

INVESTIGATING WINDOWS- TRY HACK ME- ROOM



5kullk3r

7 min read

Nov 9, 2025

The screenshot shows the TryHackMe interface. At the top, there's a navigation bar with icons for Dashboard, Learn, Practice, and Compete. Below that, a breadcrumb navigation shows 'Learn > Investigating Windows'. The main title 'Investigating Windows' is displayed with a blue Windows logo icon to its left. A description below the title reads: 'A windows machine has been hacked, its your job to go investigate this windows machine and find clu...'. It includes a timer icon indicating '45 min', a user count of '1,28,096', and two small circular icons. At the bottom of the screen, there are four buttons: 'Share your achievement' (highlighted in green), 'Start Kali Linux', 'Save Room', and '2727 Recommend'. A progress bar at the very bottom indicates 'Room completed (100%)'.

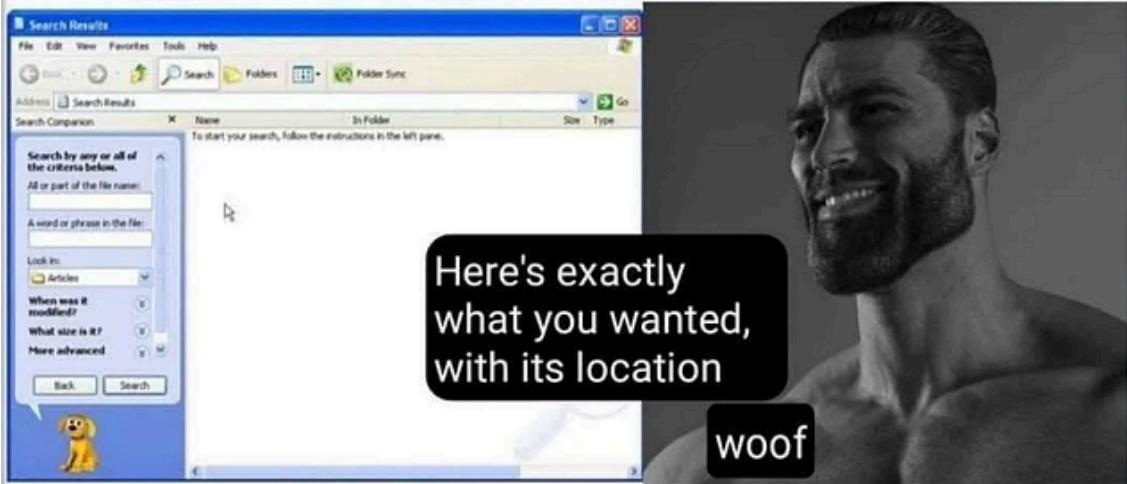
Hello everyone! This is a beginner-friendly somewhat forensic type room from the TryHackMe platform titled “**Investigating Windows**”

This room is classified as easy and is a Ctf-type challenge. I hope this write-up helps guide you through the process!

My goal is to help you understand each step and provide clear explanations so that anyone, whether a beginner or experienced, can follow along and understand the reasoning behind each action. I hope this write-up makes the process smoother and easier to grasp.

Enough talk — let’s dive right in, and I hope you enjoy the journey! :)

Old windows search bar



New windows search bar



Not a huge windows user now, but childhood Nostalgia hits different seeing this

Phase 1: Setup and Initial Access (RDP)

Establishing RDP Connection

To begin the investigation, we first need to establish a **Remote Desktop Protocol (RDP)** connection to the target Windows machine.

We start by ensuring our attacking machine is set up correctly for RDP by installing and starting the `xrdp` service.

sudo apt update && upgrade

sudo apt install xrdp -y

update-rc.d xrdp enable

service xrdp start

If you encounter an error, check if the default RDP port (3389) is already in use, kill the process, and restart the service:

```
└# sudo systemctl status xrdp open a new terminal ⇒ peass ⇒ cd /usr/share/peass/linpeas ⇒ python3 -m http.server  
* xrdp.service - xrdp daemon  
  Loaded: loaded (/usr/lib/systemd/system/xrdp.service; enabled; preset: disabled)  
  Active: failed (Result: exit-code) since Sun 2025-10-05 22:03:56 IST; 1min 6s ago  
  Invocation: 8b578a4040f74a998c5f4b162f0b1e6a  
    Docs: man:xrdp(8)  
     man:xrdp.ini(5)  
   Process: 39158 ExecStartPre=/bin/sh /usr/share/xrdp/socksetup (code=exited, status=0/SUCCESS) → trying udp port  
   Process: 39167 ExecStart=/usr/sbin/xrdp $XRDP_OPTIONS (code=exited, status=1/FAILURE)  
 Mem peak: 2.9M  
 CPU: 12ms  
 ikeexpressway.htb → → sudo ike-scan -A 10.10.11.87 --ids=ikeexpressway.htb -P ike.psk → psk-crack -d /home/ka  
Oct 05 22:03:56 kali systemd[1]: Starting xrdp.service - xrdp daemon ...  
Oct 05 22:03:56 kali xrdp[39167]: [INFO ] address [0.0.0.0] port [3389] mode 1  
Oct 05 22:03:56 kali xrdp[39167]: [INFO ] listening to port 3389 on 0.0.0.0  
Oct 05 22:03:56 kali xrdp[39167]: [ERROR] g_tcp_bind(7, 3389) failed bind IPv6 (errno=98) and IPv4 (errno=22).  
Oct 05 22:03:56 kali xrdp[39167]: [ERROR] trans_listen_address failed  
Oct 05 22:03:56 kali xrdp[39167]: [CORE] Failed to start xrdp daemon, possibly address already in use.  
Oct 05 22:03:56 kali systemd[1]: xrdp.service: Control process exited, code=exited, status=1/FAILURE  
Oct 05 22:03:56 kali systemd[1]: xrdp.service: Failed with result 'exit-code'.  
Oct 05 22:03:56 kali systemd[1]: Failed to start xrdp.service - xrdp daemon.
```

```
└# sudo lsof -i :3389
```

COMMAND	PID	USER	FD	TYPE	DEVICE	SIZE/OFF	NODE	NAME
xrdp	21085	root	11u	IPv6	80355	0t0	TCP	*:ms-wbt-server (LISTEN)

sudo lsof -i :3389

sudo kill <PID> (#use your PID accordingly)

sudo systemctl start xrdp

sudo systemctl status xrdp

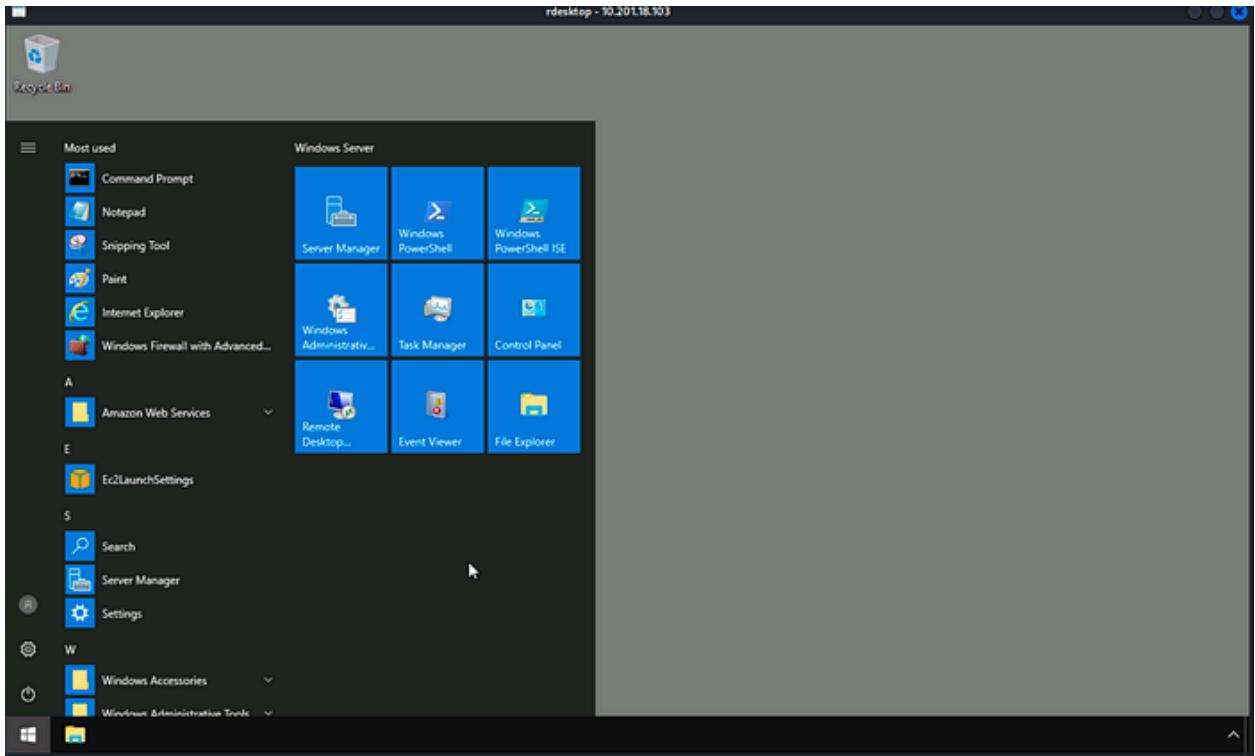
```
└# sudo systemctl status xrdp
● xrdp.service - xrdp daemon
   Loaded: loaded (/usr/lib/systemd/system/xrdp.service; enabled; preset: disabled)
   Active: active (running) since Sun 2025-10-05 22:06:29 IST; 36s ago
     Invocation: 9d4df2c5e2214e01b2d37465cb239fb8
       Docs: man:xrdp(8)
              man:xrdp.ini(5)
    Process: 40567 ExecStartPre=/bin/sh /usr/share/xrdp/socksetup (code=exited, status=0/SUCCESS)
    Process: 40576 ExecStart=/usr/sbin/xrdp $XRDP_OPTIONS (code=exited, status=0/SUCCESS)
      Main PID: 40579 (xrdp)
         Tasks: 1 (limit: 4495)
        Memory: 1.1M (peak: 2.8M)
          CPU: 12ms
         CGroup: /system.slice/xrdp.service
                   └─40579 /usr/sbin/xrdp
```

Once the service is verified as running, we use `rdesktop` to connect to the target IP as the **Administrator** user, using the credentials provided by the room (which were known for initial access):

```
└# rdesktop -u Administrator -p 'letmein123!' 10.201.18.103
ATTENTION! The server uses an invalid security certificate which can not be trusted for the following identified reason(s);
1. Certificate issuer is not trusted by this system.
```

`rdesktop -u Administrator -p 'letmein123!' 10.201.84.31`

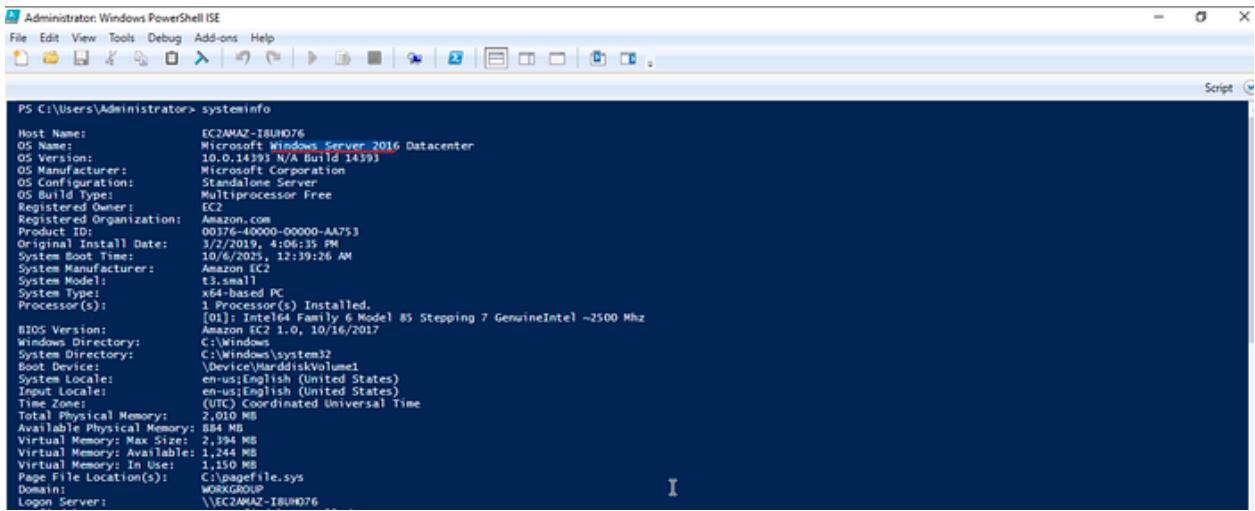
and we get to see it in our screen



Phase 2: System Reconnaissance and User Analysis

Initial System Information Gathering

Upon gaining RDP access, we head to **PowerShell** to gather initial system information, specifically to find the version of Windows running.



```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Script

PS C:\Users\Administrator> systeminfo
Host Name: EC2AMAZ-IBUH076
OS Name: Microsoft Windows Server 2016 Datacenter
OS Version: 10.0.14393 N/A Build 14393
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Server
OS Build Type: Multiprocessor Free
Registered Owner: EC2AMAZ-IBUH076
Registered Organization: Amazon.com
Product ID: 00176-40000-00000-AAZ53
Original Install Date: 3/2/2019, 4:06:35 PM
System Boot Time: 10/6/2025, 12:39:26 AM
System Manufacturer: Amazon EC2
System Model: t3.small
System Type: x64-based PC
Processor(s):
  1 Processor(s) Installed.
    (Model: Intel(R) Core(TM) i5-6500 CPU @ 3.20GHz)
    (L1 Cache: 32 MB, L2 Cache: 6 MB, L3 Cache: 6 MB)
    (Clock Speed: ~2500 MHz)
BIOS Version: Amazon EC2 1.0, 10/16/2017
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) Coordinated Universal Time
Total Physical Memory: 2,010 MB
Available Physical Memory: 884 MB
Virtual Memory: Max Size: 2,394 MB
Virtual Memory: Available: 1,244 MB
Virtual Memory: In Use: 1,150 MB
Page File Location(s): C:\pagefile.sys
Domain: WORKGROUP
Logon Server: \\EC2AMAZ-IBUH076
```

systeminfo

We see : **Windows Server 2016**

As soon as we run this command, we notice a **notepad file opening in the background**, which is a sign of concurrent

user activity or a triggered process.

User Logins and Compromise Date

Next, we investigate who the users are and when they last logged in to determine the attacker's path.

```
PS C:\Users\Administrator> net user  
User accounts for \\EC2AMAZ-I8UH076  
-----  
Administrator          DefaultAccount          Guest  
Jenny                 John                    
The command completed successfully.
```

net user

we see jeny & john

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

net user jenny

shows never

```
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.
```

net user john

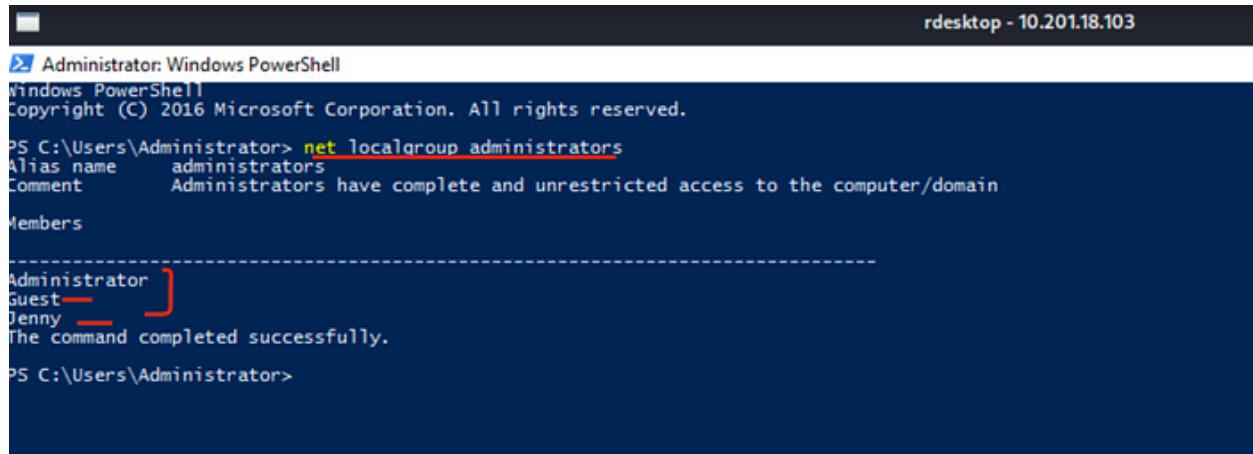
shows 3/2/2019 5:48:32 PM

The **last user who logged in was administrator**, as that is who we signed in as through RDP.

We also found a reference to the IP `10.34.2.3` in a small pop-up alert when initializing the RDP connection, which could be an internal host or C2 server.

We check for other administrator-level accounts:

net localgroup administrators



```
rdesktop - 10.201.18.103
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

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.

PS C:\Users\Administrator>
```

administrator accounts => Guest & 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      *Users
Global Group memberships       *None
The command completed successfully.

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

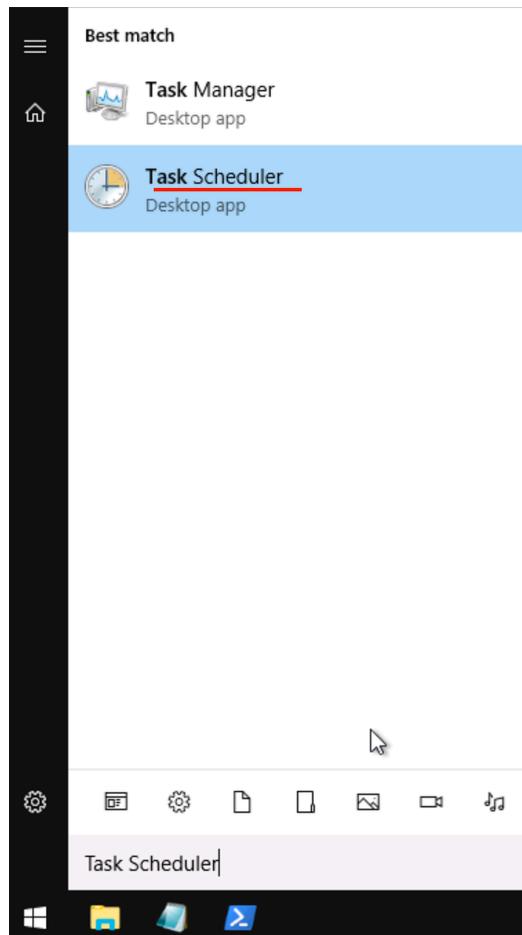
Logon hours allowed            All

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

Throughout these checks, we consistently see the date **3/2/2019** appearing, which suggests this is the likely **date of compromise.**

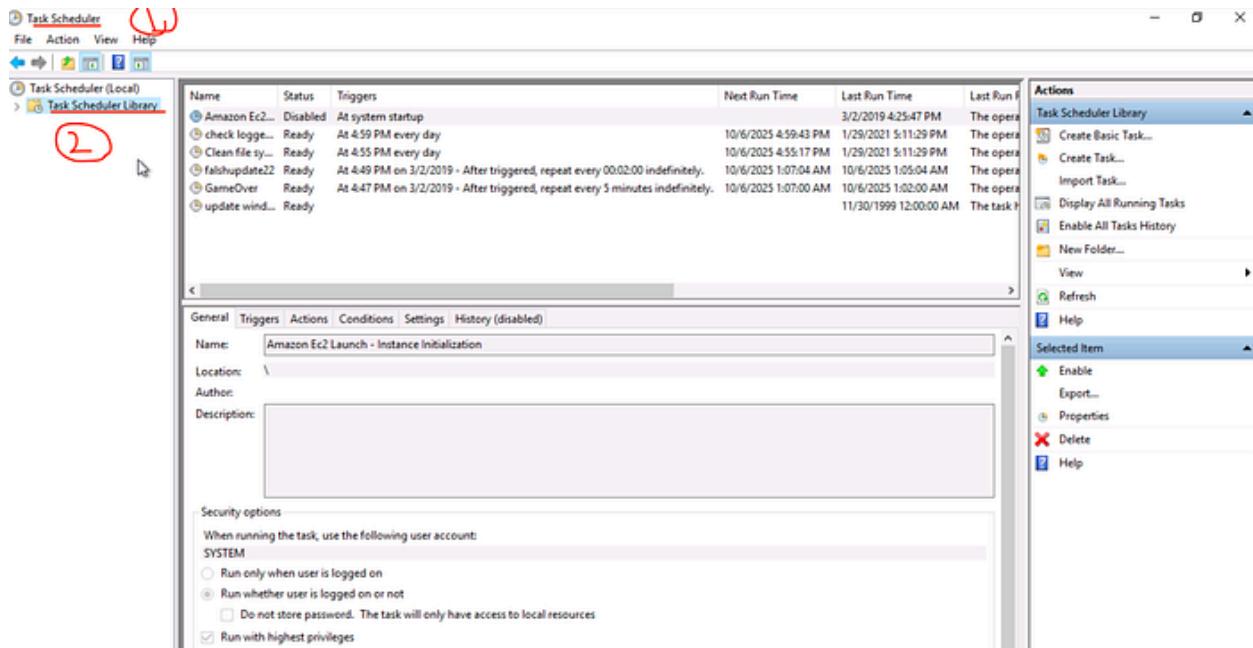
Phase 3: Tracing Attacker Activity

Malicious Scheduled Task Analysis

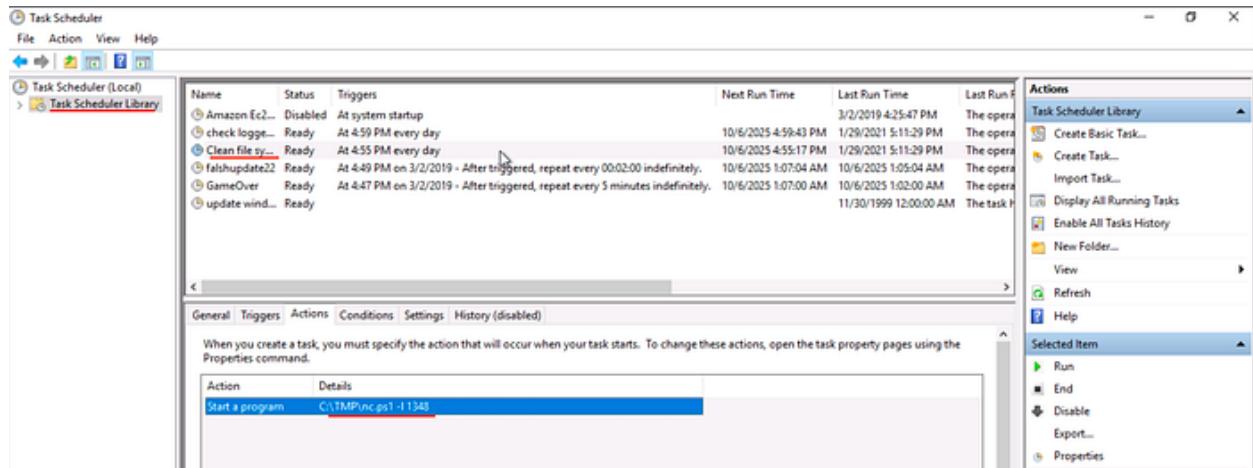


We now pivot to the **Task Scheduler** to look for persistence mechanisms.

Go to task scheduler



Then double click on task schedule library then we then see some task



Looking at each task and its actions, we identify a suspicious task named `clean file system`.

Looking at each of them and actions:

We see `clean file system`

it has a nc going on -> `\nc.ps1 -l 1348` using a powershell script for a different port which is shady

This task was running a PowerShell script to start a Netcat listener.

- File it was trying to run daily is: \nc.ps1 -l 1348
- Port used is: 1348

```
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

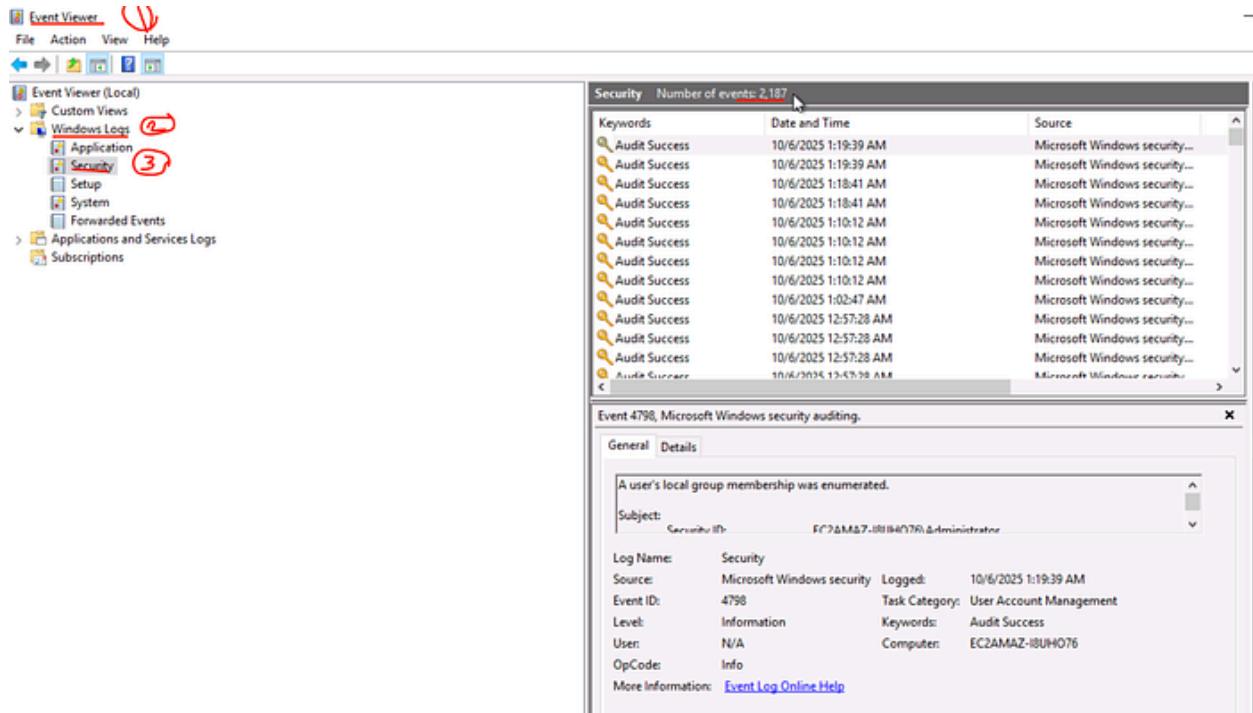
Workstations allowed All
Logon script
User profile
Home directory
Last logon          Never
Logon hours allowed All

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

We confirm that **Jenny last logged in “never”**, a detail noted during the user enumeration phase.

Event Viewer Timeline Analysis

To pinpoint the exact moment special privileges were given (a key action in a compromise), we use the **Event Viewer**.



go to event viewer -> windows log -> security

```
# there are 2,162 events
```

We filter the events using the time hint we found: the date of compromise, 3/2/2019.

And searching up the special privilege code(4672) and using that as a filter

To work with special privileges in Windows, developers must use the Win32 API to enable or disable specific rights within a process's security token. These special privileges (known as user rights) allow a program to perform system-level operations that would otherwise be blocked, such as debugging another process or modifying system time.

The key Windows APIs for managing privileges are:

- `OpenProcessToken()` : Gets a handle to the access token of a process.

filtering using the date event on: 3/2/2019 12AM-11:59PM

Event ID	Task Category
4798	User Account
4672	Special Logon
4624	Logon
4799	Security Log
4799	Security Log
4799	Security Log
4634	Logoff
4634	Logoff
4634	Logoff
4672	Serial Logon

Scrolling down we find the exact match : 03/02/2019 4:04:49

PM

Filter Current Log X

Filter **XML**

Logged:

Event level: Critical Warning Verbose
 Error Information

By log Event logs:

By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

4672

Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>

This timestamp confirms the precise moment the security event occurred.

Security Number of events: 2,187					
Filtered: Log: Security; Source: ; Event ID: 4672 Date Range: From 3/2/2019 12:00:00 AM to 3/2/2019 11:59:59 PM. Number of events: 64					
Keywords	Date and Time	Source	Event ID	Task Category	
🔍 Audit Success	3/2/2019 4:04:53 PM	Microsoft Windows security...	4672	Special Logc	
🔍 Audit Success	3/2/2019 4:04:53 PM	Microsoft Windows security...	4672	Special Logc	
🔍 Audit Success	3/2/2019 4:04:52 PM	Microsoft Windows security...	4672	Special Logc	
🔍 Audit Success	3/2/2019 4:04:52 PM	Microsoft Windows security...	4672	Special Logc	
🔍 Audit Success	3/2/2019 4:04:49 PM	Microsoft Windows security...	4672	Special Logc	
🔍 Audit Success	3/2/2019 4:04:40 PM	Microsoft Windows security...	4672	Special Logc	
🔍 Audit Success	3/2/2019 4:04:39 PM	Microsoft Windows security...	4672	Special Logc	
🔍 Audit Success	3/2/2019 4:04:39 PM	Microsoft Windows security...	4672	Special Logc	
🔍 Audit Success	3/2/2019 4:04:39 PM	Microsoft Windows security...	4672	Special Logc	
🔍 Audit Success	3/2/2019 4:04:39 PM	Microsoft Windows security...	4672	Special Logc	
🔍 Audit Success	3/2/2019 4:04:39 PM	Microsoft Windows security...	4672	Special Logc	
🔍 Audit Success	3/2/2019 4:04:39 PM	Microsoft Windows security...	4672	Special Logc	

Viewing it as a text file:

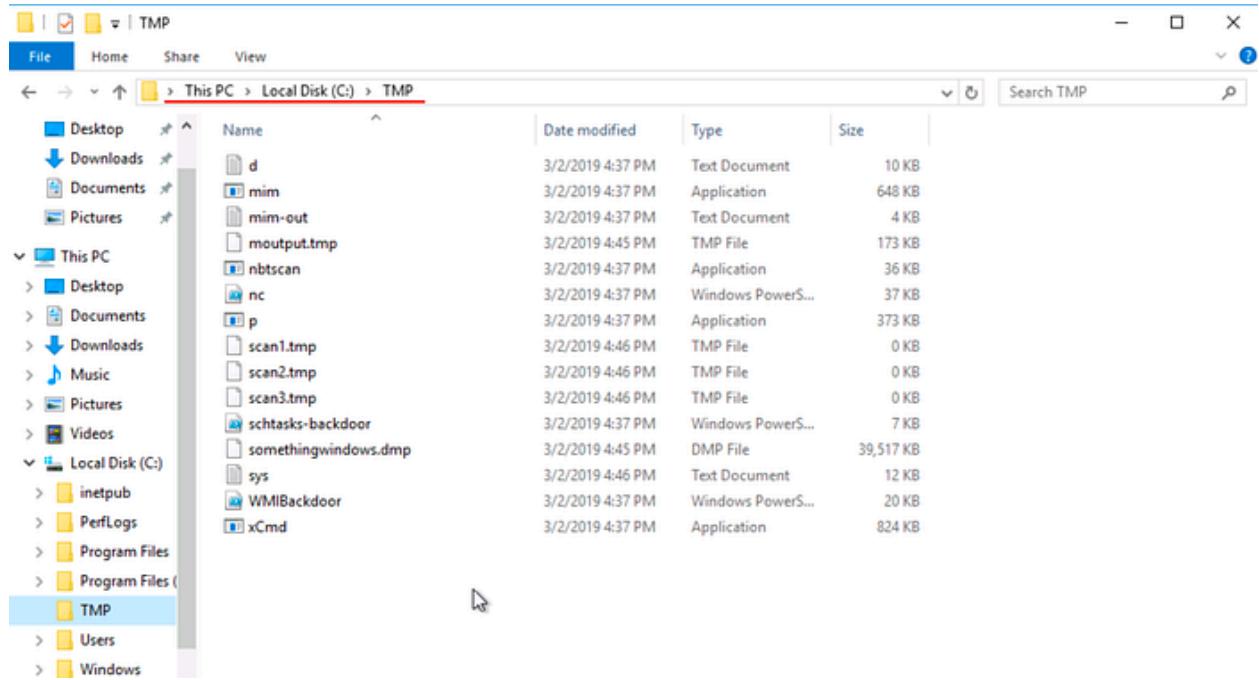
```
Log Name: Security
Source: Microsoft-Windows-Security-Auditing
Date: 3/2/2019 4:04:49 PM
Event ID: 4672
Task Category: Special Logon
Level: Information
Keywords: Audit Success
User: N/A
Computer: EC2AMAZ-I8UH076
Description:
Special privileges assigned to new logon.

Subject:
  Security ID: SYSTEM
  Account Name: SYSTEM
  Account Domain: NT AUTHORITY
  Logon ID: 0x3E7

Privileges: SeAssignPrimaryTokenPrivilege
            SeTcbPrivilege
            SeSecurityPrivilege
            SeTakeOwnershipPrivilege
            SeLoadDriverPrivilege
            SeBackupPrivilege
            SeRestorePrivilege
            SeDebugPrivilege
            SeAuditPrivilege
            SeSystemEnvironmentPrivilege
            SeImpersonatePrivilege
            SeDelegateSessionUserImpersonatePrivilege
```

Artifacts and Persistence Check

We check the temporary directory for any uploaded tools:



Next going to **TMP folder -> file explorer -> c drive -> tmp**

-> we see mim file which is the mimikatz file

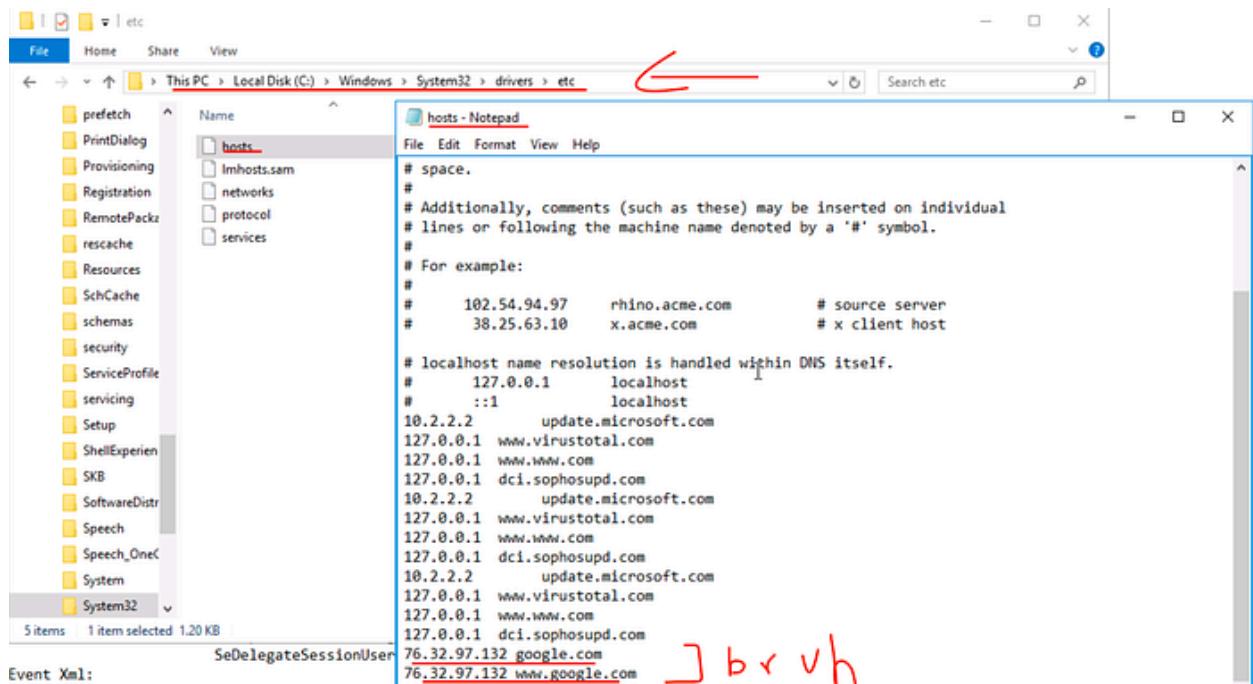
Now, for those who are newbies like :p lol:

What is Mimikatz?

Mimikatz is an open-source application that allows users to view and save authentication credentials such as [Kerberos tickets](#). The toolset works with the current release of Windows and includes a collection of different network attacks to help assess vulnerabilities.

Attackers commonly use Mimikatz to steal credentials and escalate privileges because in most cases, endpoint protection software and antivirus systems will not detect or delete the attack. Conversely, [pen testers](#) use Mimikatz to detect and exploit vulnerabilities in your networks so you can fix them.

Next, we check the `etc/hosts` file, a common location for malicious redirection:



etc /hosts -> windows c drive -> drivers -> etc -> hosts

scrolling down I see the spoofing google attempt lol

Google Public DNS is a free service that offers alternative Domain Name System (DNS) resolvers at addresses like 8.8.8.8 and 8.8.4.4 to make the web faster, more secure, and more reliable by providing faster lookups and protecting against DNS-based attacks. You can use it by manually changing your device's network settings to point to these public DNS servers, effectively replacing your Internet Service Provider's (ISP) DNS. 

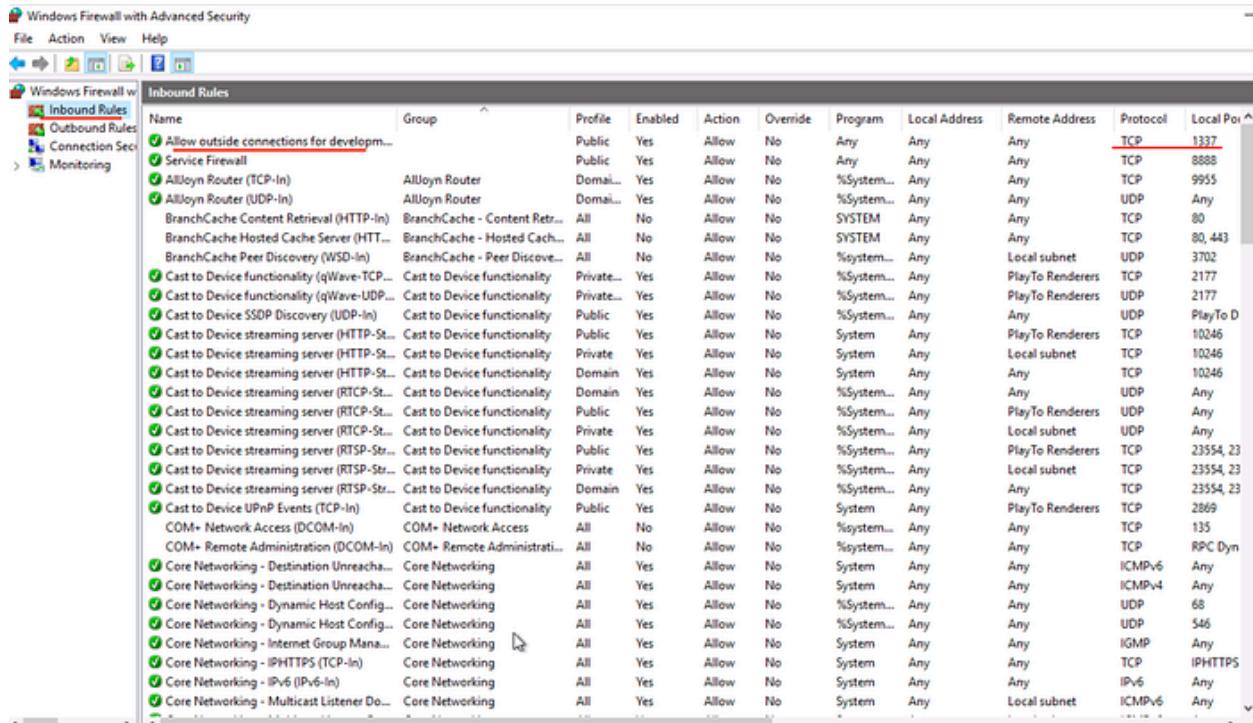
The hosts file modification is the **Command and Control (C&C)** mechanism, and the poisoned site was `google.com`

We check for web shell persistence in the web root:

to check for the shell extension -> **go to inetpub -> www -> and we .jsp**

This PC > Local Disk (C:) > inetpub > wwwroot				
Name	Date modified	Type	Size	
b.jsp	3/2/2019 4:37 PM	JSP File	74 KB	
shell	3/2/2019 4:37 PM	GIF File	13 KB	
tests.jsp	3/2/2019 4:37 PM	JSP File	1 KB	

Finally, we look at the firewall rules to find the last port that was opened, which is often used for exfiltration or establishing a new C2 channel:



The screenshot shows the Windows Firewall with Advanced Security interface. The left pane displays navigation options: File, Action, View, Help, Inbound Rules (selected), Outbound Rules, Connection Sec..., and Monitoring. The right pane is titled 'Inbound Rules' and lists various rules. One rule, 'Allow outside connections for development...', is highlighted with a red box. This rule has the following details:

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port
Allow outside connections for development...		Public	Yes	Allow	No	Any	Any	Any	TCP	1337
Service Firewall		Public	Yes	Allow	No	Any	Any	Any	TCP	8888
AllJoyn Router (TCP-In)	AllJoyn Router	Domain	Yes	Allow	No	%System% Any	Any	Any	TCP	9955
AllJoyn Router (UDP-In)	AllJoyn Router	Domain	Yes	Allow	No	%System% Any	Any	Any	UDP	Any
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	Allow	No	SYSTEM Any	Any	Any	TCP	80
BranchCache Hosted Cache Server (HTTP-In)	BranchCache - Hosted Cach...	All	No	Allow	No	SYSTEM Any	Any	Any	TCP	80, 443
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No	Allow	No	%System% Any	Local subnet	Any	UDP	3702
Cast to Device functionality (qWave-TCP-In)	Cast to Device functionality	Private	Yes	Allow	No	%System% Any	PlayTo Renderers	TCP	2177	
Cast to Device functionality (qWave-UDP-In)	Cast to Device functionality	Private	Yes	Allow	No	%System% Any	PlayTo Renderers	UDP	2177	
Cast to Device SSDP Discovery (UDP-In)	Cast to Device functionality	Public	Yes	Allow	No	%System% Any	Any	Any	UDP	PlayTo D...
Cast to Device streaming server (HTTP-Stream)	Cast to Device functionality	Public	Yes	Allow	No	System Any	PlayTo Renderers	TCP	10246	
Cast to Device streaming server (HTTP-Stream)	Cast to Device functionality	Private	Yes	Allow	No	System Any	Local subnet	TCP	10246	
Cast to Device streaming server (HTTP-Stream)	Cast to Device functionality	Domain	Yes	Allow	No	System Any	Any	TCP	10246	
Cast to Device streaming server (RTCP-Stream)	Cast to Device functionality	Domain	Yes	Allow	No	%System% Any	Any	UDP	Any	
Cast to Device streaming server (RTCP-Stream)	Cast to Device functionality	Public	Yes	Allow	No	%System% Any	PlayTo Renderers	UDP	Any	
Cast to Device streaming server (RTSP-Stream)	Cast to Device functionality	Private	Yes	Allow	No	%System% Any	PlayTo Renderers	TCP	23554, 23	
Cast to Device streaming server (RTSP-Stream)	Cast to Device functionality	Private	Yes	Allow	No	%System% Any	Local subnet	TCP	23554, 23	
Cast to Device streaming server (RTSP-Stream)	Cast to Device functionality	Domain	Yes	Allow	No	%System% Any	Any	TCP	23554, 23	
Cast to Device UPnP Events (TCP-In)	Cast to Device functionality	Public	Yes	Allow	No	System Any	PlayTo Renderers	TCP	2869	
COM+ Network Access (DCOM-In)	COM+ Network Access	All	No	Allow	No	%System% Any	Any	TCP	135	
COM+ Remote Administration (DCOM-In)	COM+ Remote Administrati...	All	No	Allow	No	%System% Any	Any	TCP	RPC Dyn...	
Core Networking - Destination Unreacha...	Core Networking	All	Yes	Allow	No	System Any	Any	ICMPv6 Any		
Core Networking - Destination Unreacha...	Core Networking	All	Yes	Allow	No	System Any	Any	ICMPv4 Any		
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow	No	%System% Any	Any	UDP 68		
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow	No	%System% Any	Any	UDP 546		
Core Networking - Internet Group Mana...	Core Networking	All	Yes	Allow	No	System Any	Any	IGMP Any		
Core Networking - IPHTTPS (TCP-In)	Core Networking	All	Yes	Allow	No	System Any	Any	TCP IPHTTPS		
Core Networking - IPv6 (IPv6-In)	Core Networking	All	Yes	Allow	No	System Any	Any	IPv6 Any		
Core Networking - Multicast Listener Do...	Core Networking	All	Yes	Allow	No	System Any	Local subnet	ICMPv6 Any		

Next to find the last opened port -> go to firewall -> inbound
-> and the topmost is the latest connection -> port 1337

What's the version and year of the windows machine?

Windows Server 2016

✓ Correct Answer

Which user logged in last?

Administrator

✓ Correct Answer

💡 Hint

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

✓ Correct Answer

💡 Hint

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

10.34.2.3

✓ Correct Answer

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

Answer format: List them in alphabetical order.

Guest, Jenny

✓ Correct Answer

What's the name of the scheduled task that is malicious?

Clean file system

✓ Correct Answer

What file was the task trying to run daily?

nc.ps1

✓ Correct Answer

What port did this file listen locally for?

1348

✓ Correct Answer

When did Jenny last logon?

Never

✓ Correct Answer

At what date did the compromise take place?

Answer format: MM/DD/YYYY

03/02/2019

✓ Correct Answer

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 ✓ Correct Answer 💡 Hint

What tool was used to get Windows passwords?

Mimikatz ✓ Correct Answer

What was the attackers external control and command servers IP?

76.32.97.132 ✓ Correct Answer

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

.jsp ✓ Correct Answer

What was the last port the attacker opened?

1337 ✓ Correct Answer 💡 Hint

Check for DNS poisoning, what site was targeted?

google.com ✓ Correct Answer

CONCLUSION:

I hope this write-up walkthrough was helpful to you all!

This room was more of a forensic based room on Windows OS
and it was fun!

Now that I've gotten through it, I hope it helps you and gets you
through the room as well. I plan on putting out more like these in
the future!

If you guys want me to cover any specific room or challenge, or if you have any queries, feel free to drop a comment.

I'll check it out and get back to you as soon as I can. Also, you can find all of my writeups and future ones on my GitHub:

<https://github.com/5kullk3r>

Imma bounce for now, but I'll catch you all in the next writeup!