# *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!

| | |
|---|---|
| **#1** | **Whats the version and year of the windows machine?** |

```
PS:> systeminfo /fo csv | ConvertFrom-Csv | select OS*, System*, Hotfix* | Format-List
```

**Windows Server 2016**

| | |
|---|---|
| **#2** | **Which user logged in last?** |

```
PS:> quser
```

**Administrator**

| | |
|---|---|
| **#3** | **When did John log onto the system last?**<br>**Answer format: MM/DD/YYYY H:MM:SS AM/PM** |

```
PS:> net user john | findstr /C:"Last logon"
```

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

| | |
|---|---|
| **#4** | **What IP does the system connect to when it first starts?** |

**run registry editor (regedit) and go to HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run**

**the value = C:\TMP\p.exe -s \\10.34.2.3 'net user' > C:\TMP\o2.txt**

## 10.34.2.3

| | |
|---|---|
| #5 | What two accounts had administrative privileges (other than the Administrator user)?<br>Answer format: username1, username2 |

**use Event Viewer**

## Jenny,Guest

| | |
|---|---|
| #6 | Whats the name of the scheduled task that is malicous. |

**run Task Scheduler to find malicious task**

## clean file system

| | |
|---|---|
| #7 | What file was the task trying to run daily? |

## nc.ps1

| | |
|---|---|
| #8 | What port did this file listen locally for? |

## 1348

| | |
|---|---|
| #9 | When did Jenny last logon? |

## never

| | |
|---|---|
| #10 | At what date did the compromise take place?<br><br>Answer format: MM/-DD/YY |

## 03/02/2019

| | |
|---|---|
| #11 | At what time did Windows first assign special privileges to a new logon?<br><br>Answer format: MM/-DD/YYYY HH:MM:SS AM/PM |

## 03/02/2019 4:04:49 PM

| | |
|---|---|
| #12 | What tool was used to get Windows passwords? |

**find in Event Viewer**

## mimikatz

| | |
|---|---|
| #13 | What was the attackers external control and command servers IP? |

## 76.32.97.132

| | |
|---|---|
| #14 | What was the extension name of the shell uploaded via the servers website? |

.jsp

| | |
|---|---|
| #15 | What was the last port the attacker opened? |

1337