Penetration Test Report - Relevant

MrG3tty
TRYHACKME

Contents

Executive Summary

MrG3tty Security (MGS) was contracted by THM Labs to conduct a penetration test on a virtual environment. All activities were conducted in a manner that simulated a malicious actor engaged in a targeted attack against Relevant with the goals of:

- Identifying if a remote attacker could obtain remote control of Relevant
- Determine the impact of a security breach on:
    - Confidentiality of Relevant's data
    - Secure User.txt and Root.txt as proof of machine compromise

Efforts were focused on the identification and exploitation of misconfigurations, and security weaknesses that could allow a remote attacker to gain unauthorized access to private data. The attack was conducted with a level of access that a general internet user would have.

Summary of Results

Initial reconnaissance of Relevant resulted in the discovery of open Server Message Block Shares. Further enumeration revealed the share names. The discovery of the misconfigured SMB service allowed the finding of hashed credentials in a text file, and allowed the upload of a malicious payload, facilitating remote access to the system as a low-level user.

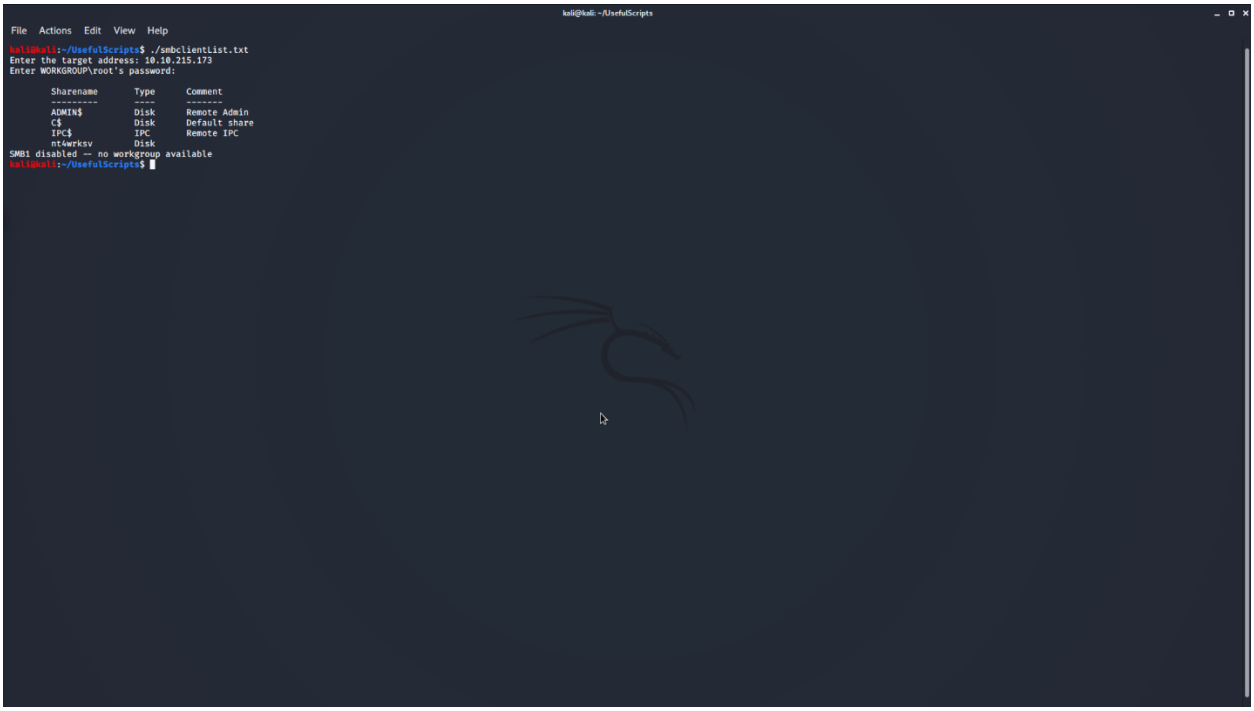
System examination revealed that Relevant has SeImpersonatePrivilege enabled. The use of printspoofer.exe allowed us to abuse this privilege to impersonate the system administrator and gain full control over the machine. Using the privileges of system admin, we were able to recover both the user.txt and the root.txt flag. (https://itm4n.github.io/printspoofer-abusing-impersonate-privileges/ n.d.)

Remote System Recon

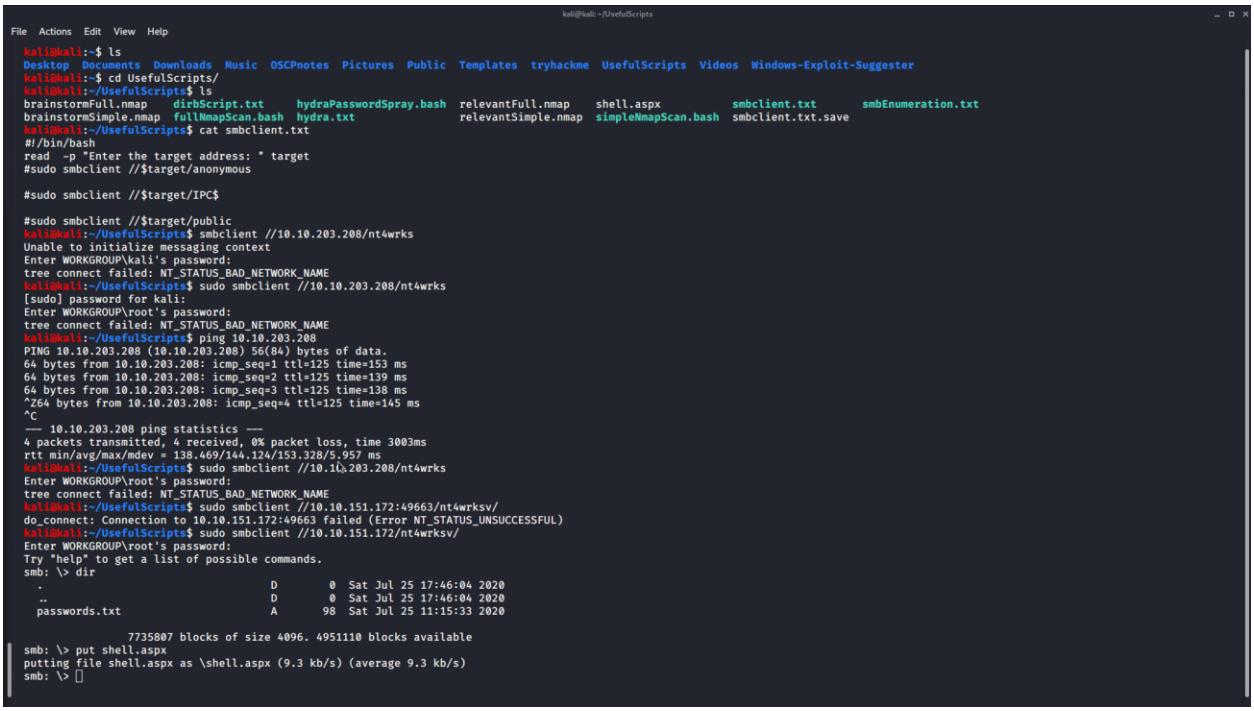
For the purposes of this assessment, MGS was provided with minimal information outside of the IP address of the target host. Manual exploitation methods were used throughout the engagement.

To gain initial knowledge on what services are running on the target, we examined the open ports as shown in Figure 1.

From the output from nmap, we can see that remote desk protocol and simple message block is exposed to the public. We do not currently have any credentials, so we will leave RDP alone for now, and enumerate SMB in figure 2.



Now that we know some of the shares available running on this machine, we try to anonymously connect to them. We succeed with this tactic, by anonymously signing into the nt4wrksv share shown in figure 3.

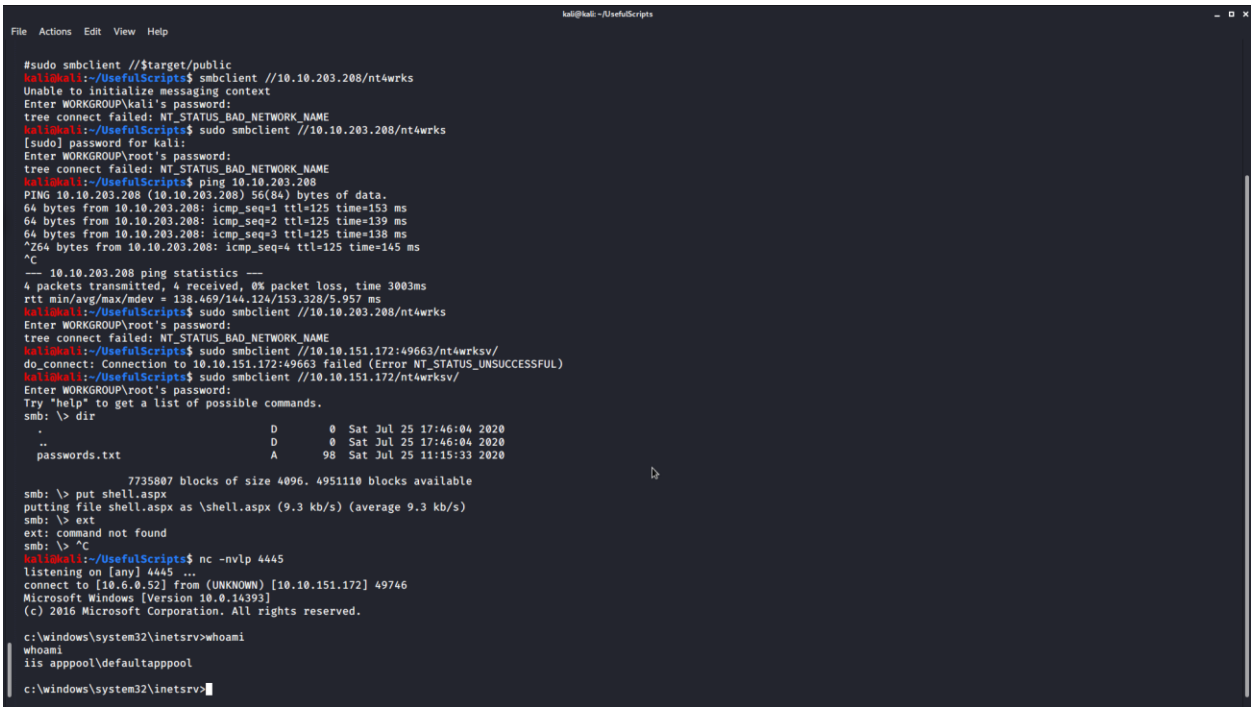


In figure 3, we can see that there is a passwords.txt file. We can download this to our attack machine and inspect the contents. The file contains a hash: Qm9iIC0gIVBAJCRXMHJEITEyMw==

QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk

We can decrypt this hash, and we are left with: Bob - !P@$$W0rD!123

This password failed to get us an RDP session, so Bob may have changed his password since creating this file. While we did not get an RDP session, we were able to upload a malicious payload as shown in figure 3 and trigger a reverse shell as shown in Figure 4.



Once we have an initial reverse shell, we can begin enumerating the system, user, network, passwords, anti-virus, and firewall. This information will be included in the appendix.

System Enumeration

Host Name:	RELEVANT
OS Name:	Microsoft Windows Server 2016 Standard Evaluation
OS Version:	10.0.14393 N/A Build 14393

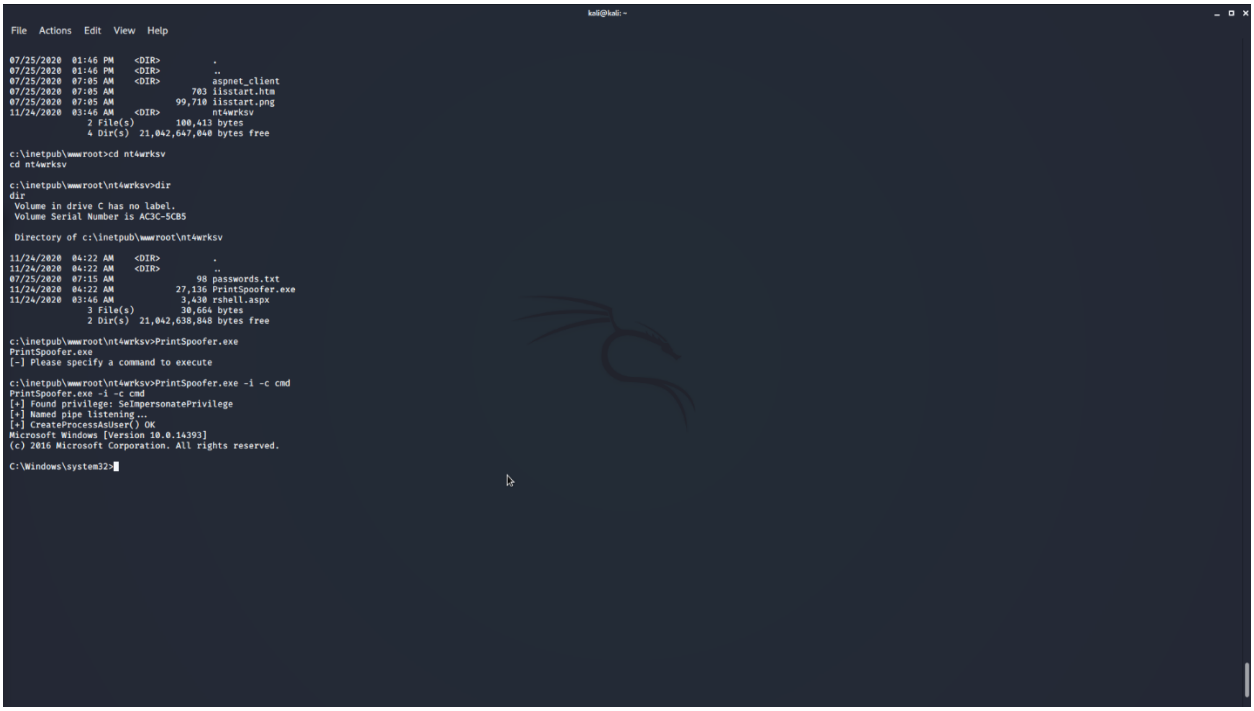
User Enumeration

SeImpersonatePrivilege	Impersonate a client after authentication Enabled

These are small snippets from our system and user enumeration output. This is enough information to let us know that this system is possibly vulnerable to potato and printspoofer attacks. All attempts at potato attacks failed, so we moved on to printspoofer.

Privilege Escalation

After uploading our printspoofer executable to the nt4wrksv smb share, we navigate to its location from our initial reverse shell and execute it. This triggers our net cat listener and gives us an administrator reverse shell as shown in figure 5.



Appendix

###Nmap###

Nmap 7.80 scan initiated Sun Nov 22 21:05:33 2020 as: nmap -sV -sC -v -Pn --min-rate 5000 -oN relevantSimple.nmap 10.10.129.133

Nmap scan report for 10.10.129.133

Host is up (0.18s latency).

Not shown: 995 filtered ports

PORT STATE SERVICE VERSION

80/tcp open http 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 Microsoft Windows RPC

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

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

3389/tcp open ms-wbt-server 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: 2020-11-23T02:05:47+00:00

| ssl-cert: Subject: commonName=Relevant

| Issuer: commonName=Relevant

| Public Key type: rsa

| Public Key bits: 2048

| Signature Algorithm: sha256WithRSAEncryption

| Not valid before: 2020-07-24T23:16:08

| Not valid after: 2021-01-23T23:16:08

| MD5: aa09 9a56 8e66 6a87 ca06 7b93 aeae 7032

|_SHA-1: 46f8 9a48 9216 c45b 555c 6f42 690e 3aa0 a694 dc37

|_ssl-date: 2020-11-23T02:06:26+00:00; +3s from scanner time.

Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:

|_clock-skew: mean: 1h36m04s, deviation: 3h34m40s, median: 3s

| 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: 2020-11-22T18:05:48-08:00

| 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: 2020-11-23T02:05:50

|_ start_date: 2020-11-23T01:57:30

Read data files from: /usr/bin/../share/nmap

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done at Sun Nov 22 21:06:23 2020 -- 1 IP address (1 host up) scanned in 50.27 seconds

PORT STATE SERVICE VERSION

80/tcp open http Microsoft IIS httpd 10.0

135/tcp open msrpc Microsoft Windows RPC

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

445/tcp open microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds

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

49663/tcp open http Microsoft IIS httpd 10.0

Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

###SMB Enumeration###

PORT STATE SERVICE

445/tcp open microsoft-ds

Host script results:

| smb-enum-shares:

| account_used: guest

| \\10.10.129.133\ADMIN$:

| Type: STYPE_DISKTREE_HIDDEN

| Comment: Remote Admin

| Anonymous access: <none>

| Current user access: <none>

| \\10.10.129.133\C$:

| Type: STYPE_DISKTREE_HIDDEN

| Comment: Default share
| Anonymous access: <none>
| Current user access: <none>
| \\10.10.129.133\IPC$:
| Type: STYPE_IPC_HIDDEN
| Comment: Remote IPC
| Anonymous access: <none>
| Current user access: READ/WRITE
| \\10.10.129.133\nt4wrksv:
| Type: STYPE_DISKTREE
| Comment:
| Anonymous access: <none>
|_ Current user access: READ/WRITE
|_smb-enum-users: ERROR: Script execution failed (use -d to debug)

###Interesting Finds###

Within://10.10.206.158/nt4wrksv

stored within a text file named passwords.txt

Penetration Test Report - Relevant

Qm9iIC0gIVBAJCRXMHJEITEyMw==

QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk

###Initial foothold###

I uploaded a aspx reverse shell using the smb services on nt4wrksv. I triggered it using curl.

###System Enumeration###

Host Name: RELEVANT

OS Name: Microsoft Windows Server 2016 Standard Evaluation

OS Version: 10.0.14393 N/A Build 14393

OS Manufacturer: Microsoft Corporation

OS Configuration: Standalone Server

OS Build Type: Multiprocessor Free

Registered Owner: Windows User

Registered Organization:

Product ID: 00378-00000-00000-AA739

Original Install Date: 7/25/2020, 7:56:59 AM

Penetration Test Report - Relevant

System Boot Time: 11/23/2020, 3:16:17 AM

System Manufacturer: Xen

System Model: HVM domU

System Type: x64-based PC

Processor(s): 1 Processor(s) Installed.

[01]: Intel64 Family 6 Model 63 Stepping 2 GenuineIntel ~2400 Mhz

BIOS Version: Xen 4.2.amazon, 8/24/2006

Windows Directory: C:\Windows

System Directory: C:\Windows\system32

Boot Device: \Device\HarddiskVolume1

System Locale: en-us;English (United States)

Input Locale: en-us;English (United States)

Time Zone: (UTC-08:00) Pacific Time (US & Canada)

Total Physical Memory: 1,024 MB

Available Physical Memory: 420 MB

Virtual Memory: Max Size: 2,048 MB

Virtual Memory: Available: 1,346 MB

Virtual Memory: In Use: 702 MB

Page File Location(s): C:\pagefile.sys

Domain: WORKGROUP

Logon Server: N/A

Hotfix(s): 3 Hotfix(s) Installed.

[01]: KB3192137

[02]: KB3211320

[03]: KB3213986

Network Card(s): 1 NIC(s) Installed.

[01]: AWS PV Network Device

Connection Name: Ethernet 2

DHCP Enabled: Yes

DHCP Server: 10.10.0.1

IP address(es)

[01]: 10.10.28.8

[02]: fe80::3c5b:c633:c400:bbb5

Hyper-V Requirements: A hypervisor has been detected. Features required for Hyper-V will not be displayed.

c:\windows\system32\inetsrv>

c:\windows\system32\inetsrv>hostname

hostname

Relevant

c:\windows\system32\inetsrv>wmic qfe get Caption,Description,HotFixID,InstallatedOn

wmic qfe get Caption,Description,HotFixID,InstallatedOn

Node - RELEVANT

ERROR:

Description = Invalid query

c:\windows\system32\inetsrv>wmic logicaldisk get caption,description,providername

wmic logicaldisk get caption,description,providername

Caption Description ProviderName

C: Local Fixed Disk

###User Enumeration###

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

c:\windows\system32\inetsrv>

c:\windows\system32\inetsrv>whoami /groups

whoami /groups

GROUP INFORMATION

Group Name Type SID Attributes

================================== ==========
==========
==========

Mandatory Label\High Mandatory Level Label S-1-16-12288

Everyone Well-known group S-1-1-0 Mandatory group, Enabled by default, Enabled group

BUILTIN\Users Alias S-1-5-32-545 Mandatory group, Enabled by default, Enabled group

NT AUTHORITY\SERVICE Well-known group S-1-5-6 Mandatory group, Enabled by default, Enabled group

CONSOLE LOGON Well-known group S-1-2-1 Mandatory group, Enabled by default, Enabled group

NT AUTHORITY\Authenticated Users Well-known group S-1-5-11 Mandatory group, Enabled by default, Enabled group

NT AUTHORITY\This Organization Well-known group S-1-5-15 Mandatory group, Enabled by default, Enabled group

BUILTIN\IIS_IUSRS Alias S-1-5-32-568 Mandatory group, Enabled by default, Enabled group

LOCAL Well-known group S-1-2-0 Mandatory group, Enabled by default, Enabled group

Unknown SID type S-1-5-82-0 Mandatory group, Enabled by default, Enabled group

c:\windows\system32\inetsrv>

c:\windows\system32\inetsrv>net user

net user

User accounts for \\

Administrator Bob DefaultAccount

Guest

The command completed with one or more errors.

c:\windows\system32\inetsrv>net user bob

net user bob

Penetration Test Report - Relevant

User name Bob

Full Name Bob

Comment

User's comment

Country/region code 000 (System Default)

Account active Yes

Account expires Never

Password last set 7/25/2020 1:03:20 PM

Password expires Never

Password changeable 7/25/2020 1:03:20 PM

Password required Yes

User may change password No

Workstations allowed All

Logon script

User profile

Home directory

Last logon Never

Logon hours allowed All

Local Group Memberships *Users

Global Group memberships *None

The command completed successfully.

c:\windows\system32\inetsrv>net localgroup

net localgroup

Aliases for \\RELEVANT

---

*Access Control Assistance Operators

*Administrators

*Backup Operators

*Certificate Service DCOM Access

*Cryptographic Operators

*Distributed COM Users

*Event Log Readers

*Guests

*Hyper-V Administrators

*IIS_IUSRS

*Network Configuration Operators

*Performance Log Users

*Performance Monitor Users

*Power Users

*Print Operators

*RDS Endpoint Servers

*RDS Management Servers

*RDS Remote Access Servers

*Remote Desktop Users

*Remote Management Users

*Replicator

*Storage Replica Administrators

*System Managed Accounts Group

*Users

The command completed successfully.

###Network Enumeration###

ipconfig /all

Windows IP Configuration

Host Name . . . . . : Relevant

Primary Dns Suffix . . . . . :

Node Type . . . . . : Hybrid

IP Routing Enabled. . . . . : No

WINS Proxy Enabled. . . . . : No

DNS Suffix Search List. . . . . : eu-west-1.ec2-utilities.amazonaws.com

eu-west-1.compute.internal

Ethernet adapter Ethernet 2:

Connection-specific DNS Suffix . : eu-west-1.compute.internal

Description . . . . . : AWS PV Network Device #0

Physical Address. . . . . : 02-67-0E-BE-1F-49

DHCP Enabled. . . . . : Yes

Autoconfiguration Enabled . . . . : Yes

Link-local IPv6 Address . . . . . : fe80::3c5b:c633:c400:bbb5%4(Preferred)

IPv4 Address. . . . . : 10.10.28.8(Preferred)

Subnet Mask . . . . . : 255.255.0.0

Lease Obtained. . . . . : Monday, November 23, 2020 3:16:40 AM

Lease Expires . . . . . : Monday, November 23, 2020 4:46:40 AM

Default Gateway . . . . . : 10.10.0.1

DHCP Server . . . . . : 10.10.0.1

DHCPv6 IAID . . . . . : 101073078

DHCPv6 Client DUID. . . . . : 00-01-00-01-26-AE-44-DC-08-00-27-7C-35-30

DNS Servers . . . . . : 10.0.0.2

NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter isatap.eu-west-1.compute.internal:

```
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : eu-west-1.compute.internal
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

Tunnel adapter Local Area Connection* 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Teredo Tunneling Pseudo-Interface
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:0:2851:782c:1cad:3725:f5f5:e3f7(Preferred)
   Link-local IPv6 Address . . . . . : fe80::1cad:3725:f5f5:e3f7%3(Preferred)
   Default Gateway . . . . . . . . . : ::
   DHCPv6 IAID . . . . . . . . . . . : 134217728
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-26-AE-44-DC-08-00-27-7C-35-
30
   NetBIOS over Tcpip. . . . . . . . : Disabled

c:\windows\system32\inetsrv>
```

ac:\windows\system32\inetsrvarp -a

arp -a

Interface: 10.10.28.8 --- 0x4

Internet Address	Physical Address	Type
10.10.0.1	02-c8-85-b5-5a-aa	dynamic
10.10.255.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

c:\windows\system32\inetsrv>

rc:\windows\system32\inetsrv>oute print

route print

==========

Interface List

4...02 67 0e be 1f 49 ......AWS PV Network Device #0

1...........................Software Loopback Interface 1

6...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter

3...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface

==========

IPv4 Route Table

===
===============

Active Routes:

Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	10.10.0.1	10.10.28.8	25
10.10.0.0	255.255.0.0	On-link	10.10.28.8	281
10.10.28.8	255.255.255.255	On-link	10.10.28.8	281
10.10.255.255	255.255.255.255	On-link	10.10.28.8	281
127.0.0.0	255.0.0.0	On-link	127.0.0.1	331
127.0.0.1	255.255.255.255	On-link	127.0.0.1	331
127.255.255.255	255.255.255.255	On-link	127.0.0.1	331
169.254.169.123	255.255.255.255	10.10.0.1	10.10.28.8	50
169.254.169.249	255.255.255.255	10.10.0.1	10.10.28.8	50
169.254.169.250	255.255.255.255	10.10.0.1	10.10.28.8	50
169.254.169.251	255.255.255.255	10.10.0.1	10.10.28.8	50
169.254.169.253	255.255.255.255	10.10.0.1	10.10.28.8	50
169.254.169.254	255.255.255.255	10.10.0.1	10.10.28.8	50
224.0.0.0	240.0.0.0	On-link	127.0.0.1	331
224.0.0.0	240.0.0.0	On-link	10.10.28.8	281
255.255.255.255	255.255.255.255	On-link	127.0.0.1	331
255.255.255.255	255.255.255.255	On-link	10.10.28.8	281

===
===============

Persistent Routes:

Network Address	Netmask	Gateway Address	Metric
169.254.169.254	255.255.255.255	10.10.0.1	25
169.254.169.250	255.255.255.255	10.10.0.1	25
169.254.169.251	255.255.255.255	10.10.0.1	25
169.254.169.249	255.255.255.255	10.10.0.1	25
169.254.169.123	255.255.255.255	10.10.0.1	25
169.254.169.253	255.255.255.255	10.10.0.1	25

==========

IPv6 Route Table

==========

Active Routes:

If	Metric	Network Destination	Gateway
3	331	::/0	On-link
1	331	::1/128	On-link
3	331	2001::/32	On-link
3	331	2001:0:2851:782c:1cad:3725:f5f5:e3f7/128	On-link
4	281	fe80::/64	On-link
3	331	fe80::/64	On-link
3	331	fe80::1cad:3725:f5f5:e3f7/128	On-link

```
  4    281 fe80::3c5b:c633:c400:bbb5/128
                                On-link
  1    331 ff00::/8             On-link
  4    281 ff00::/8             On-link
  3    331 ff00::/8             On-link
===========================================================================
===============
Persistent Routes:
  None


c:\windows\system32\inetsrv>netstat -ano
netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       836
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       1020
  TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49663          0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       608
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       1012
```

```
TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       992
TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       1664
TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       712
TCP    0.0.0.0:49671          0.0.0.0:0              LISTENING       720
TCP    10.10.28.8:139         0.0.0.0:0              LISTENING       4
TCP    10.10.28.8:49937       10.6.0.52:4445         ESTABLISHED     3248
TCP    [::]:80                [::]:0                 LISTENING       4
TCP    [::]:135               [::]:0                 LISTENING       836
TCP    [::]:445               [::]:0                 LISTENING       4
TCP    [::]:3389              [::]:0                 LISTENING       1020
TCP    [::]:5985              [::]:0                 LISTENING       4
TCP    [::]:47001             [::]:0                 LISTENING       4
TCP    [::]:49663             [::]:0                 LISTENING       4
TCP    [::]:49664             [::]:0                 LISTENING       608
TCP    [::]:49665             [::]:0                 LISTENING       1012
TCP    [::]:49666             [::]:0                 LISTENING       992
TCP    [::]:49667             [::]:0                 LISTENING       1664
TCP    [::]:49668             [::]:0                 LISTENING       712
TCP    [::]:49671             [::]:0                 LISTENING       720
UDP    0.0.0.0:123            *:*                                    1052
UDP    0.0.0.0:3389           *:*                                    1020
UDP    0.0.0.0:5050           *:*                                    1052
UDP    0.0.0.0:5353           *:*                                    1136
UDP    0.0.0.0:5355           *:*                                    1136
```

```
  UDP    10.10.28.8:137         *:*                    4
  UDP    10.10.28.8:138         *:*                    4
  UDP    10.10.28.8:1900        *:*                    3064
  UDP    10.10.28.8:56056       *:*                    3064
  UDP    127.0.0.1:1900         *:*                    3064
  UDP    127.0.0.1:56057        *:*                    3064
  UDP    [::]:123               *:*                    1052
  UDP    [::]:3389              *:*                    1020
  UDP    [::]:5353              *:*                    1136
  UDP    [::]:5355              *:*                    1136
  UDP    [::1]:1900             *:*                    3064
  UDP    [::1]:56055            *:*                    3064
  UDP    [fe80::3c5b:c633:c400:bbb5%4]:1900  *:*                    3064
  UDP    [fe80::3c5b:c633:c400:bbb5%4]:56054  *:*                    3064
```

###Password Hunting###

Within://10.10.129.133/nt4wrksv

stored within a text file named passwords.txt

Qm9iIC0gIVBAJCRXMHJEITEyMw==

QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk

###A/V and Firewall Enumeration###

c:\windows\system32\inetsrv>sc query windefend

sc query windefend

SERVICE_NAME: windefend

TYPE : 10 WIN32_OWN_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

c:\windows\system32\inetsrv>

c:\windows\system32\inetsrv>sc queryex type= service

sc queryex type= service

SERVICE_NAME: AmazonSSMAgent

DISPLAY_NAME: Amazon SSM Agent

TYPE : 10 WIN32_OWN_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 2512

FLAGS :

SERVICE_NAME: AppHostSvc

DISPLAY_NAME: Application Host Helper Service

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 1696

FLAGS :

SERVICE_NAME: AWSLiteAgent

Penetration Test Report - Relevant

DISPLAY_NAME: AWS Lite Guest Agent

TYPE : 10 WIN32_OWN_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 1780

FLAGS :

SERVICE_NAME: BFE

DISPLAY_NAME: Base Filtering Engine

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 552

FLAGS :

Penetration Test Report - Relevant

SERVICE_NAME: BrokerInfrastructure

DISPLAY_NAME: Background Tasks Infrastructure Service

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 792

FLAGS :

SERVICE_NAME: CertPropSvc

DISPLAY_NAME: Certificate Propagation

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 980

FLAGS :

SERVICE_NAME: ClipSVC

DISPLAY_NAME: Client License Service (ClipSVC)

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 2480

FLAGS :

SERVICE_NAME: CoreMessagingRegistrar

DISPLAY_NAME: CoreMessaging

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 552

FLAGS :

SERVICE_NAME: CryptSvc

DISPLAY_NAME: Cryptographic Services

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 1140

FLAGS :

SERVICE_NAME: DcomLaunch

DISPLAY_NAME: DCOM Server Process Launcher

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 792

FLAGS :

SERVICE_NAME: Dhcp

DISPLAY_NAME: DHCP Client

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 1012

FLAGS :

SERVICE_NAME: DiagTrack

DISPLAY_NAME: Connected User Experiences and Telemetry

TYPE : 10 WIN32_OWN_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, ACCEPTS_PRESHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 1728

FLAGS :

SERVICE_NAME: Dnscache

DISPLAY_NAME: DNS Client

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 1140

FLAGS :

SERVICE_NAME: DPS

DISPLAY_NAME: Diagnostic Policy Service

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 552

FLAGS :

SERVICE_NAME: DsmSvc

DISPLAY_NAME: Device Setup Manager

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 980

FLAGS :

SERVICE_NAME: EventLog

DISPLAY_NAME: Windows Event Log

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 1012

FLAGS :

SERVICE_NAME: EventSystem

DISPLAY_NAME: COM+ Event System

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 1052

FLAGS :

SERVICE_NAME: FontCache

DISPLAY_NAME: Windows Font Cache Service

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 1052

FLAGS :

SERVICE_NAME: gpsvc

DISPLAY_NAME: Group Policy Client

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, ACCEPTS_PRESHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 980

FLAGS :

SERVICE_NAME: IISADMIN

DISPLAY_NAME: IIS Admin Service

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE,
ACCEPTS_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 1764

FLAGS :

SERVICE_NAME: iphlpsvc

DISPLAY_NAME: IP Helper

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE,
IGNORES_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 980

FLAGS :

SERVICE_NAME: KeyIso

DISPLAY_NAME: CNG Key Isolation

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 720

FLAGS : RUNS_IN_SYSTEM_PROCESS

SERVICE_NAME: LanmanServer

DISPLAY_NAME: Server

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 1788

FLAGS :

SERVICE_NAME: LanmanWorkstation

DISPLAY_NAME: Workstation

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, PAUSABLE, IGNORES_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 1140

FLAGS :

SERVICE_NAME: LicenseManager

DISPLAY_NAME: Windows License Manager Service

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 1052

FLAGS :

SERVICE_NAME: lmhosts

DISPLAY_NAME: TCP/IP NetBIOS Helper

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 1012

FLAGS :

SERVICE_NAME: LSM

DISPLAY_NAME: Local Session Manager

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 792

FLAGS :

SERVICE_NAME: MpsSvc

DISPLAY_NAME: Windows Firewall

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 552

FLAGS :

SERVICE_NAME: MSDTC

DISPLAY_NAME: Distributed Transaction Coordinator

TYPE : 10 WIN32_OWN_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 1976

FLAGS :

SERVICE_NAME: NcbService

DISPLAY_NAME: Network Connection Broker

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 480

FLAGS :

SERVICE_NAME: netprofm

DISPLAY_NAME: Network List Service

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 1052

FLAGS :

SERVICE_NAME: NlaSvc

DISPLAY_NAME: Network Location Awareness

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 1140

FLAGS :

SERVICE_NAME: nsi

DISPLAY_NAME: Network Store Interface Service

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 1052

FLAGS :

SERVICE_NAME: PcaSvc

DISPLAY_NAME: Program Compatibility Assistant Service

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 480

FLAGS :

SERVICE_NAME: PlugPlay

DISPLAY_NAME: Plug and Play

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 792

FLAGS :

SERVICE_NAME: PolicyAgent

DISPLAY_NAME: IPsec Policy Agent

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 2216

FLAGS :

SERVICE_NAME: Power

DISPLAY_NAME: Power

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 792

FLAGS :

SERVICE_NAME: ProfSvc

DISPLAY_NAME: User Profile Service

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 980

FLAGS :

SERVICE_NAME: RemoteRegistry

DISPLAY_NAME: Remote Registry

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 1052

FLAGS :

SERVICE_NAME: RpcEptMapper

DISPLAY_NAME: RPC Endpoint Mapper

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 828

FLAGS :

SERVICE_NAME: RpcSs

DISPLAY_NAME: Remote Procedure Call (RPC)

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 828

FLAGS :

SERVICE_NAME: SamSs

DISPLAY_NAME: Security Accounts Manager

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 720

FLAGS : RUNS_IN_SYSTEM_PROCESS

SERVICE_NAME: Schedule

DISPLAY_NAME: Task Scheduler

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 980

FLAGS :

SERVICE_NAME: SENS

DISPLAY_NAME: System Event Notification Service

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 980

FLAGS :

SERVICE_NAME: SessionEnv

DISPLAY_NAME: Remote Desktop Configuration

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 980

FLAGS :

SERVICE_NAME: ShellHWDetection

DISPLAY_NAME: Shell Hardware Detection

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 980

FLAGS :

SERVICE_NAME: Spooler

DISPLAY_NAME: Print Spooler

TYPE : 110 WIN32_OWN_PROCESS (interactive)

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 1680

FLAGS :

SERVICE_NAME: sppsvc

DISPLAY_NAME: Software Protection

TYPE : 10 WIN32_OWN_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 1164

FLAGS :

SERVICE_NAME: StateRepository

DISPLAY_NAME: State Repository Service

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 1848

FLAGS :

SERVICE_NAME: SystemEventsBroker

DISPLAY_NAME: System Events Broker

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 792

FLAGS :

SERVICE_NAME: TermService

DISPLAY_NAME: Remote Desktop Services

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 988

FLAGS :

SERVICE_NAME: Themes

DISPLAY_NAME: Themes

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 980

FLAGS :

SERVICE_NAME: tiledatamodelsvc

DISPLAY_NAME: Tile Data model server

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, ACCEPTS_PRESHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 1848

FLAGS :

SERVICE_NAME: TimeBrokerSvc

DISPLAY_NAME: Time Broker

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 1012

FLAGS :

SERVICE_NAME: TrkWks

DISPLAY_NAME: Distributed Link Tracking Client

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 480

FLAGS :

SERVICE_NAME: UALSVC

DISPLAY_NAME: User Access Logging Service

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, ACCEPTS_PRESHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 480

FLAGS :

SERVICE_NAME: UmRdpService

DISPLAY_NAME: Remote Desktop Services UserMode Port Redirector

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 480

FLAGS :

SERVICE_NAME: UserManager

DISPLAY_NAME: User Manager

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

```
        PID                : 980
        FLAGS              :

SERVICE_NAME: UsoSvc
DISPLAY_NAME: Update Orchestrator Service for Windows Update
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 4  RUNNING
                             (STOPPABLE, NOT_PAUSABLE,
IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
        PID                : 980
        FLAGS              :

SERVICE_NAME: vds
DISPLAY_NAME: Virtual Disk
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                             (STOPPABLE, NOT_PAUSABLE,
IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
```

WAIT_HINT : 0x0

PID : 2952

FLAGS :

SERVICE_NAME: W32Time

DISPLAY_NAME: Windows Time

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 1052

FLAGS :

SERVICE_NAME: W3SVC

DISPLAY_NAME: World Wide Web Publishing Service

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 1916

FLAGS :

SERVICE_NAME: WAS

DISPLAY_NAME: Windows Process Activation Service

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 1916

FLAGS :

SERVICE_NAME: Wcmsvc

DISPLAY_NAME: Windows Connection Manager

TYPE : 10 WIN32_OWN_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 1376

FLAGS :

SERVICE_NAME: WinDefend

DISPLAY_NAME: Windows Defender Service

TYPE : 10 WIN32_OWN_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 1956

FLAGS :

SERVICE_NAME: WinHttpAutoProxySvc

DISPLAY_NAME: WinHTTP Web Proxy Auto-Discovery Service

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 1052

FLAGS :

SERVICE_NAME: Winmgmt

DISPLAY_NAME: Windows Management Instrumentation

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 980

FLAGS :

SERVICE_NAME: WinRM

DISPLAY_NAME: Windows Remote Management (WS-Management)

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 1140

FLAGS :

SERVICE_NAME: wlidsvc

DISPLAY_NAME: Microsoft Account Sign-in Assistant

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 980

FLAGS :

SERVICE_NAME: WLMS

DISPLAY_NAME: Windows Licensing Monitoring Service

TYPE : 10 WIN32_OWN_PROCESS

STATE : 4 RUNNING

(NOT_STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 1940

FLAGS :

SERVICE_NAME: WpnService

DISPLAY_NAME: Windows Push Notifications System Service

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 980

FLAGS :

SERVICE_NAME: wuauserv

DISPLAY_NAME: Windows Update

TYPE : 20 WIN32_SHARE_PROCESS

STATE : 4 RUNNING

(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)

WIN32_EXIT_CODE : 0 (0x0)

SERVICE_EXIT_CODE : 0 (0x0)

CHECKPOINT : 0x0

WAIT_HINT : 0x0

PID : 980

FLAGS :

c:\windows\system32\inetsrv>netsh advfirewall firewall dump

netsh advfirewall firewall dump

c:\windows\system32\inetsrv>netsh firewall show state

netsh firewall show state

Firewall status:

Profile = Standard

Operational mode = Enable

Exception mode = Enable

Multicast/broadcast response mode = Enable

Notification mode = Disable

Group policy version = Windows Firewall

Remote admin mode = Disable

Ports currently open on all network interfaces:

Port Protocol Version Program

49663 TCP Any (null)

IMPORTANT: Command executed successfully.

However, "netsh firewall" is deprecated;

use "netsh advfirewall firewall" instead.

For more information on using "netsh advfirewall firewall" commands

instead of "netsh firewall", see KB article 947709

at http://go.microsoft.com/fwlink/?linkid=121488 .

c:\windows\system32\inetsrv>netsh firewall show config

netsh firewall show config

Domain profile configuration:

Operational mode = Enable

Exception mode = Enable

Multicast/broadcast response mode = Enable

Notification mode = Disable

Service configuration for Domain profile:

Mode Customized Name

Enable No Remote Desktop

Allowed programs configuration for Domain profile:

Mode Traffic direction Name / Program

Port configuration for Domain profile:

Port Protocol Mode Traffic direction Name

49663 TCP Enable Inbound 49663 Inbound

ICMP configuration for Domain profile:

Mode Type Description

Enable 2 Allow outbound packet too big

Standard profile configuration (current):

Operational mode = Enable

Exception mode = Enable

Multicast/broadcast response mode = Enable

Notification mode = Disable

Service configuration for Standard profile:

Mode Customized Name

Enable No File and Printer Sharing

Enable Yes Network Discovery

Enable No Remote Desktop

Allowed programs configuration for Standard profile:

Mode Traffic direction Name / Program

Port configuration for Standard profile:

Port Protocol Mode Traffic direction Name

49663 TCP Enable Inbound 49663 Inbound

ICMP configuration for Standard profile:

Mode Type Description

Enable 2 Allow outbound packet too big

Enable 8 Allow inbound echo request

Log configuration:

File location = C:\Windows\system32\LogFiles\Firewall\pfirewall.log

Max file size = 4096 KB

Dropped packets = Disable

Connections = Disable

IMPORTANT: Command executed successfully.

However, "netsh firewall" is deprecated;

use "netsh advfirewall firewall" instead.

For more information on using "netsh advfirewall firewall" commands

instead of "netsh firewall", see KB article 947709

at http://go.microsoft.com/fwlink/?linkid=121488 .