

Investigating windows

October 18, 2024 11:21 PM

- Task 1: Investigating windows

This is a challenge that is exactly what is says on the tin, there are a few challenges around investigating a windows machine that has been previously compromised.

Connect to the machine using RDP. The credentials the machine are as follows:

-

Username: Administrator

Password: letmein123!

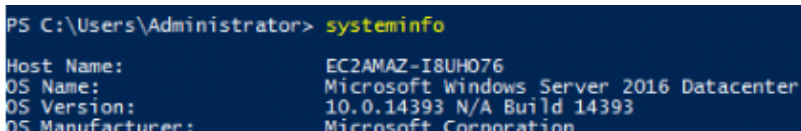
Please note that this machine does not respond to ping (ICMP) and may take a few minutes to boot up.

-

Whats the version and year of the windows machine?

- In PowerShell, run the following command

- systeminfo

- The screenshot shows the output of the 'systeminfo' command in a PowerShell terminal. The output is as follows:
PS C:\Users\Administrator> systeminfo
Host Name: EC2AMAZ-I8UH076
OS Name: Microsoft Windows Server 2016 Datacenter
OS Version: 10.0.14393 N/A Build 14393
OS Manufacturer: Microsoft Corporation

Whats the version and year of the windows machine?

-

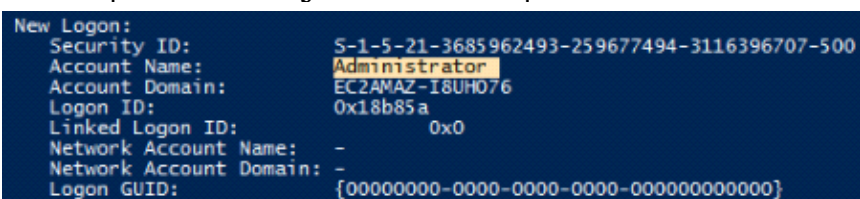
Windows Server 2016

-

Which user logged in last?

- In PowerShell, run the following command:

- Get-EventLog -LogName Security -InstanceId 4624 | Select-Object -First 1 | Format-List

- The screenshot shows the output of the 'Get-EventLog -LogName Security -InstanceId 4624 | Select-Object -First 1 | Format-List' command in a PowerShell terminal. The output is as follows:
New Logon:
Security ID: S-1-5-21-3685962493-259677494-3116396707-500
Account Name: Administrator
Account Domain: EC2AMAZ-I8UH076
Logon ID: 0x18b85a
Linked Logon ID: 0x0
Network Account Name: -
Network Account Domain: -
Logon GUID: {00000000-0000-0000-0000-000000000000}

Which user logged in last?

-

Administrator

When did John log onto the system last?

-

Answer format: MM/DD/YYYY H:MM:SS AM/PM

- In PowerShell, run the following command:

□ Net user logon

```
PS C:\Users\Administrator> net user John
User name                John
Full Name                John
Comment
User's comment
Country/region code      000 (System Default)
Account active            Yes
Account expires           Never

Password last set         3/2/2019 5:48:19 PM
Password expires          Never
Password changeable       3/2/2019 5:48:19 PM
Password required          Yes
User may change password  Yes

Workstations allowed      All
Logon script
User profile
Home directory
Last logon                3/2/2019 5:48:32 PM

Logon hours allowed       All

Local Group Memberships   *Users
Global Group memberships  *None
The command completed successfully.
```

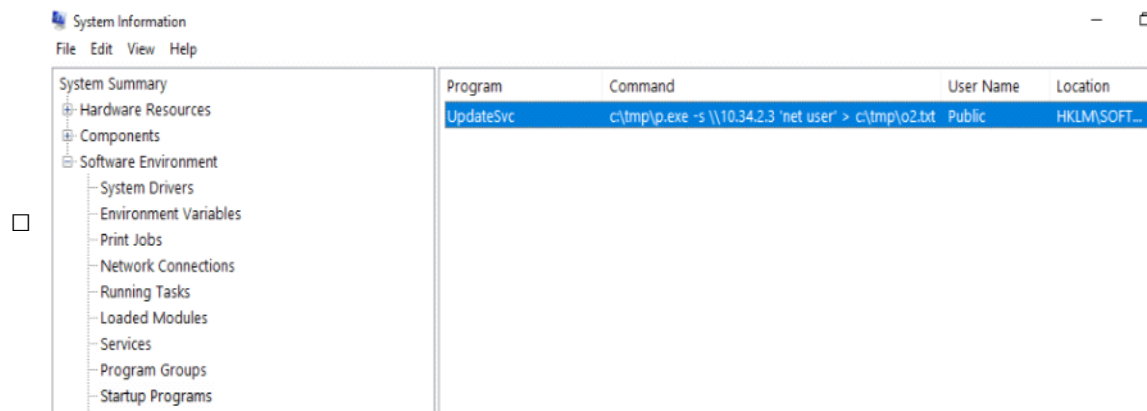
When did John log onto the system last?

■ Answer format: MM/DD/YYYY H:MM:SS AM/PM

03/02/2019 5:48:32 PM

○ What IP does the system connect to when it first starts?

- In PowerShell, I ran the following commands but couldn't find the answer.
 - Get-DnsClientServerAddress
 - ipconfig | findstr /i "Gateway"
- I can use System Information > Software Environment > Startup Programs and find the IP address that this system connects to at startup.



What IP does the system connect to when it first starts?

10.34.2.3

What two accounts had administrative privileges (other than the Administrator user)?

○

Answer format: username1, username2

- Run the following command in PowerShell:

- Net localgroup Administrators

```
PS C:\Users\Administrator> net localgroup Administrators
Alias name     Administrators
Comment       Administrators have complete and unrestricted access to the computer/domain
Members
-----
Administrator
Guest
Jenny
The command completed successfully.
```

What two accounts had administrative privileges (other than the Administrator user)?

Answer format: username1, username2

▪

Jenny, Guest

○

Whats the name of the scheduled task that is malicious.

- Run the following command in PowerShell

- Get-ScheduledTask

```
PS C:\Users\Administrator> Get-ScheduledTask

TaskPath          TaskName          State
-----
Microsoft\Windows\Amazon Ec2 Launch - Instance I... Disabled
Microsoft\Windows\check logged in                  Ready
Microsoft\Windows\Clean file system                 Ready
Microsoft\Windows\falshupdate22                    Ready
Microsoft\Windows\GameOver                          Ready
Microsoft\Windows\update windows                   Ready
Microsoft\Windows\.NET Framework\NGEN v4.0.30319   Ready
```

- Only a hacker with the intention to remove any trace would want to clean the file system.

Whats the name of the scheduled task that is malicious.

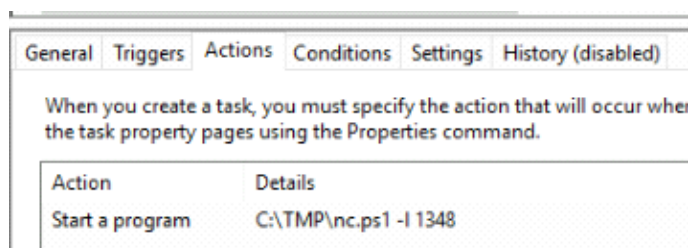
▪

Clean file system

○

What file was the task trying to run daily?

- I opened Task Scheduler. Then I looked at the Active Tasks pane and opened "Clean File System" to see its details. Under the Actions tab, I could see what file is scheduled to run.



What file was the task trying to run daily?

-

○ What port did this file listen locally for?

- The port info is in the same screenshot.

Action	Details
Start a program	C:\TMP\nc.ps1 -l 1348

○ When did Jenny last logon?

- Run the following command in PowerShell.

□ Net user Jenny

```
PS C:\Users\Administrator> net user Jenny
User name                Jenny
Full Name                Jenny
Comment
User's comment
Country/region code      000 (System Default)
Account active           Yes
Account expires          Never
Password last set        3/2/2019 4:52:25 PM
Password expires         Never
Password changeable      3/2/2019 4:52:25 PM
Password required        Yes
User may change password Yes
Workstations allowed     All
Logon script
User profile
Home directory
Last logon               Never
Logon hours allowed      All
Local Group Memberships  *Administrators
Global Group memberships *None
The command completed successfully.
```

- Safe to assume that Jenny is a user created by the Attacker with Administrative privilege and never had to be signed in later.

When did Jenny last logon?

-

At what date did the compromise take place?

- Answer format: MM/DD/YYYY
- File system:

□

This PC > Local Disk (C:)		
Name		Date modified
PerfLogs		2/23/2018 11:06 AM
Users		3/2/2019 4:09 PM
inetpub		3/2/2019 4:41 PM
Windows		3/2/2019 4:46 PM
TMP		3/2/2019 4:55 PM
Program Files		1/29/2021 11:46 AM
Program Files (x86)		1/29/2021 11:46 AM

■ Task Scheduler:

□

Name	Created
check logged in	3/2/2019 4:59:49 PM
update windows	3/2/2019 4:59:18 PM
Clean file system	3/2/2019 4:56:16 PM
falshupdate22	3/2/2019 4:50:04 PM
GameOver	3/2/2019 4:47:13 PM

■ Jenny's account information:

□

```

PS C:\Users\Administrator> net user Jenny
User name                Jenny
Full Name                Jenny
Comment
User's comment
Country/region code      000 (System Default)
Account active           Yes
Account expires          Never
Password last set        3/2/2019 4:52:25 PM
Password expires         Never
Password changeable      3/2/2019 4:52:25 PM
Password required        Yes
User may change password Yes
Workstations allowed     All
Logon script
User profile
Home directory
Last logon               Never
Logon hours allowed      All
Local Group Memberships  *Administrators
Global Group memberships *None
The command completed successfully.

```

- I checked the file system, task scheduler and Jenny's account information. I noticed one date that stood out. The attacker made changes in the file system, created scheduled tasks and created account Jenny on the same date.

At what date did the compromise take place?

- Answer format: MM/DD/YYYY

03/02/2019

During the compromise, at what time did Windows first assign special privileges to a new logon?

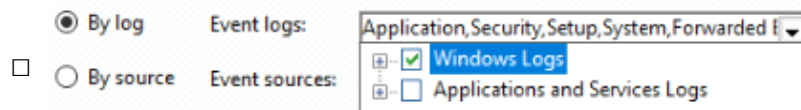
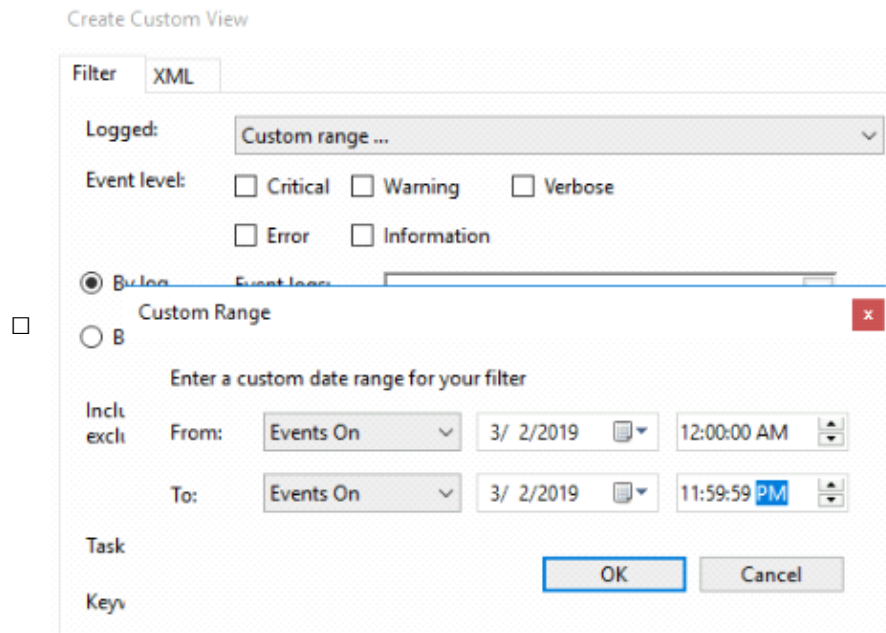
○

Answer format: MM/DD/YYYY HH:MM:SS AM/PM

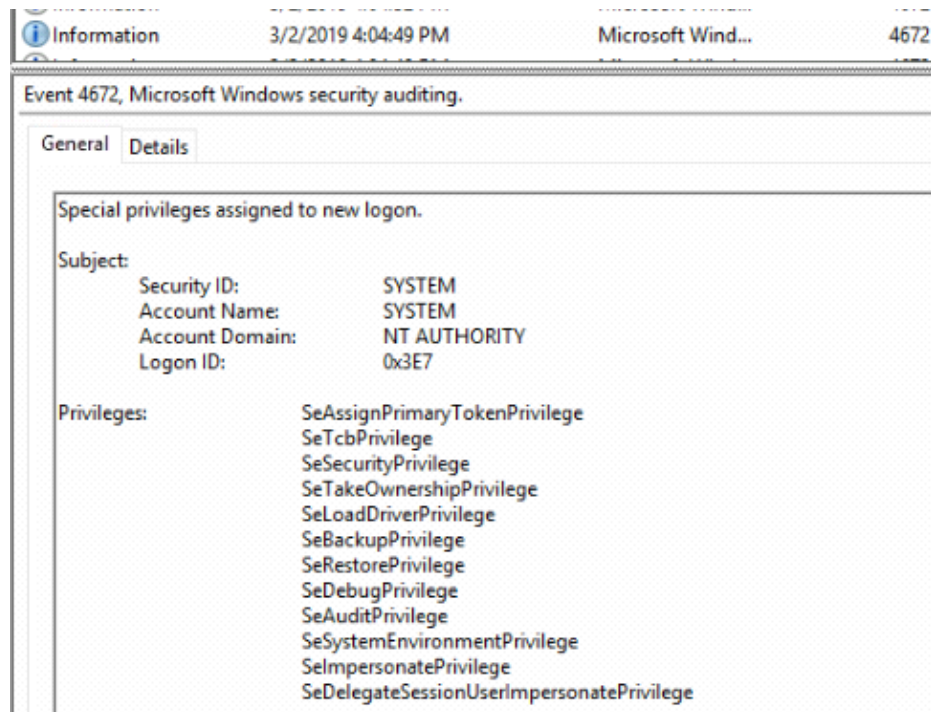
Question Hint

00/00/0000 0:00:49 PM

- I used Event Viewer to create a custom log that provides logs for the date when the system was compromised. I also selected to view only Windows Logs.



- Event ID 4672 corresponds to assigning special privileges at net logon. The question also hinted the second of this event is :49. Therefore, it was easy to figure out the event that first assigned special privileges to a new logon.



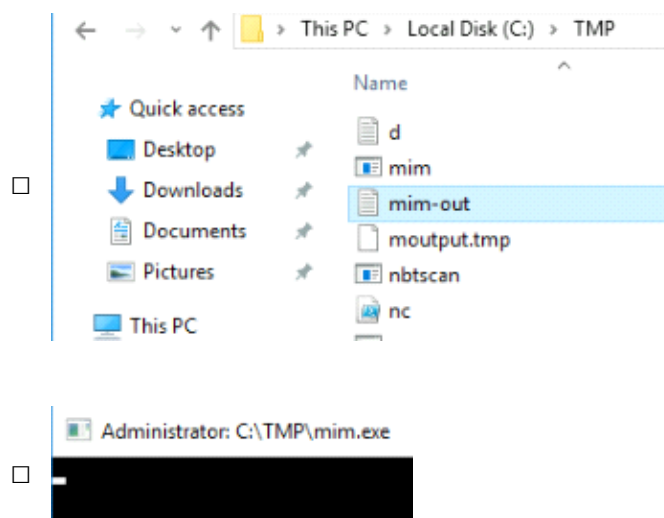
During the compromise, at what time did Windows first assign special privileges to a new logon?

Answer format: MM/DD/YYYY HH:MM:SS AM/PM

03/02/2019 4:04:49 PM

What tool was used to get Windows passwords?

- In the TMP folder inside Local Disk C, there is an application mim which gets triggered and pops on the window at a fixed frequency. Right underneath this file, another file called mim-out is visible. Opening the file gives out the tool that was used to extract passwords for this Windows machine.



```
mim-out - Notepad
File Edit Format View Help

.#####. mimikatz 2.0 alpha (x86) release "Kiwi en C" (Feb 16 2015 22:17:52)
.## ^ ##.
## / \ ## /* * *
## \ / ## Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
'## v #' http://blog.gentilkiwi.com/mimikatz (oe.eo)
'#####' with 15 modules * * */

mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 195072 (00000000:0002fa00)
Session           : Interactive from 1
User Name         : Ion
Domain            : Ion-PC
SID               : S-1-5-21-2367887663-2567669145-1589166190-1000
msv :
```

What tool was used to get Windows passwords?

-

○ What was the attackers external control and command servers IP?

- I needed to view the host file in this machine, located at C:\Windows\System32\drivers\etc\hosts

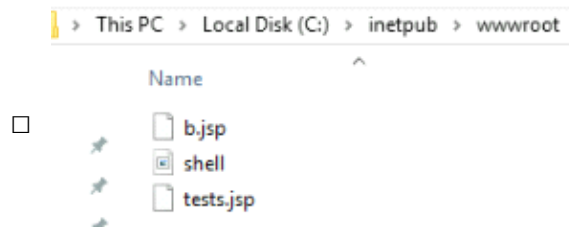
```
# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1            localhost
10.2.2.2       update.microsoft.com
127.0.0.1 www.virustotal.com
127.0.0.1 www.www.com
127.0.0.1 dci.sophosupd.com
10.2.2.2       update.microsoft.com
127.0.0.1 www.virustotal.com
127.0.0.1 www.www.com
127.0.0.1 dci.sophosupd.com
10.2.2.2       update.microsoft.com
127.0.0.1 www.virustotal.com
127.0.0.1 www.www.com
127.0.0.1 dci.sophosupd.com
76.32.97.132 google.com
76.32.97.132 www.google.com
```

What was the attackers external control and command servers IP?

-

○ What was the extension name of the shell uploaded via the servers website?

- The inetpub folder in Windows is the default directory used by Windows IIS. I discovered the following files after going to this location C:\inetpub\wwwroot.



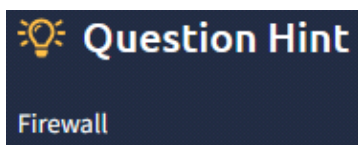
- The attacker used this location to store the shell in .jsp extension.

What was the extension name of the shell uploaded via the servers website?

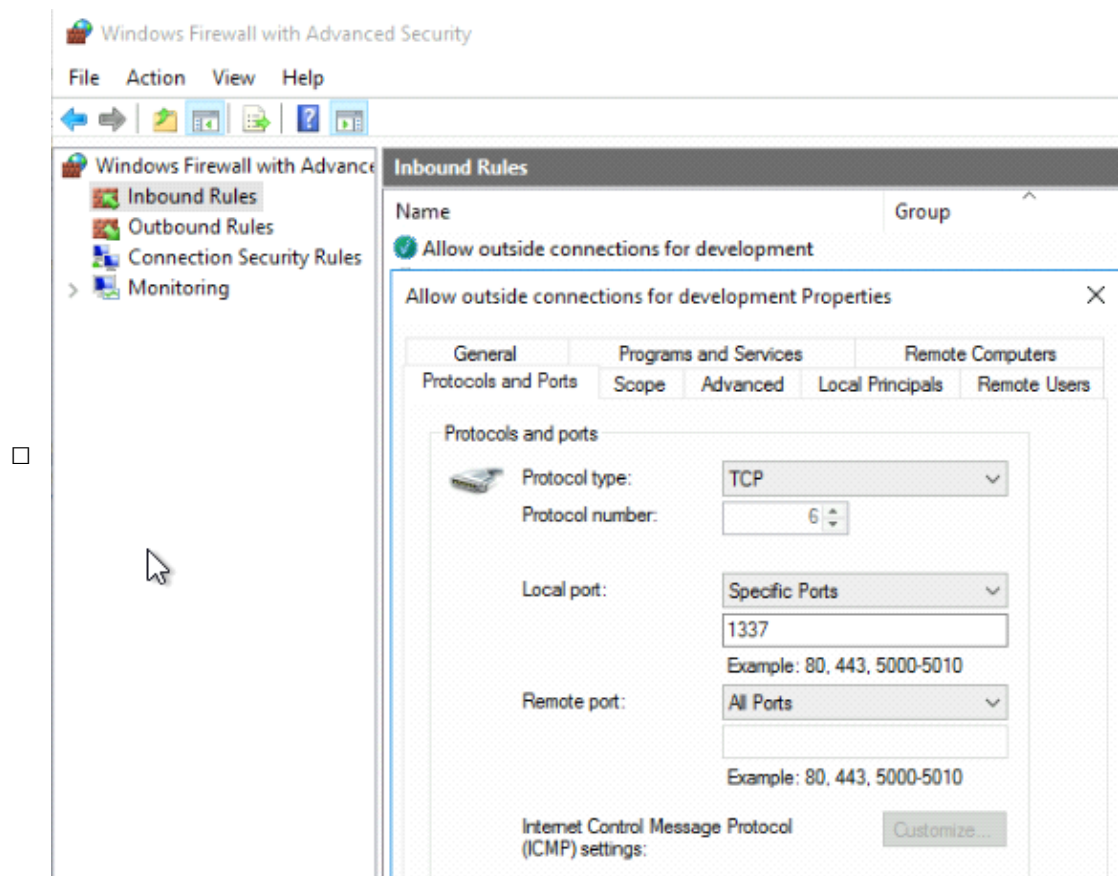
-

.jsp

- What was the last port the attacker opened?



- Checking the inbound firewall rules, the attacker left port 1337 open to allow all outside connections and named the rule "Allow outside connections for development".



What was the last port the attacker opened?

-

○ Check for DNS poisoning, what site was targeted?

- Checking at the host file again, the DNS poisoned site can be found.

□

```
# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
10.2.2.2       update.microsoft.com
127.0.0.1     www.virustotal.com
127.0.0.1     www.www.com
127.0.0.1     dci.sophosupd.com
10.2.2.2       update.microsoft.com
127.0.0.1     www.virustotal.com
127.0.0.1     www.www.com
127.0.0.1     dci.sophosupd.com
10.2.2.2       update.microsoft.com
127.0.0.1     www.virustotal.com
127.0.0.1     www.www.com
127.0.0.1     dci.sophosupd.com
76.32.97.132  google.com
76.32.97.132  www.google.com
```

Check for DNS poisoning, what site was targeted?

-