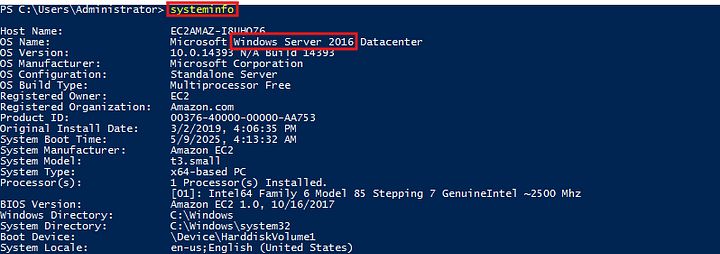
### **Investigating Windows — TryHackMe**

A windows machine has been hacked, its your job to go investigate this windows machine and find clues to what the hacker might have done.

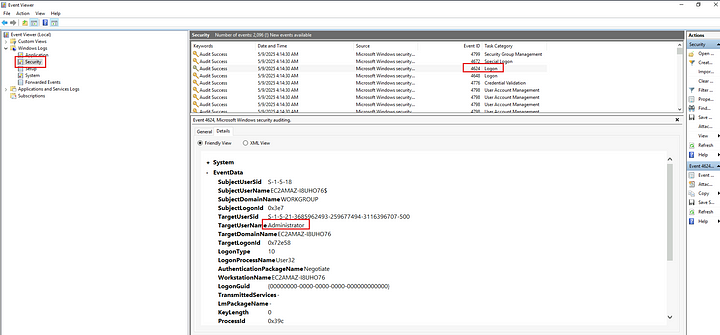
**1.What's the version and year of the windows machine?**

systeminfo



**Answer:** Windows Server 2016

**2. Which user logged in last?**That should be us.

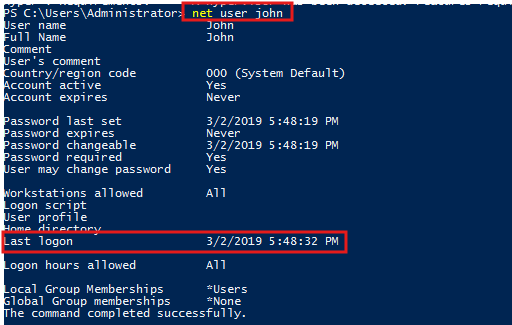


**Answer:** Administrator

**3. When did John log onto the system last?**

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

net user john

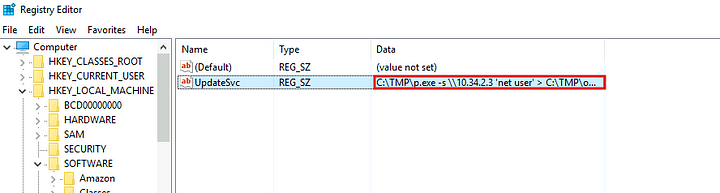


**Answer:** 03/02/2019 5:48:32 PM

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

This is refering to a startup process. We can check this in the registry keys.

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

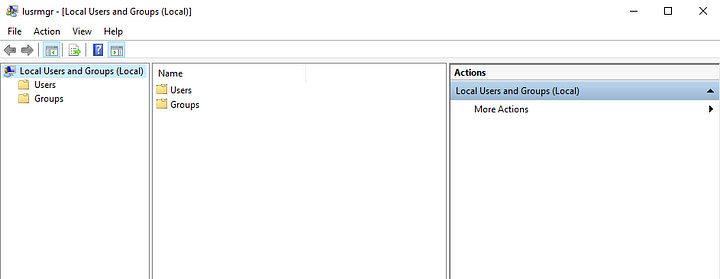


**Answer:** 10.34.2.3

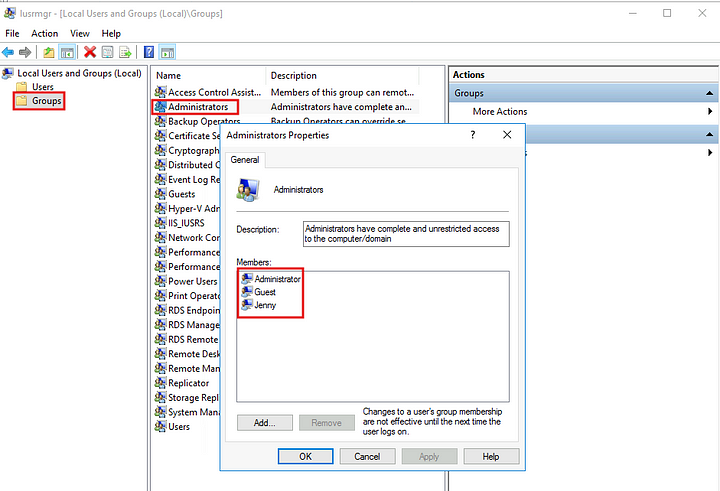
**5.What two accounts had administrative privileges (other than the Administrator user)?**

**Answer format: List them in alphabetical order.**

click windows + r to open the run window. Then type lusrmgr.msc. This opens the local users and groups



Now click on groups and select Administrators.



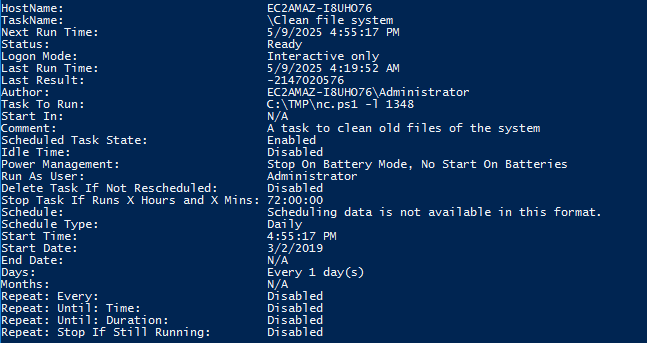
**Answer:** Guest, Jenny

**6.Whats the name of the scheduled task that is malicious.**

We can list out the scheduled tasks using the following command

schtasks /query /fo LIST /v

This gives a lot of output, if we search through the output there is a task, which is executing PowerShell script from the TMP folder which is suspicious.



As we can see above this is creating a netcat listener and it is scheduled to run every day at 4:55.

**Answer:** Clean File System

**7. What file was the task trying to run daily?**

The answer to this is in the above screenshot.

**Answer:** nc.ps1

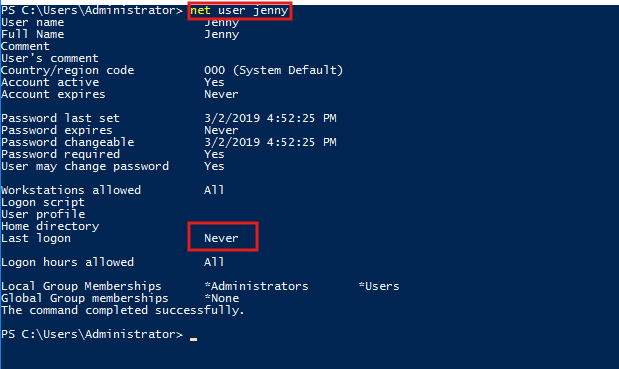
**8. What port did this file listen locally for?**

This is also found in the above screenshot.

**Answer:** 1348

9. When did Jenny last logon?

net user jenny

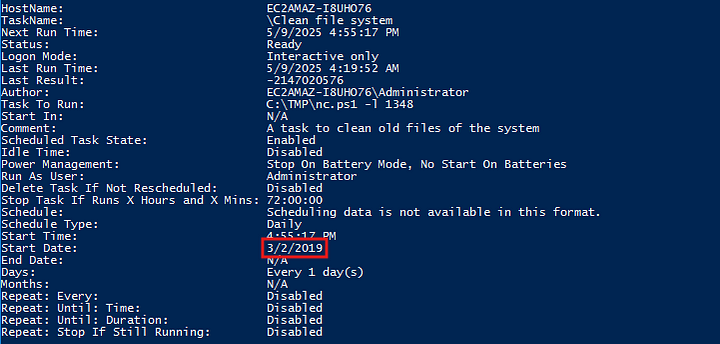


**Answer:** Never

**10. At what date did the compromise take place?**

**Answer format: MM/DD/YYYY**

This is clearly seen in the screenshot in question 6.

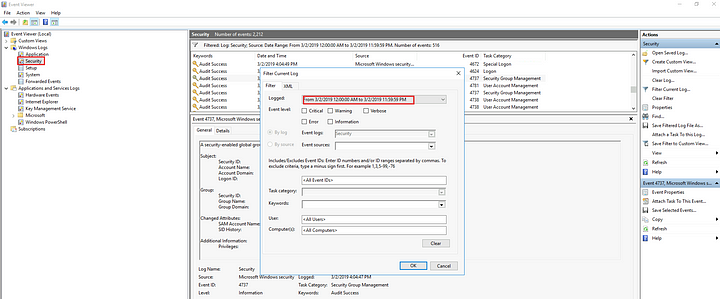


**Answer:** 03/02/2019

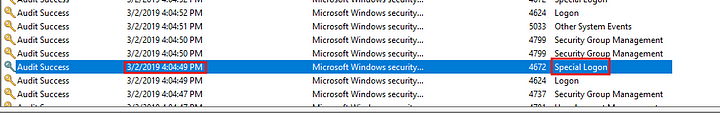
**11. During the compromise, at what time did Windows first assign special privileges to a new logon?**

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

In event viewer, under the security logs, click filter events and select the date at which the malicious activity started.



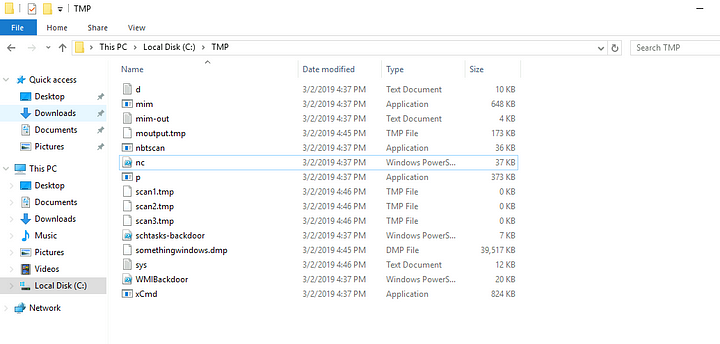
Then, as per the hint the answer ends with 49. Looking for special logon attempts, we can see the answer.



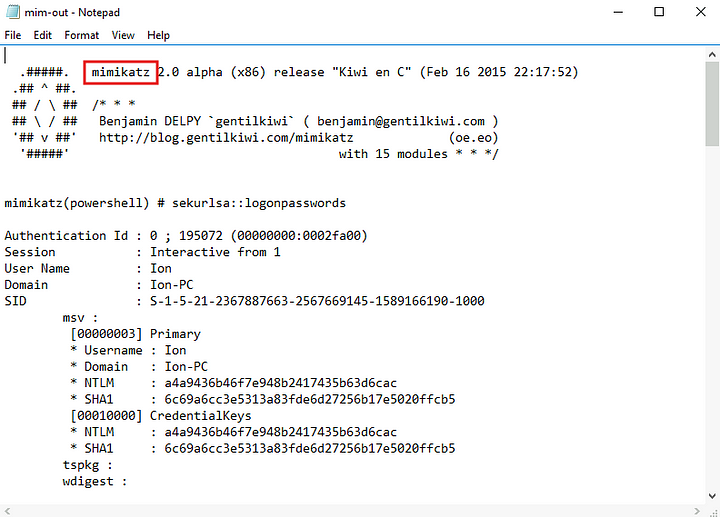
**Answer:** 03/02/2019 4:04:49 PM

**12. What tool was used to get Windows passwords?**

Let us look at the TMP directory to see if we can find anything, as the suspicious registry key and the sceduled task are pointing towards this directory.



We can see and executable named mim and a text file named mim-out. Let us read this text file.



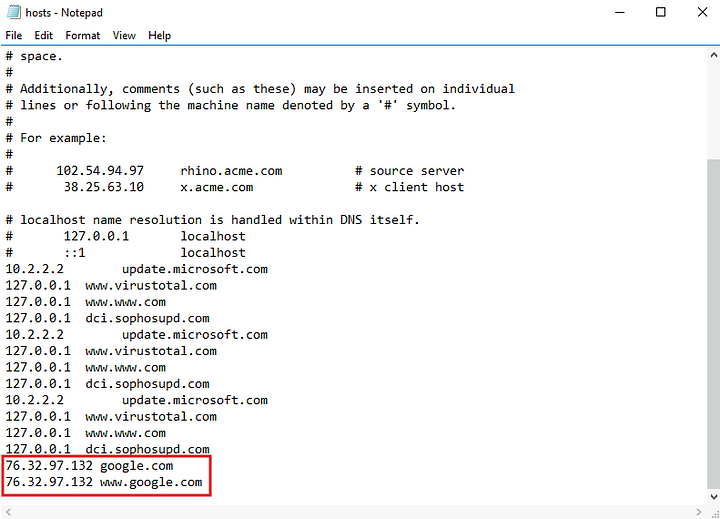
As we can see a reference to Mimikatz which is a tool used by attackers to extract credentials.

**Answer:** Mimikatz

**13. What was the attackers external control and command servers IP?**

I checked the code to find any reference to the IP address but there is none. So let us check the hosts file on windows, this file acts like a local address book for websites and servers. Usually when an attacker is would modify this file to block any security sites and updates.

Path: C:\Windows\System32\drivers\etc\hosts



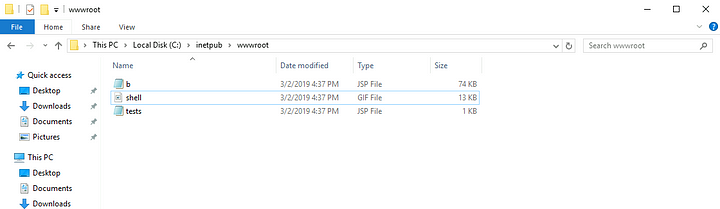
**Answer:** 76.32.97.132

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

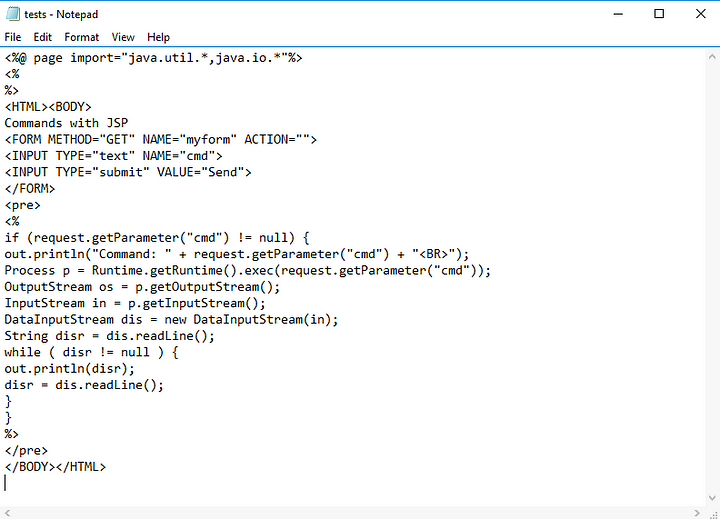
We can check the inetpub folder which is the default webserver directory for windows, where it stores websites and related files.

**Path:** C:\inetpub\wwwroot

There are three files in this folder



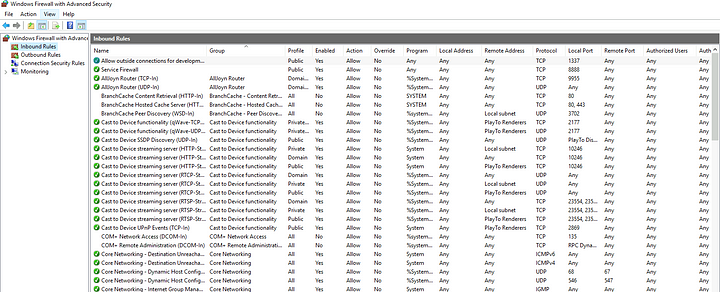
If we inspect these files, we can find that the third file is the one that gives a shell.



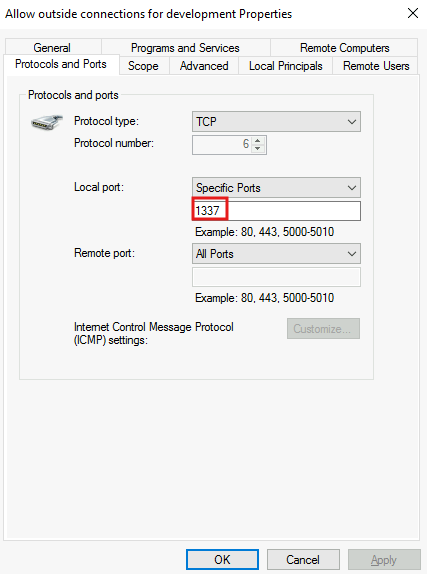
**Answer:** .jsp

**15. What was the last port the attacker opened?**

The hint to this is pointing at the firewall, so the attacker had likely changed the firewall rules to allow the connection from the outside. So we open the firewall and check the inbound rules.



We can see the first rule, let us open it to check what its configuration

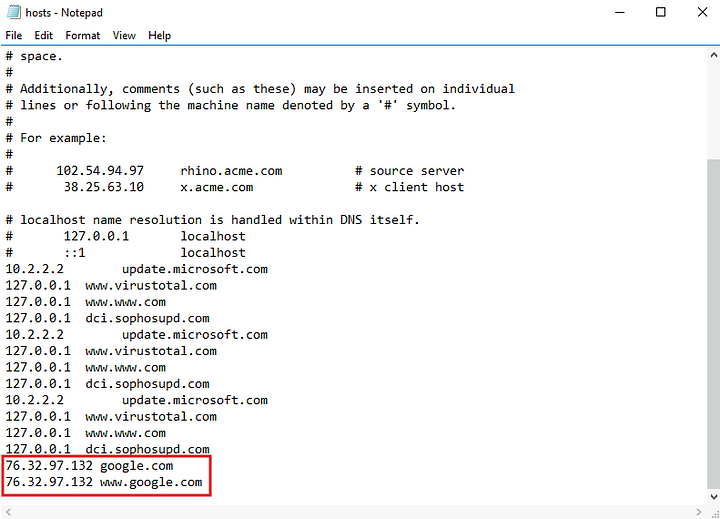


We can see port 1337 which is commonly used by hackers to show skill or expertise.

**Answer:** 1337

**16.Check for DNS poisoning, what site was targeted?**

We can find the answer to this in the question 13, where we can see that the attacker actually is pointing the malicious IP to google.com.



**Answer:** google.com

To sum up this attack,

First the attacker uploaded a shell to the webserver and then opened a connection to the remote IP and then using mimikatz they collected the credentials of the users and sent them over the remote connection.

This is the end of the investigation.