NAME [IP]

Relevant by TryHackMe

nano /etc/hosts
$MachineIP$ relevant.thm

HOST

OS: Windows Server 2016 Standard Evaluation 14393 (Windows Server 2016 Standard Evaluation 6.3)

ENUM

PORT STATE SERVICE REASON VERSION

80/tcp open http syn-ack Microsoft IIS httpd 10.0

135/tcp open msrpc syn-ack Microsoft Windows RPC

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

445/tcp open microsoft-ds syn-ack Windows Server 2016 Standard Evaluation 14393 microsoft-ds

3389/tcp open ms-wbt-server syn-ack Microsoft Terminal Services

VULN

tcp/445/nmap-smb - Nmap script found a potential vulnerability. (State: VULNERABLE)

Possible Post: exploit/windows/local/cve_2017_8464_lnk_lpe

SERVICE ENUM

TCP

[NMAP OVERVIEW]

Nmap 7.91 scan initiated Tue Mar 23 23:17:04 2021 as: nmap -vv --reason -Pn -sV -sC --version-all -oN /home/user/Desktop/results/-10.10.124.236/scans/_quick_tcp_nmap.txt -oX /home/user/Desktop/results/10.10.124.236/scans/xml/_quick_tcp_nmap.xml 10.10.124.236
Nmap scan report for 10.10.124.236
Host is up, received user-set (0.18s latency).
Scanned at 2021-03-23 23:17:04 GMT for 85s
Not shown: 995 filtered ports
Reason: 995 no-responses
PORT STATE SERVICE REASON VERSION
80/tcp open http syn-ack Microsoft IIS httpd 10.0
| http-methods:
| Supported Methods: OPTIONS TRACE GET HEAD POST
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
135/tcp open msrpc syn-ack Microsoft Windows RPC
139/tcp open netbios-ssn syn-ack Microsoft Windows netbios-ssn
445/tcp open microsoft-ds syn-ack Windows Server 2016 Standard Evaluation 14393 microsoft-ds
3389/tcp open ms-wbt-server syn-ack Microsoft Terminal Services
| rdp-ntlm-info:
| Target_Name: RELEVANT
| NetBIOS_Domain_Name: RELEVANT

```
|   NetBIOS_Computer_Name: RELEVANT
|   DNS_Domain_Name: Relevant
|   DNS_Computer_Name: Relevant
|   Product_Version: 10.0.14393
|_  System_Time: 2021-03-23T23:17:49+00:00
| ssl-cert: Subject: commonName=Relevant
| Issuer: commonName=Relevant
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-03-22T23:05:09
| Not valid after:  2021-09-21T23:05:09
| MD5:   29bb f252 f8d1 666a c46c 6821 d0ef 0263
| SHA-1: b428 357e 13a7 a71b e2ca 3db3 5086 3dcc a287 83a4
| -----BEGIN CERTIFICATE-----
| MIIC1DCCAbygAwIBAgIQGjaCJocCeptHTv+SyXn2QjANBgkqhkiG9w0BAQsFADAT
| MREwDwYDVQQDEwhSZWxldmFudDAeFw0yMTAzMjIyMzA1MDlaFw0yMTA5MjEyMzA1
| MDlaMBMxETAPBgNVBAMTCFJlbGV2YW50MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
| MIIBCgKCAQEAtAL+hyuRioSIv217KRbjifZ4a5ESpGxXJVJ/1A2NpNz6yqH5v+zW
| ZV/1WHP7Nf0+0t3z3MDBsVOdzgLKGWcFDMlLwaHXcFV9a26JpW2+i2CaDwigqS5C
| eoro0yLJnknHgxIMz/FgaE3YsgV9xeoQlr0AfDZARdloSyqofRD8GY38VQqxKtQj
| hdonDO2qyrTAcKK0uV78H8AEkDKc/x4YCImUkgHJrBAKyH4weKOWyqII7tDS+4GA
| 3LoD715fuk2DCiifY/At6muKUy+agZZVsUeoyF7TMjZ4l80K2dDnr66algvHk3Wj
| DJTlPLoXvgckln0LmM4G5FgFEOF11arOlQIDAQABoyQwIjATBgNVHSUEDDAKBggr
| BgEFBQcDATALBgNVHQ8EBAMCBDAwDQYJKoZIhvcNAQELBQADggEBAHTUFX0OdIxI
| 6QCAbCkKkLqj7UzM3DCT5FTkgDvJhfO3SMrEZrd+LXmfguojyRS+R9i4/6Cr+iB+
| 7Cdq7l1bRIUkgtG9DX/zVM7vXaBCQ7skhzkCnPbTsii6ZkAVcN3XtBNgNiKHmHjZ
| bRGybTbyazUK17lat/EEEVgSH9vFGs9DihiUgYeBbQIiQ3unzQWJEIUceFKYBiKe
| PpFEFNQWpXgCReNqY5rZCWWpHmWNz8wgrq634vAZFFkZkuyHf6IB28EU2BX/QdBZ
| yAzSdYdX8E8psHjanpHlCzBTXukz00O6MOuwbel3s31T3HUTQlJt3+uNCBZ13DEH
| KV2DuGG5Ivg=
|_-----END CERTIFICATE-----
|_ssl-date: 2021-03-23T23:18:28+00:00; 0s from scanner time.
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1h24m00s, deviation: 3h07m50s, median: 0s
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 31361/tcp): CLEAN (Timeout)
|   Check 2 (port 24639/tcp): CLEAN (Timeout)
|   Check 3 (port 47514/udp): CLEAN (Timeout)
|   Check 4 (port 36235/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-os-discovery:
|   OS: Windows Server 2016 Standard Evaluation 14393 (Windows Server 2016 Standard Evaluation 6.3)
|   Computer name: Relevant
|   NetBIOS computer name: RELEVANT\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2021-03-23T16:17:49-07:00
| 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: 2021-03-23T23:17:51
|_  start_date: 2021-03-23T23:05:10

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

HTTP (80)

Nothing of too much intrest it seems for right now its gonna be a microsoft server side thing

ENUM

This enum is useful because the box seems to hide a secondary webserver at a higher port so that our basic scans don't find it which is unfortunate since using RUSTSCAN, Threader3000, or nmap with the ratelimit modified you can scan all 65k ports in under a minute on average with a VM

nikto

SCAN OUTPUT

```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.124.236
+ Target Hostname:    10.10.124.236
+ Target Port:        80
+ Start Time:         2021-03-23 23:18:30 (GMT0)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/10.0
+ Retrieved x-powered-by header: ASP.NET
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Retrieved x-aspnet-version header: 4.0.30319
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect (timeout): Operation now in progress
+ Scan terminated:  19 error(s) and 7 item(s) reported on remote host
+ End Time:           2021-03-23 23:31:52 (GMT0) (802 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

nmap

SCAN OUTPUT

```
# Nmap 7.91 scan initiated Tue Mar 23 23:18:29 2021 as: nmap -vv --reason -Pn -sV -p 80 "--script=banner,(http* or ssl*) and not (brute or broadcast or dos or external or http-slowloris* or fuzzer)" -oN /home/user/Desktop/results/10.10.124.236/scans/-tcp_80_http_nmap.txt -oX /home/user/Desktop/results/10.10.124.236/scans/xml/tcp_80_http_nmap.xml 10.10.124.236
Nmap scan report for 10.10.124.236
Host is up, received user-set (0.43s latency).
Scanned at 2021-03-23 23:18:30 GMT for 188s

PORT   STATE SERVICE REASON  VERSION
80/tcp open  http    syn-ack Microsoft IIS httpd 10.0
|_http-chrono: Request times for /; avg: 16039.76ms; min: 16026.29ms; max: 16049.03ms
| http-comments-displayer:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.10.124.236
|
|     Path: http://10.10.124.236:80/
|     Line number: 7
|     Comment:
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
```

```
|
|
|_       -->
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-date: Tue, 23 Mar 2021 23:18:38 GMT; +59m59s from local time.
|_http-devframework: ASP.NET detected. Found related header.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-errors: Couldn't find any error pages.
|_http-feed: Couldn't find any feeds.
|_http-fetch: Please enter the complete path of the directory to save data in.
| http-headers:
|   Content-Length: 703
|   Content-Type: text/html
|   Last-Modified: Sat, 25 Jul 2020 15:05:21 GMT
|   Accept-Ranges: bytes
|   ETag: "2db43349562d61:0"
|   Server: Microsoft-IIS/10.0
|   X-Powered-By: ASP.NET
|   Date: Tue, 23 Mar 2021 23:18:43 GMT
|   Connection: close
|
|_  (Request type: HEAD)
|_http-jsonp-detection: Couldn't find any JSONP endpoints.
|_http-litespeed-sourcecode-download: Request with null byte did not work. This web server might not be vulnerable
|_http-malware-host: Host appears to be clean
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-mobileversion-checker: No mobile version detected.
| http-php-version: Logo query returned unknown hash 242c23ea412530c7d94b77a7a978c176
|_Credits query returned unknown hash 242c23ea412530c7d94b77a7a978c176
|_http-referer-checker: Couldn't find any cross-domain scripts.
|_http-security-headers:
|_http-server-header: Microsoft-IIS/10.0
| http-sitemap-generator:
|   Directory structure:
|     /
|       Other: 1
|   Longest directory structure:
|     Depth: 0
|     Dir: /
|   Total files found (by extension):
|_    Other: 1
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-title: IIS Windows Server
| http-useragent-tester:
|   Allowed User Agents:
|     Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
|     libwww
|     lwp-trivial
|     libcurl-agent/1.0
|     PHP/
|     Python-urllib/2.5
|     GT::WWW
|     Snoopy
|     MFC_Tear_Sample
|     HTTP::Lite
|     PHPCrawl
|     URI::Fetch
|     Zend_Http_Client
|     http client
|   Change in Status Code:
|     WWW-Mechanize/1.34: 200
|     Wget/1.13.4 (linux-gnu): 200
|_    PECL::HTTP: 200
| http-vhosts:
|_128 names had status 200
|_http-wordpress-users: [Error] Wordpress installation was not found. We couldn't find wp-login.php
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

Nmap done at Tue Mar 23 23:21:38 2021 -- 1 IP address (1 host up) scanned in 188.84 seconds

Threader3000

```
        Threader 3000 - Multi-threaded Port Scanner
                    Version 1.0.7
                A project by The Mayor
---------------------------------------------------------------
Enter your target IP address or URL here: 10.10.222.206
---------------------------------------------------------------
Scanning target 10.10.222.206
Time started: 2021-03-25 03:36:46.777855
---------------------------------------------------------------
Port 49669 is open
Port 49663 is open
Port 49667 is open
Port scan completed in 0:01:42.281303
```

SERVER

Version:Microsoft-IIS/10.0

NOTES AND THEORIES

RABBIT HOLE

HTTP (49963)

Attack Vector 2

VULNS

VULN A

Name: File Upload and Execution due to exposed SMB share
Link: http://relevant.tm:49663/nt4wrksv/shell.aspx
What does it do: Allows for the uploading of malisous code to a web server that shows the smb directory hosted from the computers directory
What does it require: A reverse shell and a connection to the smb server

Explain code:

Reverse Tcp connection that executes due to the visiting of file on the SMB share directory nt4wrksv that is exposed on the web server hosted on port 496634

SMB

NAME Relevant
VERSION OS: Windows Server 2016 Standard Evaluation 14393 (Windows Server 2016 Standard Evaluation 6.3)
What does this service do? Server Message Block is a network protocol that enables users to communicate with remote computers and servers
What is the most valuable asset this service has/has access to? SMB exploits have the option to directly go to root without privesc and also has the ability to spread like a worm (SMBGHOST)
What are its sensitive files?
PASSWORDS: Passwords.txt
USERS: Bob and Bill
Technologies used: smbclient

ENUM

smbclient

mbclient -L 10.10.107.193
Enter WORKGROUP\root's password:

```
        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        nt4wrksv        Disk
SMB1 disabled -- no workgroup available
```

---

smbclient\\\\10.10.107.193\nt4wrksv

nmap

```
3389/tcp open  ms-wbt-server syn-ack Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: RELEVANT
|   NetBIOS_Domain_Name: RELEVANT
|   NetBIOS_Computer_Name: RELEVANT
|   DNS_Domain_Name: Relevant
|   DNS_Computer_Name: Relevant
|   Product_Version: 10.0.14393
|_  System_Time: 2021-03-23T23:17:49+00:00
| ssl-cert: Subject: commonName=Relevant
| Issuer: commonName=Relevant
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-03-22T23:05:09
| Not valid after:  2021-09-21T23:05:09
| MD5:   29bb f252 f8d1 666a c46c 6821 d0ef 0263
| SHA-1: b428 357e 13a7 a71b e2ca 3db3 5086 3dcc a287 83a4
| -----BEGIN CERTIFICATE-----
| MIIC1DCCAbygAwIBAgIQGjaCJocCeptHTv+SyXn2QjANBgkqhkiG9w0BAQsFADAT
| MREwDwYDVQQDEwhSZWxldmFudDAeFw0yMTAzMjIyMzA1MDlaFw0yMTA5MjEyMzA1
| MDlaMBMxETAPBgNVBAMTCFJlbGV2YW50MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
| MIIBCgKCAQEAtAL+hyuRioSIv217KRbjifZ4a5ESpGxXJVJ/1A2NpNz6yqH5v+zW
| ZV/1WHP7Nf0+0t3z3MDBsVOdzgLKGWcFDMlLwaHXcFV9a26JpW2+i2CaDwigqS5C
| eoro0yLJnknHgxlMz/FgaE3YsgV9xeoQlr0AfDZARdloSyqofRD8GY38VQqxKtQj
| hdonDO2qyrTAcKK0uV78H8AEkDKc/x4YCImUkgHJrBAKyH4weKOWyqII7tDS+4GA
| 3LoD715fuk2DCiifY/At6muKUy+agZZVsUeoyF7TMjZ4l80K2dDnr66algvHk3Wj
| DJTlPLoXvgckln0LmM4G5FgFEOF11arOlQIDAQABoyQwIjATBgNVHSUEDDAKBggr
| BgEFBQcDATALBgNVHQ8EBAMCBDAwDQYJKoZIhvcNAQELBQADggEBAHTUFX0OdIxI
| 6QCAbCkKkLqj7UzM3DCT5FTkgDvJhfO3SMrEZrd+LXmfguojyRS+R9i4/6Cr+iB+
| 7Cdq7l1bRlUkgtG9DX/zVM7vXaBCQ7skhzkCnPbTsii6ZkAVcN3XtBNgNiKHmHjZ
| bRGybTbyazUK17lat/EEEVgSH9vFGs9DihiUgYeBbQIiQ3unzQWJEIUceFKYBiKe
| PpFEFNQWpXgCReNqY5rZCWWpHmWNz8wgrq634vAZFFkZkuyHf6IB28EU2BX/QdBZ
| yAzSdYdX8E8psHjanpHlCzBTXukz00O6MOuwbel3s31T3HUTQlJt3+uNCBZ13DEH
| KV2DuGG5Ivg=
|_-----END CERTIFICATE-----
|_ssl-date: 2021-03-23T23:18:28+00:00; 0s from scanner time.
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1h24m00s, deviation: 3h07m50s, median: 0s
| p2p-conficker:
|   Checking for Conficker.C or higher...
```

| Check 1 (port 31361/tcp): CLEAN (Timeout)
| Check 2 (port 24639/tcp): CLEAN (Timeout)
| Check 3 (port 47514/udp): CLEAN (Timeout)
| Check 4 (port 36235/udp): CLEAN (Timeout)
|_ 0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-os-discovery:
| OS: Windows Server 2016 Standard Evaluation 14393 (Windows Server 2016 Standard Evaluation 6.3)
| Computer name: Relevant
| NetBIOS computer name: RELEVANT\x00
| Workgroup: WORKGROUP\x00
|_ System time: 2021-03-23T16:17:49-07:00
| 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: 2021-03-23T23:17:51
|_ start_date: 2021-03-23T23:05:10

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done at Tue Mar 23 23:18:29 2021 -- 1 IP address (1 host up) scanned in 85.33 seconds

Enum4Linux

enum4linux -a -r -o -i -n -v mbclient -L 10.10.107.193
Enter WORKGROUP\root's password:

        Sharename   Type   Comment
        ---------   ----   -------
        ADMIN$ Disk   Remote Admin
        C$ Disk   Default share
        IPC$ IPC   Remote IPC
        nt4wrksv   Disk
SMB1 disabled -- no workgroup available
[V] Dependent program "nmblookup" found in /usr/bin/nmblookup
[V] Dependent program "net" found in /usr/bin/net
[V] Dependent program "rpcclient" found in /usr/bin/rpcclient
[V] Dependent program "smbclient" found in /usr/bin/smbclient
[V] Dependent program "polenum" found in /usr/bin/polenum
[V] Dependent program "ldapsearch" found in /usr/bin/ldapsearch
Starting enum4linux v0.8.9 (http://labs.portcullis.co.uk/application/enum4linux/) on Wed Mar 24 04:19:21 2021

 ==========================
| Target Information |
 ==========================
Target ..... mbclient
RID Range 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

 ==
| Enumerating Workgroup/Domain on mbclient |
 ==
[V] Attempting to get domain name with command: nmblookup -A 'mbclient'
[E] Can't find workgroup/domain

 =====================================
| Nbtstat Information for mbclient |
 =====================================
Looking up status of 0.0.0.0
No reply from 0.0.0.0

 ================================
| Session Check on mbclient |

```
 ==================================
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 437.
[V] Attempting to make null session using command: smbclient -W '' //'mbclient'/ipc$ -U''%'' -c 'help' 2>&1
[E] Server doesn't allow session using username '', password ''.  Aborting remainder of tests.
>
>
>
>
> e
> exit
>
```

nmapvulnscan

nmap -oA nmap-vuln -Pn -script vuln -p 80,135,139,445,3389 10.10.61.45

```
PORT     STATE SERVICE
80/tcp   open  http
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
|_ssl-ccs-injection: No reply from server (TIMEOUT)
|_sslv2-drown:

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
| 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://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Nmap done: 1 IP address (1 host up) scanned in 172.95 seconds
```

STEPS TAKEN FOR ENUM

Used tool AutoRecon too have initial recon to be in the background while I investigated the port scan; then seeing SMB I did a nmapvuln scan to see if I could do anything with Samba and found EternalBlue Exploit that we are going to try to exploit using the username and password that we aquired from the SMB share.

VULN

This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker sends specially crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server.

This security update is rated Critical for all supported releases of Microsoft Windows. For more information, see the Affected Software and Vulnerability Severity Ratings section.

The security update addresses the vulnerabilities by correcting how SMBv1 handles specially crafted requests.

For more information about the vulnerabilities, see the Vulnerability Information section.

For more information about this update, see Microsoft Knowledge Base Article 4013389.

STEPS TO CONFIRM VULN

[Nmap Vuln Scan Output]

```
 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).
```

NOTES AND THEORIES

It seems that eternalblue exploit exists but I don't really feel like installing pip2 and mysmb so we are just going to go with the hidden web server

SUMMARY OF VULNERABILITIES

2 vulnerabilites found.

First, Eternal{Blue/Romance} which is a CVE 9-10 so pretty bad.

Second, Remote File and code execution vulnerability that allows for us to open a reverse tcp connection. Using both a Reverse shell and web based command prompt

POST-EX

This is where I got stuck.

ENUM

God I hate Windows

PERMISSIONS

```
c:\windows\system32\inetsrv>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeAuditPrivilege              Generate security audits                  Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
```

SUMMARY OF VULNERABILITIES

Permission vulnerability

ATTACK SURFACE

What are the vulnerabilities?

if you have SeAssignPrimaryToken or SeImpersonate privilege, you are SYSTEM

They allow you to run code or even create a new process in the context of another user

What seems most likely or most straightforward to leverage and why?

This Vuln

Do we have all the correct files/versions/access to exploit?

YES

LOOT

CREDS

Bob - !P******D!
Bill - Ju**********$

PROOF

C:\Windows\system32>whoami
whoami
nt authority\system

SUMMARY OF ESCALATION

Name: Set ImpersonatePrivilege Exploit
Link: https://github.com/itm4n/PrintSpoofer
TYPE: Privelage Impersonation
EXPLANATION: Allows you to impersonate system and spawn a shell

HOW WAS THIS DISCOVERED (should be in steps for enum, vuln)?

Googling

HOW WAS THIS EXPLOITED?

By using PrintSpoofer tool found by said googling

MISC NOTES

Dump whatever in here.

PrintSpoofer - Github: https://github.com/dievus/printspoofer

Check me out at Monopolys Cyber World: https://www.youtube.com/channel/UCIbKn80E8gwRHOin82dzv7w