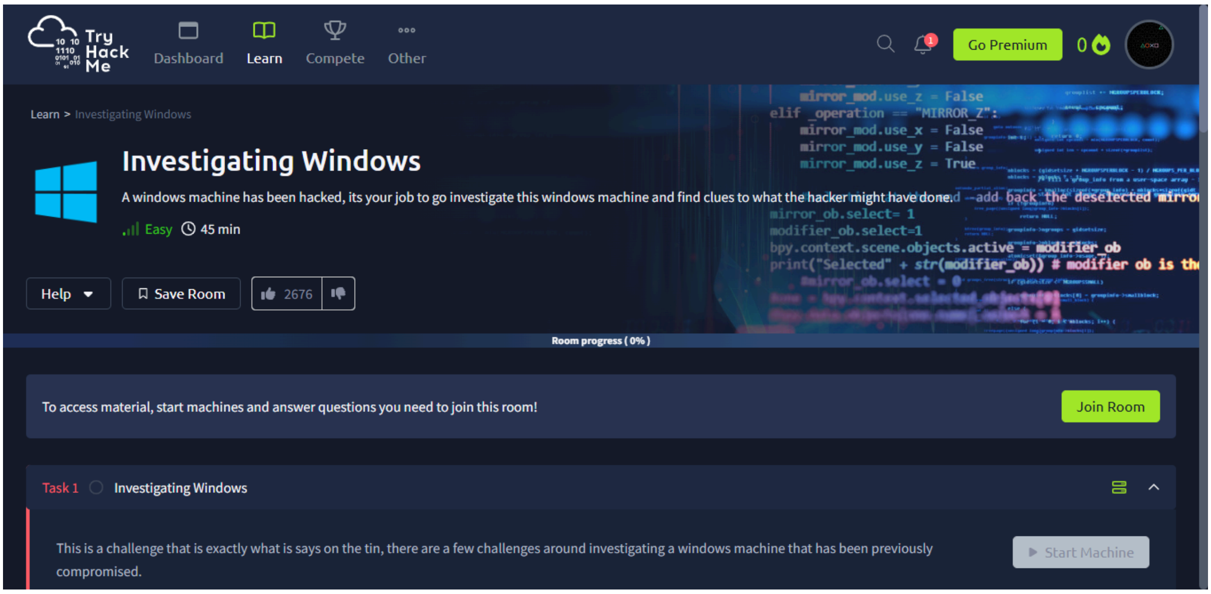
Investigating Windows - A TryHackMe CTF Writeup

- By Nobin Sijo

Below is a rite-up documenting the tasks completed in the TryHackMe CTF room "Investigating Windows".



Learn > Investigating Windows

Investigating Windows

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.

Easy 45 min

Room progress (0%)

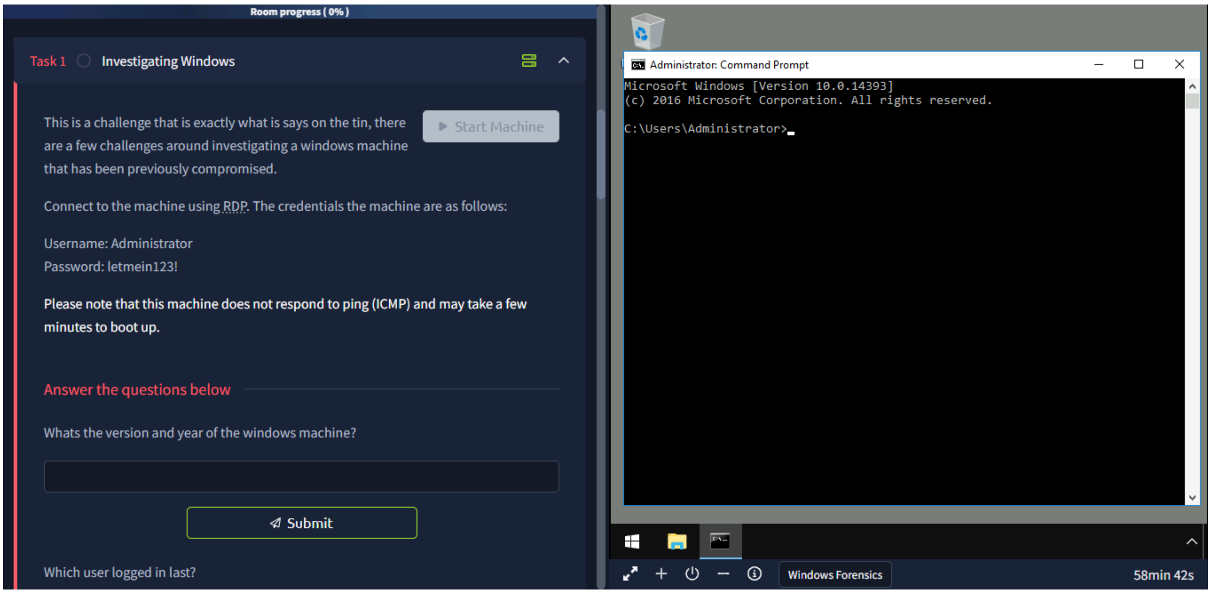
To access material, start machines and answer questions you need to join this room!

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.

Connected to the Windows machine using RDP with the credentials: Username: Administrator, Password: letmein123!.

1) Determined Windows Version and Year



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.

Answer the questions below

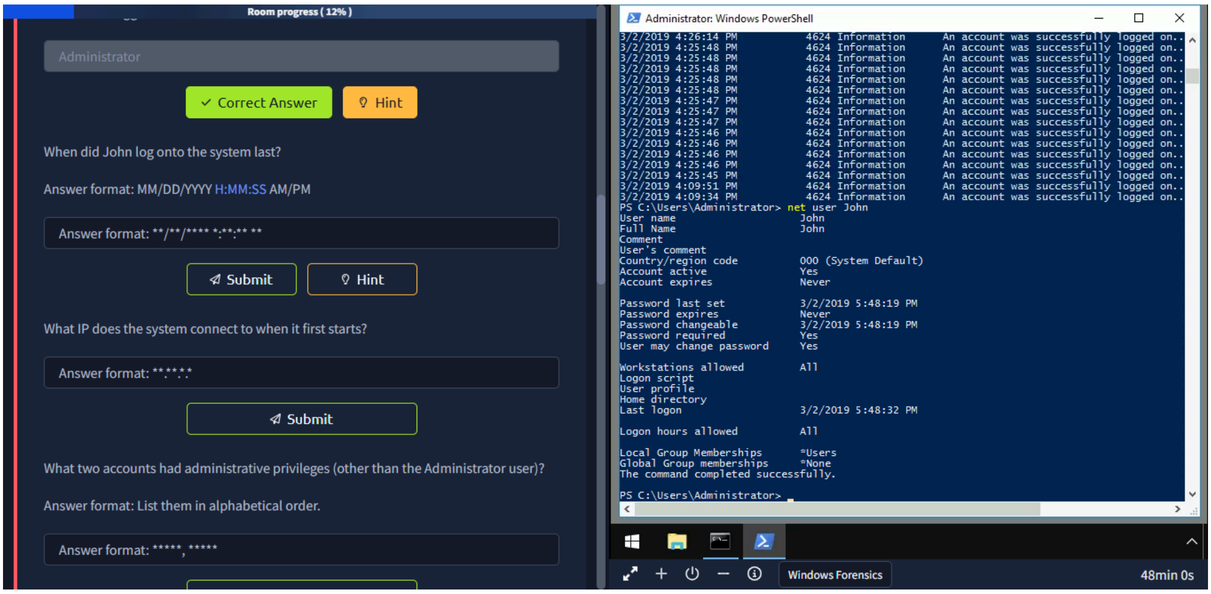
Whats the version and year of the windows machine?

Which user logged in last?

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>_
```

- Pathway: Command Prompt
- Action: Checked the command prompt version details using winver
- Finding: Identified the system as Windows 10 Server, Version 10.0.14393, released in 2016.

2) Identified Last User to Log In



Administrator

When did John log onto the system last?

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

Answer format: **/**/**** *:**:** **

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

Answer format: **.*.*.*

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

Answer format: List them in alphabetical order.

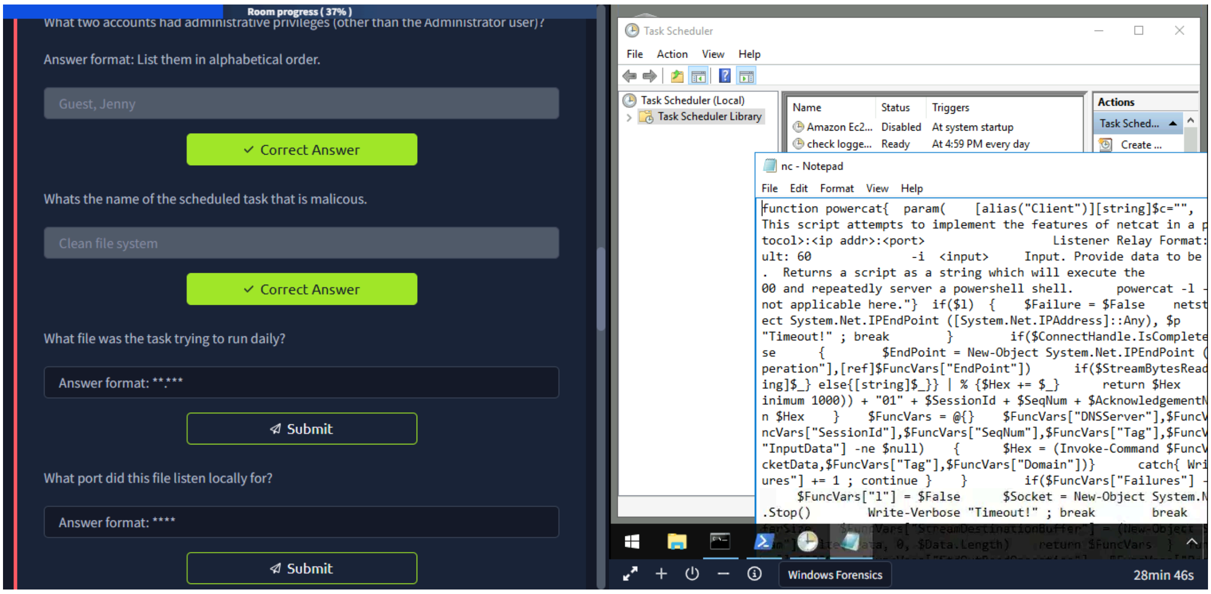
Answer format: *****, *****

```
3/2/2019 4:26:14 PM          4624 Information      An account was successfully logged on..
3/2/2019 4:25:48 PM          4624 Information      An account was successfully logged on..
3/2/2019 4:25:48 PM          4624 Information      An account was successfully logged on..
3/2/2019 4:25:48 PM          4624 Information      An account was successfully logged on..
3/2/2019 4:25:48 PM          4624 Information      An account was successfully logged on..
3/2/2019 4:25:48 PM          4624 Information      An account was successfully logged on..
3/2/2019 4:25:47 PM          4624 Information      An account was successfully logged on..
3/2/2019 4:25:47 PM          4624 Information      An account was successfully logged on..
3/2/2019 4:25:47 PM          4624 Information      An account was successfully logged on..
3/2/2019 4:25:46 PM          4624 Information      An account was successfully logged on..
3/2/2019 4:25:46 PM          4624 Information      An account was successfully logged on..
3/2/2019 4:25:46 PM          4624 Information      An account was successfully logged on..
3/2/2019 4:25:46 PM          4624 Information      An account was successfully logged on..
3/2/2019 4:25:45 PM          4624 Information      An account was successfully logged on..
3/2/2019 4:09:51 PM          4624 Information      An account was successfully logged on..
3/2/2019 4:09:34 PM          4624 Information      An account was successfully logged on..
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.

PS C:\Users\Administrator> _
```

- Pathway: Administrator: Windows PowerShell
- Action: Ran the command net user John.

- Finding: Confirmed John as the last user to log in, with the last logon time of 3/2/2019 5:48:32 PM.

3) Determined Date of Compromise



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

Answer format: List them in alphabetical order.

Guest, Jenny

Whats the name of the scheduled task that is malcious.

Clean file system

What file was the task trying to run daily?

Answer format: **.***

What port did this file listen locally for?

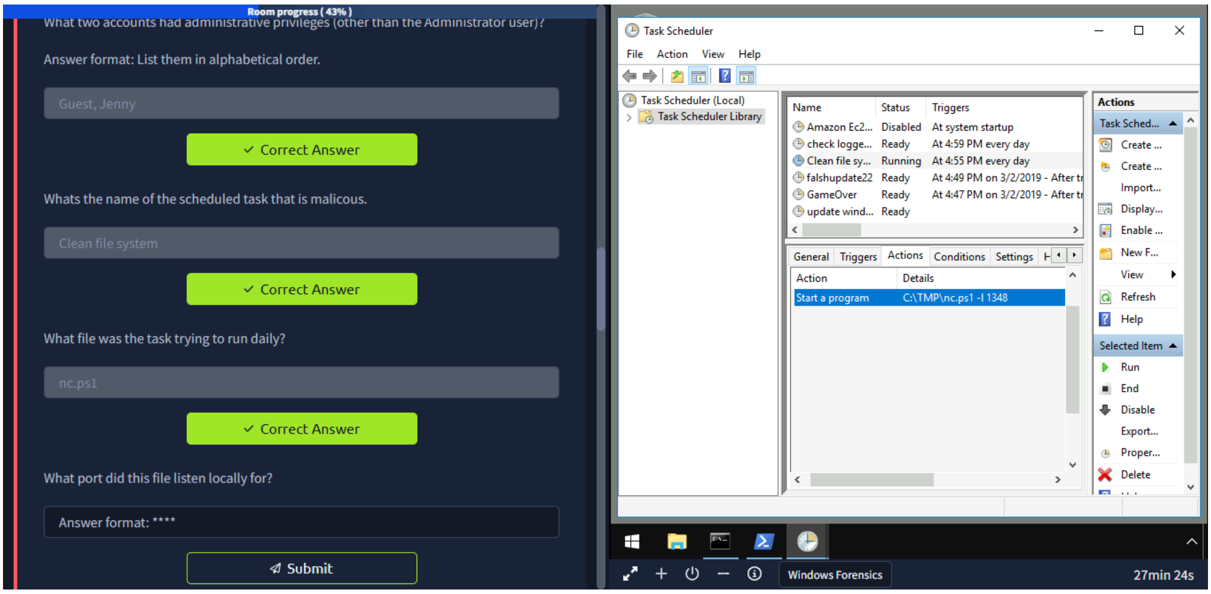
Answer format: ****

Name	Status	Triggers
Amazon Ec2...	Disabled	At system startup
check logge...	Ready	At 4:59 PM every day

```
function powercat{  param(    [alias("Client")][string]$c="",
This script attempts to implement the features of netcat in a p
tocol>:<ip addr>:<port>                          Listener Relay Format:
ult: 60                 -i  <input>     Input. Provide data to be
.  Returns a script as a string which will execute the
00 and repeatedly server a powershell shell.     powercat -l -
not applicable here."}  if($l)  {    $Failure = $False    netst
ect System.Net.IPEndPoint ([System.Net.IPAddress]::Any), $p
"Timeout!" ; break        }         if($ConnectHandle.IsComplete
se      {         $EndPoint = New-Object System.Net.IPEndPoint (
peration"],[ref]$FuncVars["EndPoint"])      if($StreamBytesRead
ing]$_} else{[string]$_}} | % {$Hex += $_}       return $Hex
inimum 1000)) + "01" + $SessionId + $SeqNum + $AcknowledgementN
n $Hex    }    $FuncVars = @{}    $FuncVars["DNSServer"],$FuncV
ncVars["SessionId"],$FuncVars["SeqNum"],$FuncVars["Tag"],$FuncV
"InputData"] -ne $null)    {      $Hex = (Invoke-Command $FuncV
cketData,$FuncVars["Tag"],$FuncVars["Domain"])}       catch{ Wri
ures"] += 1 ; continue }    }        if($FuncVars["Failures"] -
    $FuncVars["l"] = $False     $Socket = New-Object System.N
.Stop()       Write-Verbose "Timeout!" ; break       break
```

- Pathway: Windows Event Viewer -> Security
- Action: Reviewed security logs for the first successful logon event.
- Finding: The compromise took place on 03/02/2019.

4) Identified Time of First Special Privileges Assignment



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

Answer format: List them in alphabetical order.

Guest, Jenny

Whats the name of the scheduled task that is malicous.

Clean file system

What file was the task trying to run daily?

nc.ps1

What port did this file listen locally for?

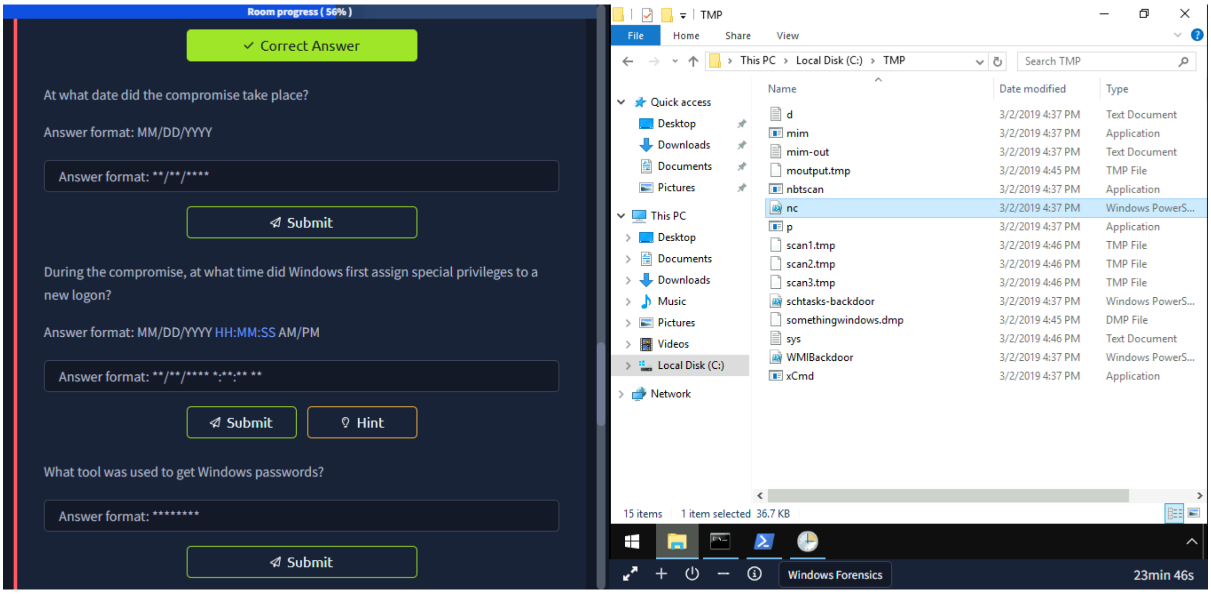
Answer format: ****

Name	Status	Triggers
Amazon Ec2...	Disabled	At system startup
check logge...	Ready	At 4:59 PM every day
Clean file sy...	Running	At 4:55 PM every day
falshupdate22	Ready	At 4:49 PM on 3/2/2019 - After tr
GameOver	Ready	At 4:47 PM on 3/2/2019 - After tr
update wind...	Ready	

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

- Pathway: Windows Event Viewer -> Security
- Action: Analyzed logon events for special privilege assignments.
- Finding: Windows first assigned special privileges to a new logon on 3/2/2019 4:04:49 PM.

5) Identified Tool Used to Get Windows Passwords



At what date did the compromise take place?

Answer format: MM/DD/YYYY

Answer format: **/**/****

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

Answer format: **/**/**** *:**:** **

What tool was used to get Windows passwords?

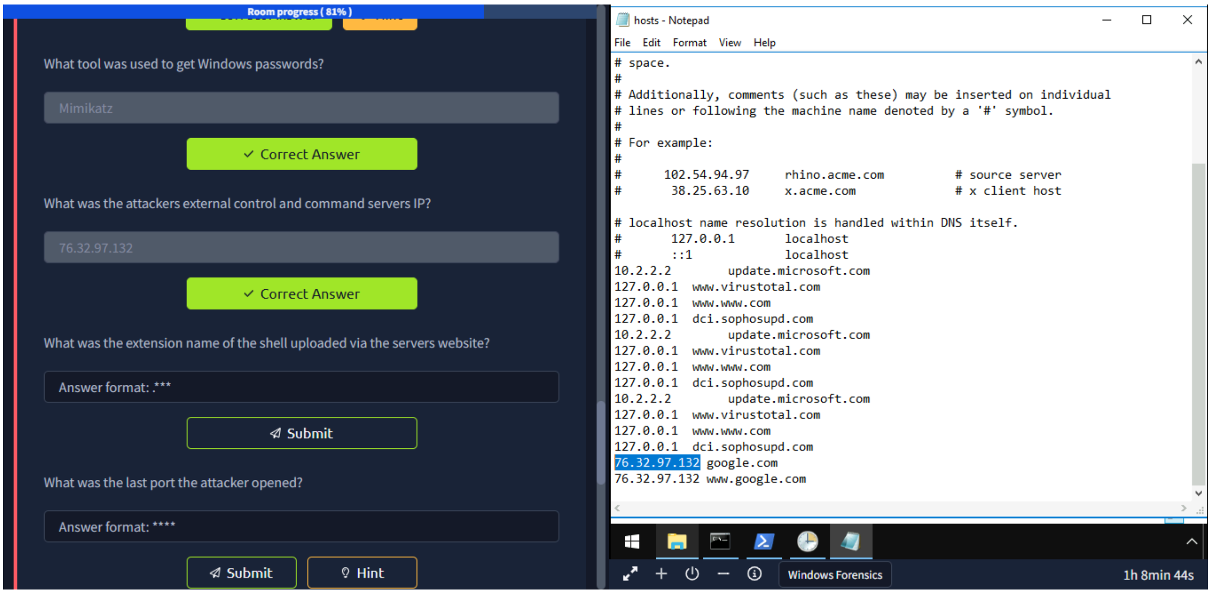
Answer format: *******

Name	Date modified	Type
d	3/2/2019 4:37 PM	Text Document
mim	3/2/2019 4:37 PM	Application
mim-out	3/2/2019 4:37 PM	Text Document
moutput.tmp	3/2/2019 4:45 PM	TMP File
nbtscan	3/2/2019 4:37 PM	Application
nc	3/2/2019 4:37 PM	Windows PowerS...
p	3/2/2019 4:37 PM	Application
scan1.tmp	3/2/2019 4:46 PM	TMP File
scan2.tmp	3/2/2019 4:46 PM	TMP File
scan3.tmp	3/2/2019 4:46 PM	TMP File
schtasks-backdoor	3/2/2019 4:37 PM	Windows PowerS...
somethingwindows.dmp	3/2/2019 4:45 PM	DMP File
sys	3/2/2019 4:37 PM	Text Document
WMIBackdoor	3/2/2019 4:37 PM	Windows PowerS...
xCmd	3/2/2019 4:37 PM	Application

15 items 1 item selected 36.7 KB

- Pathway: C:/TMP/ms.ps1
- Action: Answered based on investigation clues.
- Finding: The tool used was Mimikatz.

6) Determined Attackers' External Control and Command Server IP



What tool was used to get Windows passwords?

Mimikatz

What was the attackers external control and command servers IP?

76.32.97.132

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

Answer format: .***

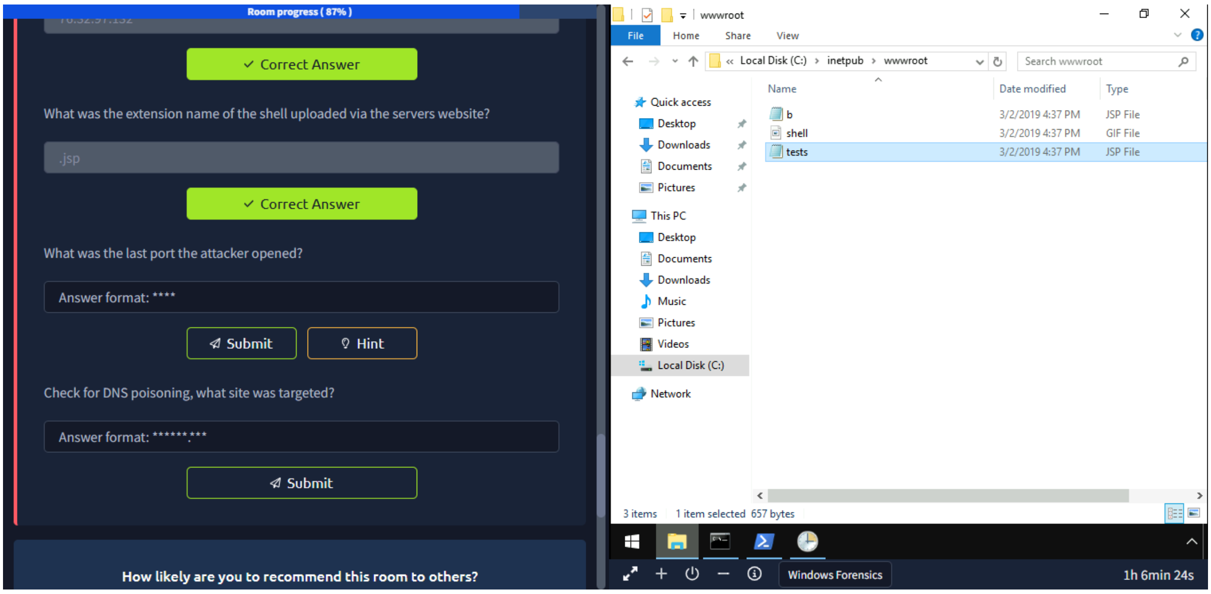
What was the last port the attacker opened?

Answer format: ****

```
# space.
#
# 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
```

- Pathway:C:/Windows/System32/drivers/etc/host
- Action: Inferred from context and provided answers.
- Finding: The IP was 76.32.97.132.

7)Identified Extension Name of the Shell Uploaded via Server Website



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

.jsp

What was the last port the attacker opened?

Answer format: ****

Check for DNS poisoning, what site was targeted?

Answer format: ******.***

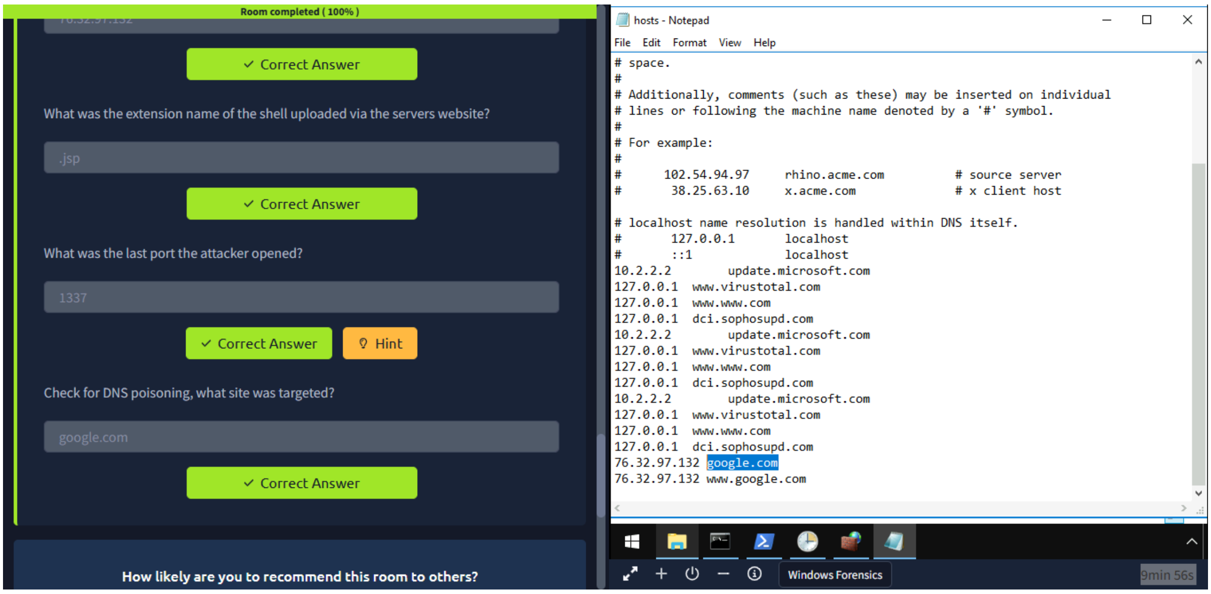
How likely are you to recommend this room to others?

Name	Date modified	Type
b	3/2/2019 4:37 PM	JSP File
shell	3/2/2019 4:37 PM	GIF File
tests	3/2/2019 4:37 PM	JSP File

3 items   1 item selected 657 bytes

- Pathway: This PC -> Local Disk (C:) -> inetpub -> wwwroot
- Action: Examined the uploaded files in the wwwroot directory.
- Finding: The extension name was .jsp.

8) Checked for DNS Poisoning and Targeted Site



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

.jsp

What was the last port the attacker opened?

1337

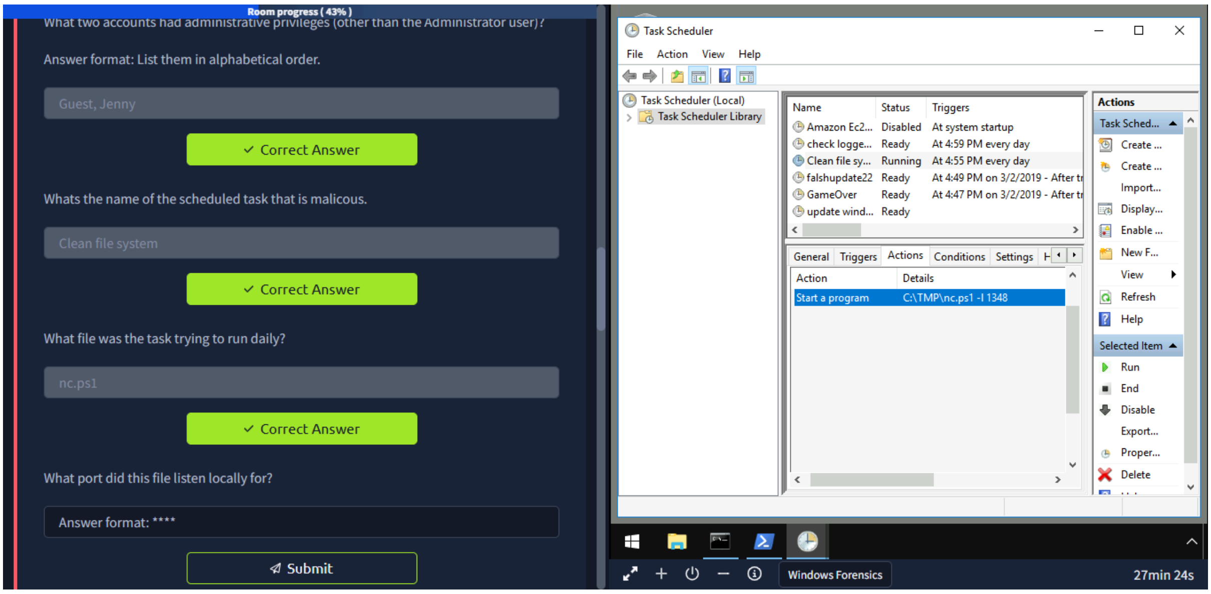
Check for DNS poisoning, what site was targeted?

google.com

```
# space.
#
# 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
```

- Pathway: Notepad -> hosts file
- Action: Reviewed the hosts file for malicious entries.
- Finding: DNS poisoning targeted google.com.

9) Identified File the Task Was Trying to Run Daily



Room progress (43%)

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

Answer format: List them in alphabetical order.

Guest, Jenny

✓ Correct Answer

Whats the name of the scheduled task that is malicous.

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?

Answer format: ****

Submit

Task Scheduler

File Action View Help

Task Scheduler (Local)
Task Scheduler Library

Name	Status	Triggers
Amazon Ec2...	Disabled	At system startup
check logge...	Ready	At 4:59 PM every day
Clean file sy...	Running	At 4:55 PM every day
falshupdate22	Ready	At 4:49 PM on 3/2/2019 - After tr
GameOver	Ready	At 4:47 PM on 3/2/2019 - After tr
update wind...	Ready	

General | Triggers | Actions | Conditions | Settings | H

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

- Pathway: Task Scheduler -> Task Scheduler Library -> nc - Notepad
- Action: Reviewed the task action details.
- Finding: The file was nc.ps1

Conclusion

You did it! 🎉 Investigating Windows complete!

Points earned	Completed tasks	Room type	Difficulty	Streak
480	1	Challenge	Easy	1

75,989 users are actively learning this week

Looking back at this TryHackMe CTF room "Investigating Windows," it’s been an eye-opening journey that really shows how upskilling can make a difference. Diving into the investigation—tracking down the attacker’s moves, spotting the malicious "Clean file system" task, and uncovering tools like Mimikatz—felt like piecing together a puzzle.For anyone thinking about upskilling, this experience shows it’s not just a resume booster—it’s a way to grow, stay curious, and make a real impact, one solved mystery at a time!