

# PSP0201

## Week 5

## Writeup

Group Name: ikun no 1

Members

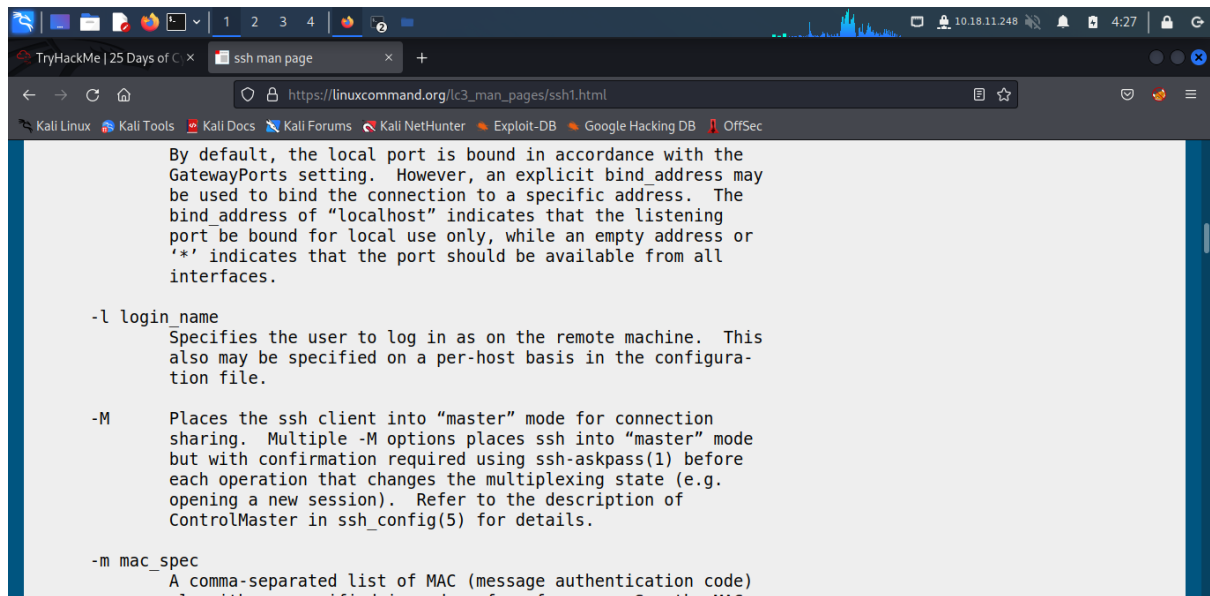
| ID         | Name                            | Role   |
|------------|---------------------------------|--------|
| 1211102058 | Chu Liang Chern                 | Leader |
| 1211101401 | Chong Jii Hong                  | Member |
| 1211103206 | Ng Kai Keat                     | Member |
| 1211103095 | Siddiq Ferhad Bin Khairil Anual | Member |

## Day 20: Blue Teaming PowershellELIF to the rescue

Tool used: Kali-Linux

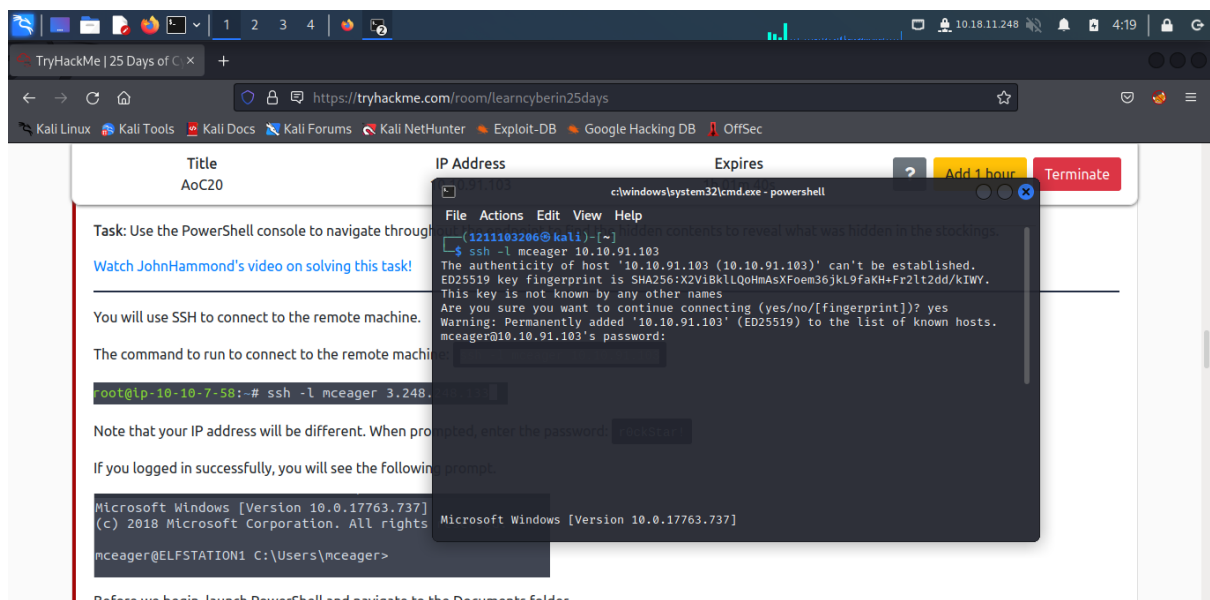
Solution/walkthrough:

### Question 1



Google search the answer.

### Question 2



First login the account with ssh.

**Title**  
Aoc20

**IP Address**  
10.10.91.1

PowerShell has grown in popularity in the last few years among those who have heard of PowerShell but never dabbled with it, fret not, today we will learn how to use it.

Recall from the definition above that PowerShell is a command-line shell. We must tell PowerShell what to do. PowerShell commands are known as cmdlets. To list the contents of the current directory we are in, we can use the `Get-ChildItem` cmdlet. We can also enhance its capabilities further.

- Path** Specifies a path to one or more locations. Wildcards can be used.
- File / -Directory** To get a list of files, use the `File` parameter with `File` and/or `Directory` parameters.
- Filter** Specifies a filter to qualify the `Path` parameter.
- Recurse** Gets the items in the specified locations and all subdirectories.
- Hidden** To get only hidden items, use the `Hidden` parameter.
- ErrorAction SilentlyContinue** Specifies what action to take if the command encounters an error.

For example, if you want to view all of the hidden files in the current directory you are in, you can issue the following command:

```
Get-ChildItem -File -Hidden -ErrorAction SilentlyContinue
```

Then, Is it and set location to the Documents file.

**Title**  
Aoc20

**IP Address**  
10.10.91.1

Note: You can always use the `Get-Help` cmdlet to get help on any cmdlet.

**Answer the questions below**

Search for the first hidden elf file within the Documents folder.

Answer format: \*\*\*\*\*

Search on the desktop for a hidden folder that contains the file 'elfone.txt'. Read the contents of this file. What is the name of that movie that Elf 2 wants?

Answer format: \*\*\*\*\*

Search the Windows directory for a hidden folder that contains the file 'elfone.txt'. What is the name of the hidden folder? (This command will take a while)

Answer format: \*\*\*\*\*

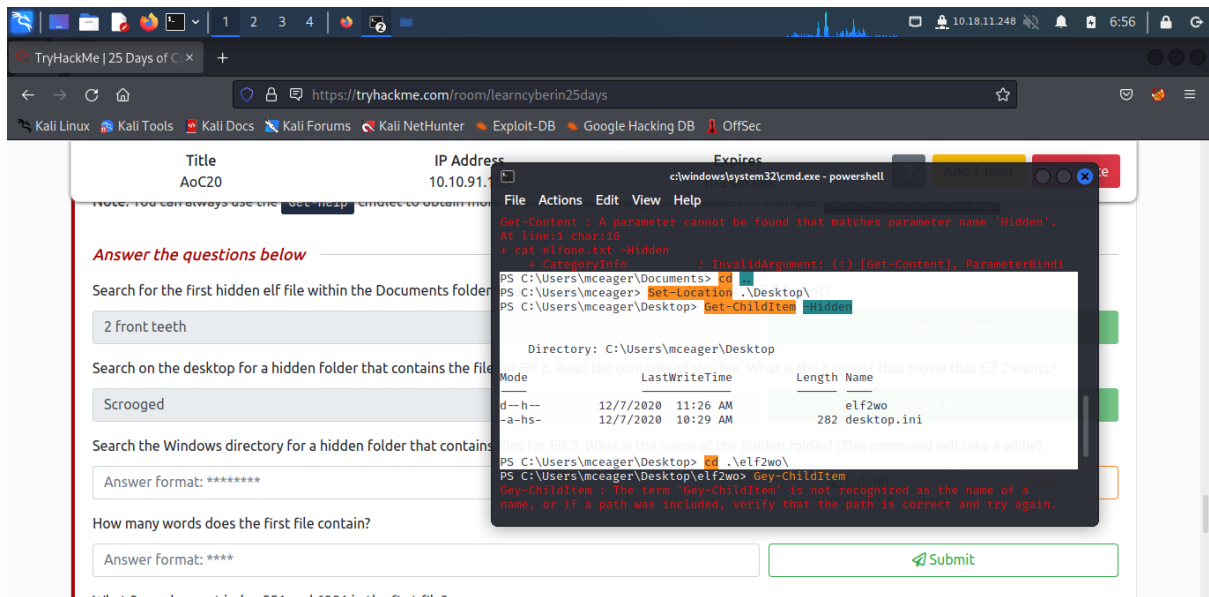
How many words does the first file contain?

Answer format: \*\*\*\*

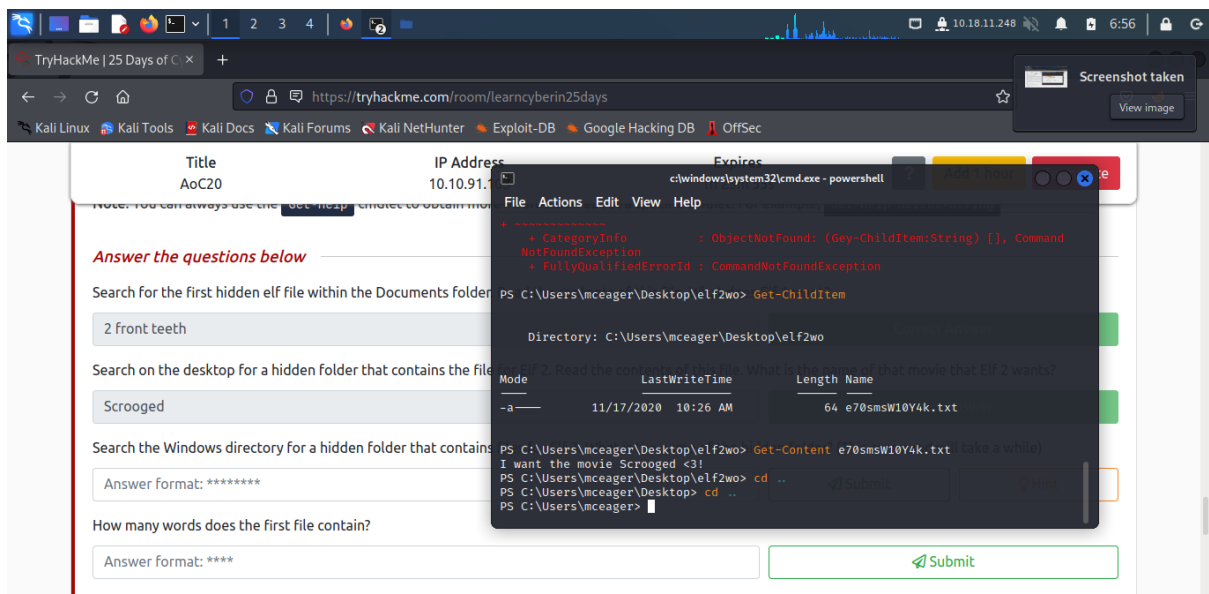
**Submit**

Get the file with Get-ChildItem and add -File -Hidden to get the hidden file. Lastly, get the content and the answer shown.

### Question 3

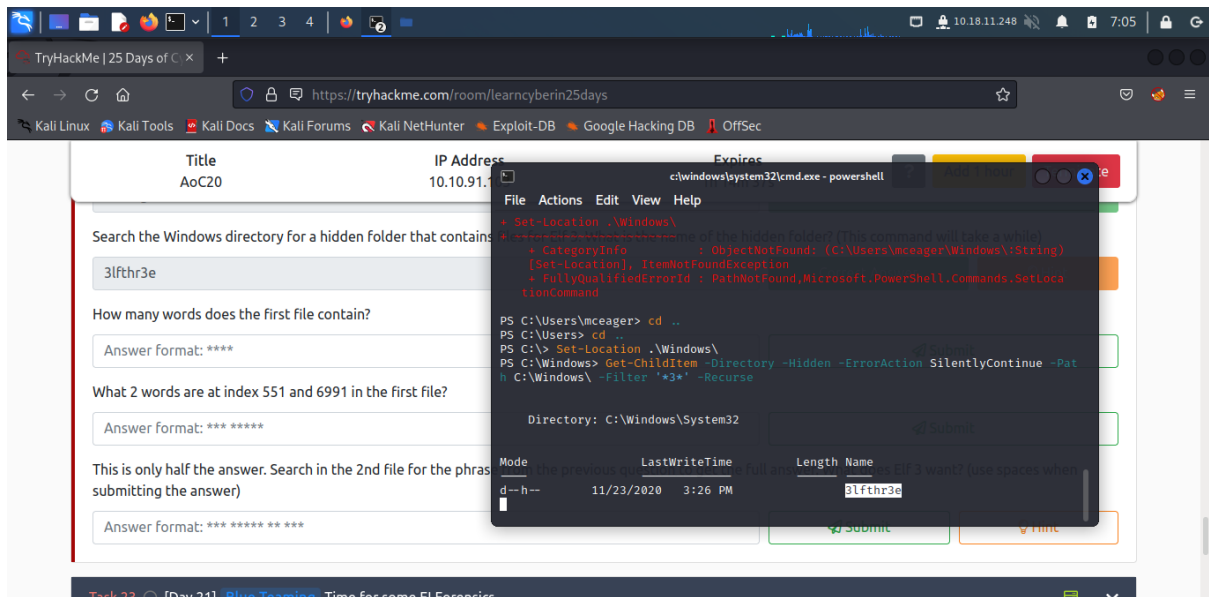


Set location to desktop and list the file with -Hidden.



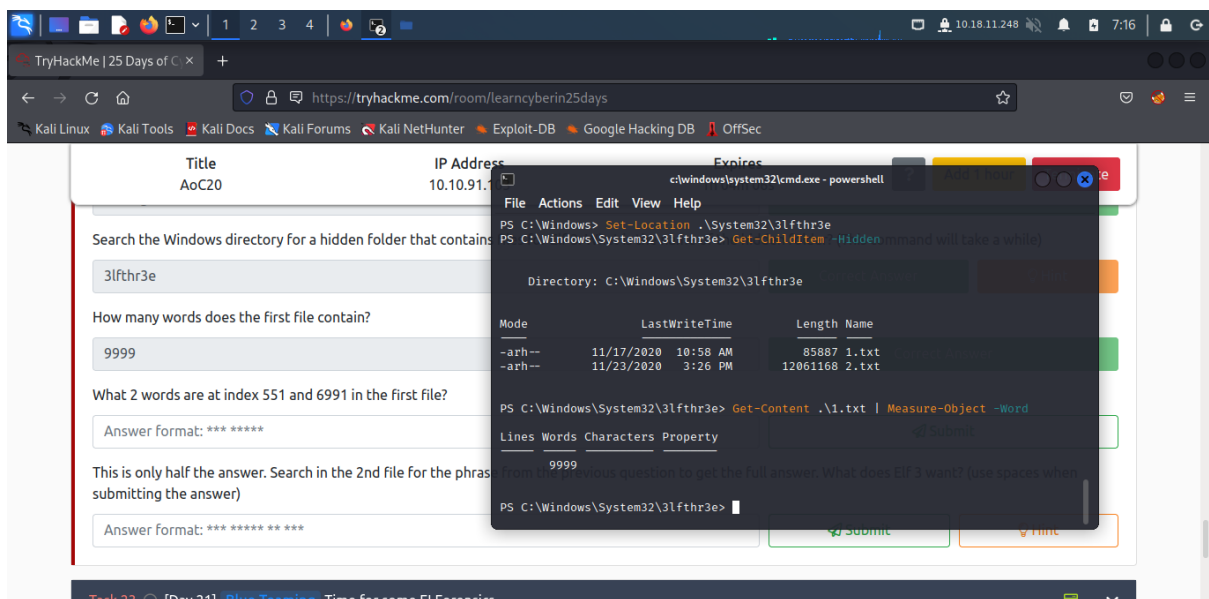
Then, Is the directory and cat the txt and the answer shown.

#### Question 4



Set the location to windows and filter it. Then, the answer shown.

### Question 5



Set location to the 3lfthr3e and ls it with hidden. Next, use Measure Object to word count the txt. Then, the answer shown.

### Question 6

The screenshot shows a web browser window at <https://tryhackme.com/room/learnncyberin25days>. The page displays a challenge titled 'AoC20' with an IP address of 10.10.91.1. The challenge instructions are as follows:

- Search the Windows directory for a hidden folder that contains files for Ell 3. What is the name of the hidden folder? (This command will take a while)
- How many words does the first file contain?
- What 2 words are at index 551 and 6991 in the first file?

Input fields for these questions are present, with the first containing '3lfthr3e' and the second containing '9999'. A terminal window is overlaid on the page, showing the following commands and output:

```

c:\windows\system32\cmd.exe - powershell
Directory: C:\Windows\System32\3lfthr3e
Mode                LastWriteTime         Length Name
----                -
-arh--             11/17/2020   10:58 AM           85887 1.txt
-arh--             11/23/2020    3:26 PM       12061168 2.txt

PS C:\Windows\System32\3lfthr3e> Get-Content .\1.txt | Measure-Object -Word
Lines Words Characters Property
-----
9999

PS C:\Windows\System32\3lfthr3e> (Get-Content .\1.txt)[551]
Red
PS C:\Windows\System32\3lfthr3e> (Get-Content .\1.txt)[6991]
want? (use spaces when
Ryder
PS C:\Windows\System32\3lfthr3e>
  
```

Use `(Get-Content -Path file.txt)[index]` to get the exact position. Then, the answer shown.

## Question 7

The screenshot shows the same TryHackMe room interface. The terminal window now displays additional commands and output:

```

PS C:\Windows\System32\3lfthr3e> Get-Content .\1.txt | Measure-Object -Word
Lines Words Characters Property
-----
9999

PS C:\Windows\System32\3lfthr3e> (Get-Content .\1.txt)[551]
Red
PS C:\Windows\System32\3lfthr3e> (Get-Content .\1.txt)[6991]
want? (use spaces when
Ryder
PS C:\Windows\System32\3lfthr3e> Select-String .\2.txt -Pattern "redryder"
2.txt:558704:redryderbbgun
PS C:\Windows\System32\3lfthr3e>
  
```

The background page shows instructions for using `Get-Content`, `Set-Location`, and `Select-String` cmdlets. A note at the bottom states: "Note: You can always use the `Get-Help` cmdlet to obtain more information about a specific cmdlet. For example, `Get-Help Select-String`".

Use `select string` to find the phrase.