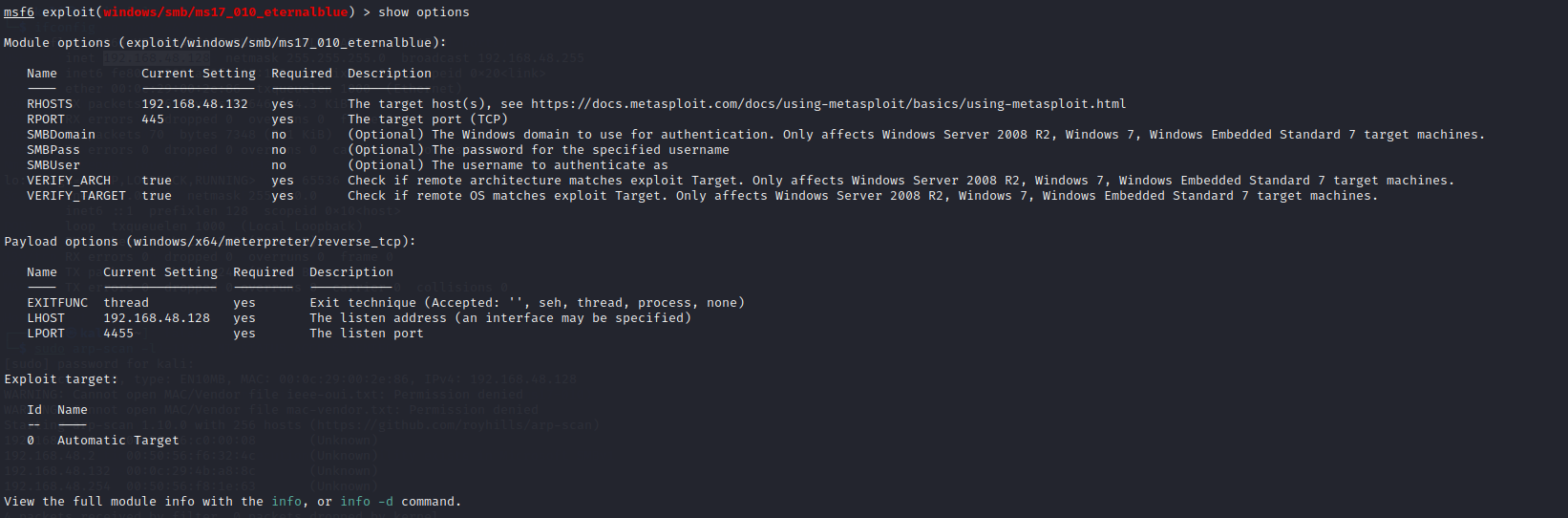
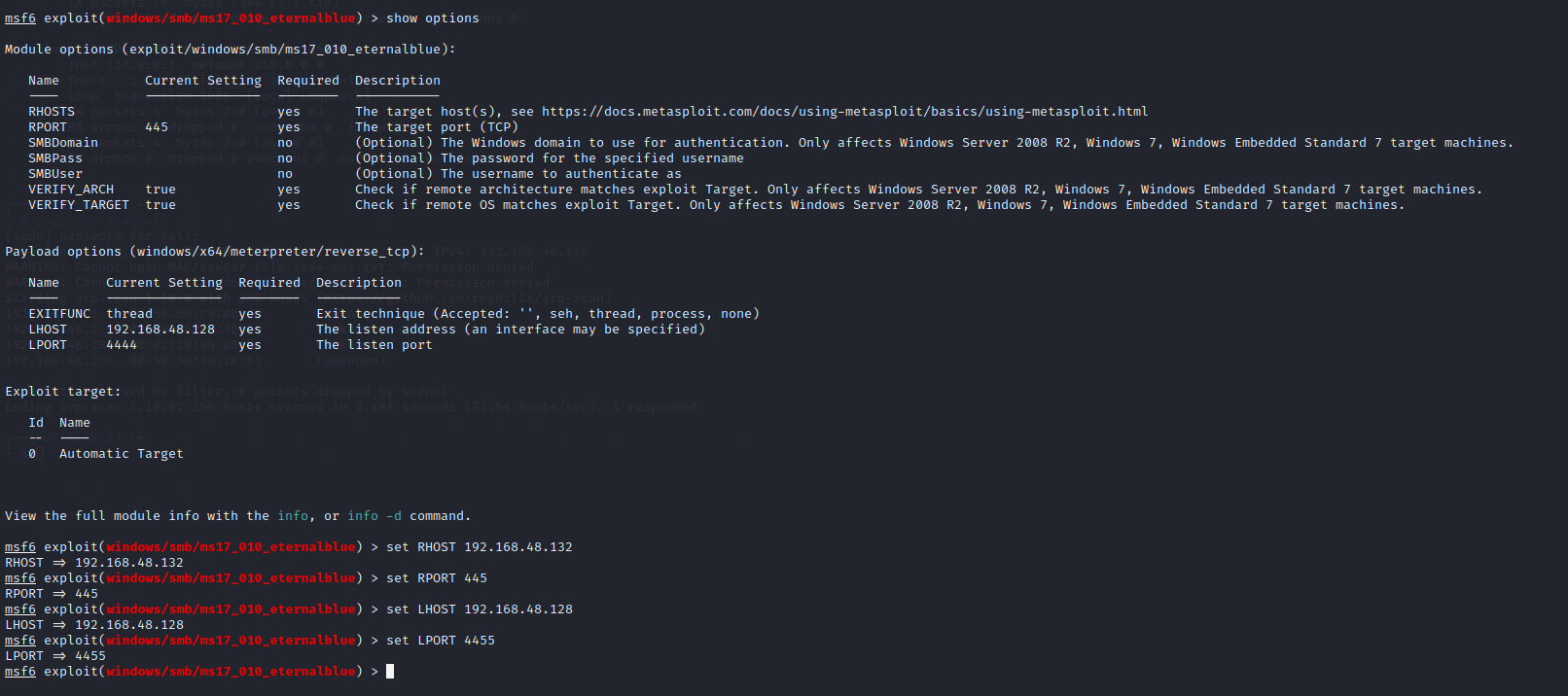


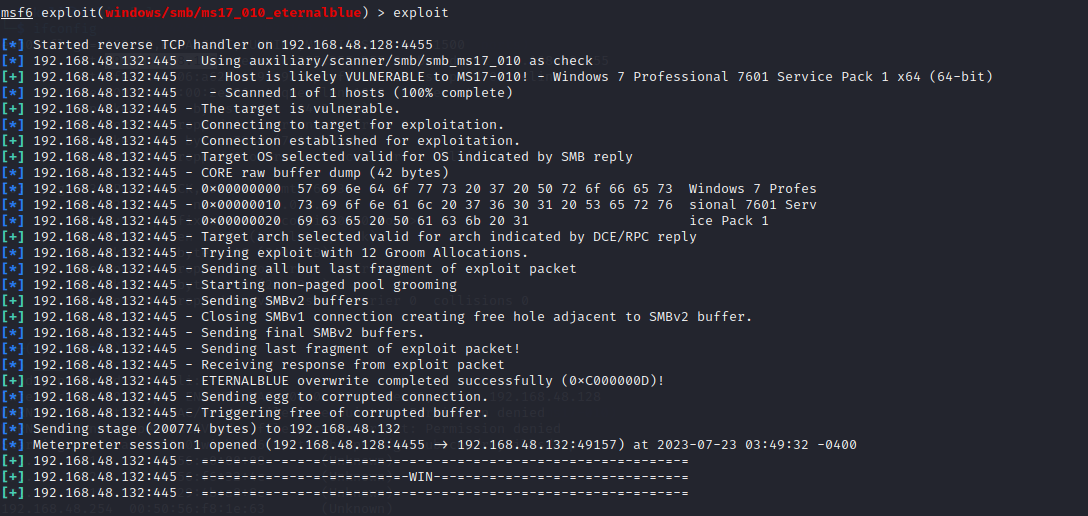
1. After entering into the Metasploit we search the vulnerability name ms17-010and we get the modules.



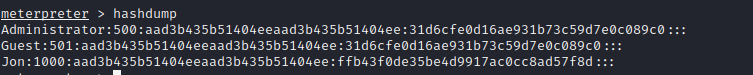
1. To interact with modules name or index. we have given the command **use “module no.” or info “module no”.**



1. Then we have set payloads. 
2. exploit.



**6.**After the command exploit the session was created. then we have to use the command the **hashdump.** **hashdump** is a term commonly associated with password-cracking tools, particularly in the context of penetration testing and security assessments. It refers to the process of extracting and dumping password hashes from a target system or a security database.

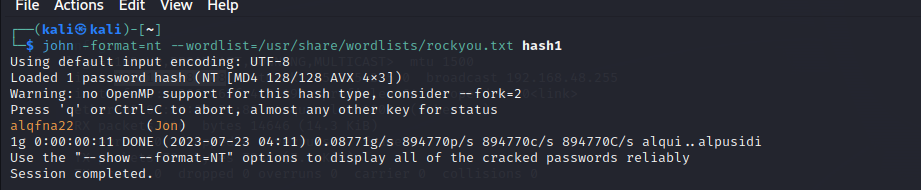


**7.**after the hashdump we get password of the machine in the hash form. now we have cracked the hash. There are many tools to crack the password but we are using **John The Ripper .**

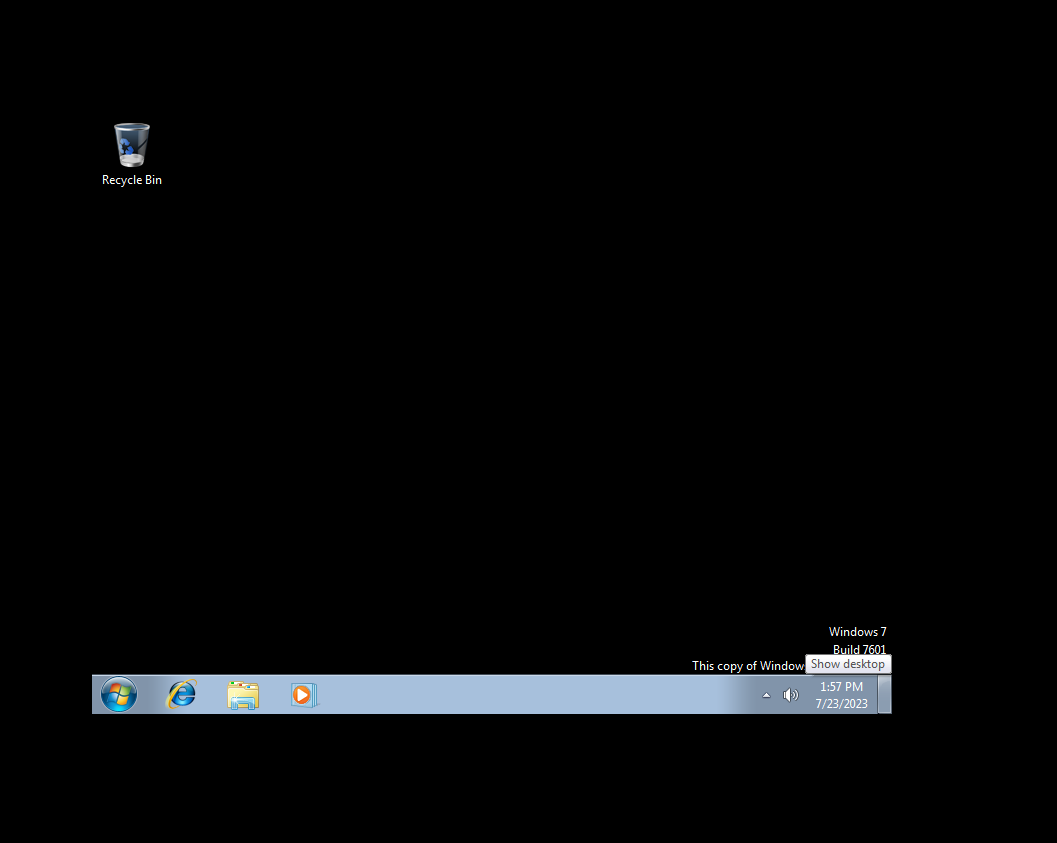
**8.** now create the file using nano editor to store the hash.

**9.** here the hash type we got is nt . so we have to crack the hash using command.

**john –format=nt --wordlist=/usr/share/wordlists/rockyou.txt “hashfile”**

****

**THE PASSOWRD OF THE VULNERABLE MACHINE IS** alqfna22



**Conclusion: -**

Keep the system up to date with the latest security patches.

Install and use a firewall.

Use antivirus and anti-malware software.

Be careful about what software you install on the system.

Be careful about what websites you visit and what links you click on.

**THANK YOU**