

So welcome again...

Now with first windows room <https://tryhackme.com/room/investigatingwindows>

So let's start

Whats the version and year of the windows machine?

So go to start menu >> settings >> system >> about

About

PC name EC2AMAZ-I8UHO76

Rename PC

Organization WORKGROUP

Join a domain

Edition Windows Server 2016 Datacenter

Version 1607

OS Build 14393.2791

Product ID 00376-40000-00000-AA753

Processor Intel(R) Xeon(R) Platinum 8259CL CPU @
2.50GHz 2.50 GHz

Answer >> windows server 2016

When did John log onto the system last?

Open cmd >> net user John

```

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.

```

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

Which user logged in last?

```
C:\Users\Administrator>
```

Answer > Administrator

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

Answer >> 10.34.2.3

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

Cmd >> net users >> net user Jenny & net user Guest since we saw the output for John


```
C:\Users\Administrator>net user Guest
User name                Guest
Full Name
Comment                  Built-in account for guest access to the com
ter/domain
User's comment
Country/region code      000 (System Default)
Account active            Yes
Account expires           Never

Password last set        3/2/2019 4:39:43 PM
Password expires          Never
Password changeable       3/2/2019 4:39:43 PM
Password required         No
User may change password  No

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.
```




```
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.
```

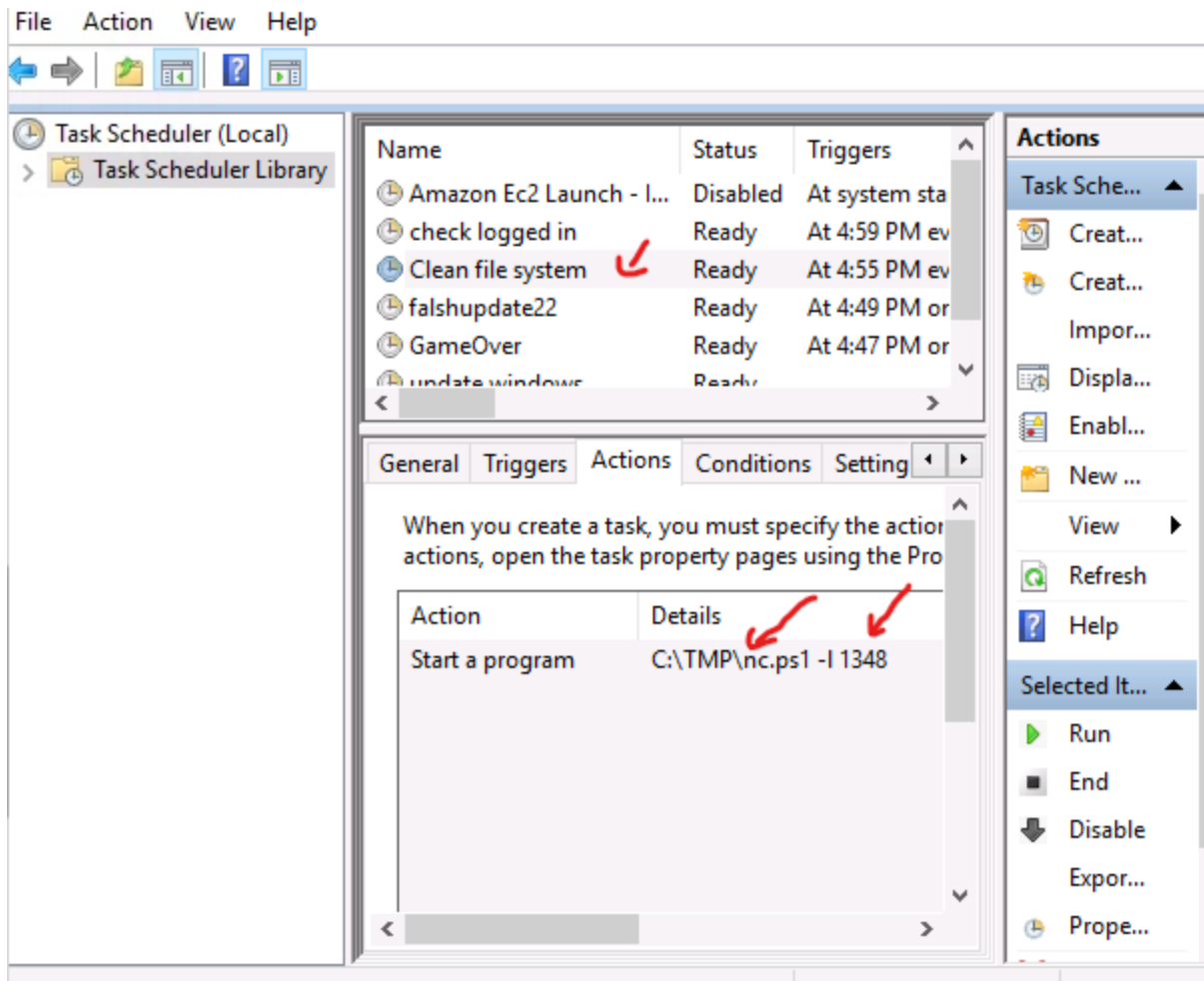


Answer >> Jenny, Guest

When did Jenny last logon?

Answer >> Never

Whats the name of the scheduled task that is malicious.



Answer >> clean file system

What file was the task trying to run daily?

Answer > nc.ps1

What port did this file listen locally for?

Answer >> 1348

At what time did Windows first assign special privileges to a new logon?

Use event id 4672 for special priv. assignment

Applic	Audit Success	3/2/2019 4:04:53 PM	Microsoft Windows security...	4672
--------	---------------	---------------------	-------------------------------	------

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

At what date did the compromise take place?

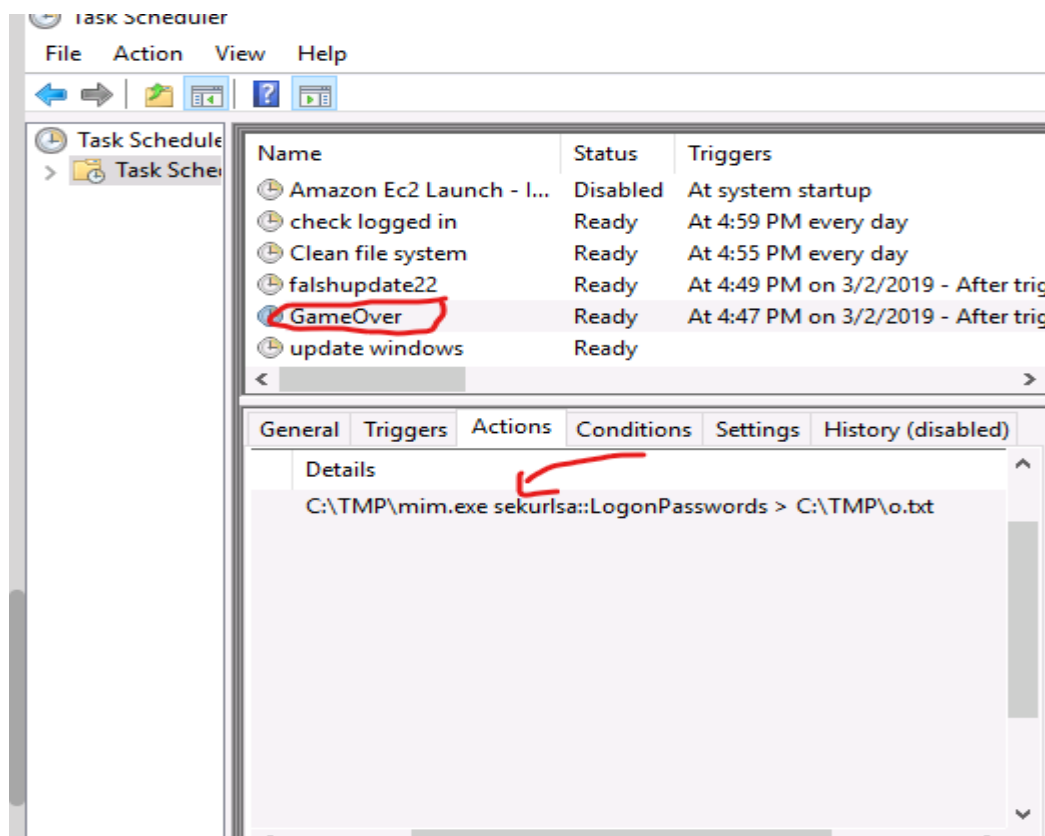
Answer >> 03/02/2019

What tool was used to get Windows passwords?

In task schedule there's one named GameOver so I checked it and a file mim.exe in TMP which

Triggered every 5 mins the output file in C:\TMP\o.txt

when I went to TMP I found no o.txt but I found mim_out instead



```
|
.#####.  mimikatz 2.0 alpha (x86) release "Kiwi en C" (Feb 16 2015 22:17:
.## ^ ##.
## / \ ## /* * *
## \ / ## 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 :
[00000003] Primary
* Username : Ion
* Domain   : Ion-PC
* NTLM     : -4-042654667-0485044742560240---
```

Answer >> mimikatz

What was the attackers external control and command servers IP?

Go to C:\Windows\System32\drivers\etc\hosts find out google.com has a weird IP which doesn't belong to it

File Edit Format View Help

```
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97      rhino.acme.com      # source server
#      38.25.63.10      x.acme.com         # x client host

# 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
```

Answer >> 76.32.97.132

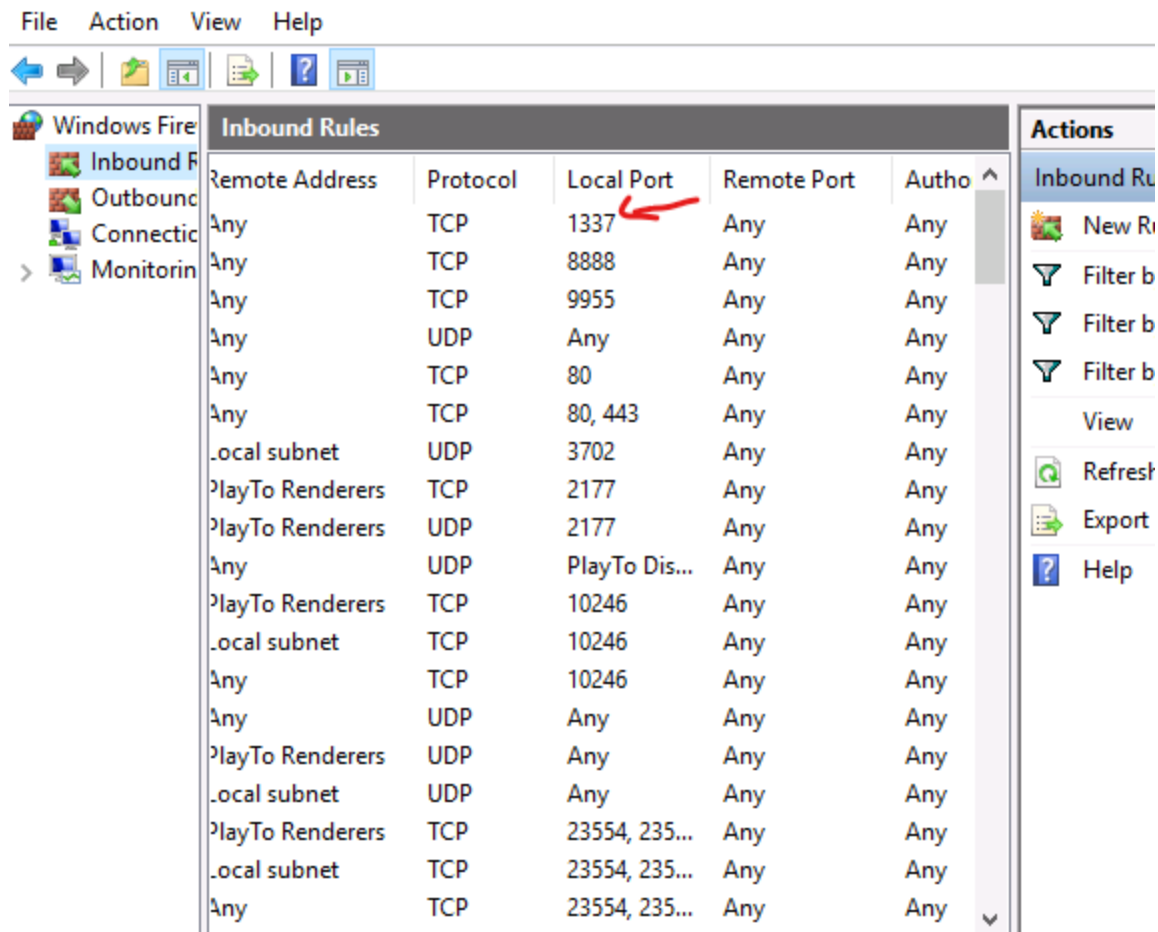
Check for DNS poisoning, what site was targeted?

Answer >>

Google.com

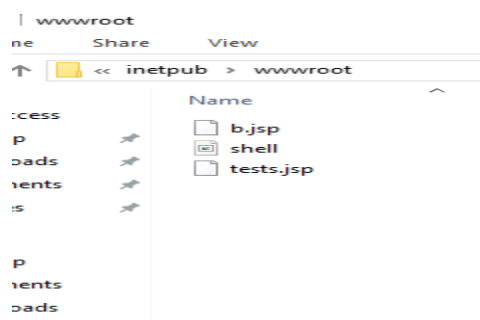
What was the last port the attacker opened?

Go to Windows firewall and advanced security the inbound rules and check the port of first rule



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

Since default webserver is IIS so I went to inetpub folder then wwwroot



Answer >> .jsp



Congratulations

You've completed the room!



Share on Twitter



Share on Facebook

 Share on LinkedIn