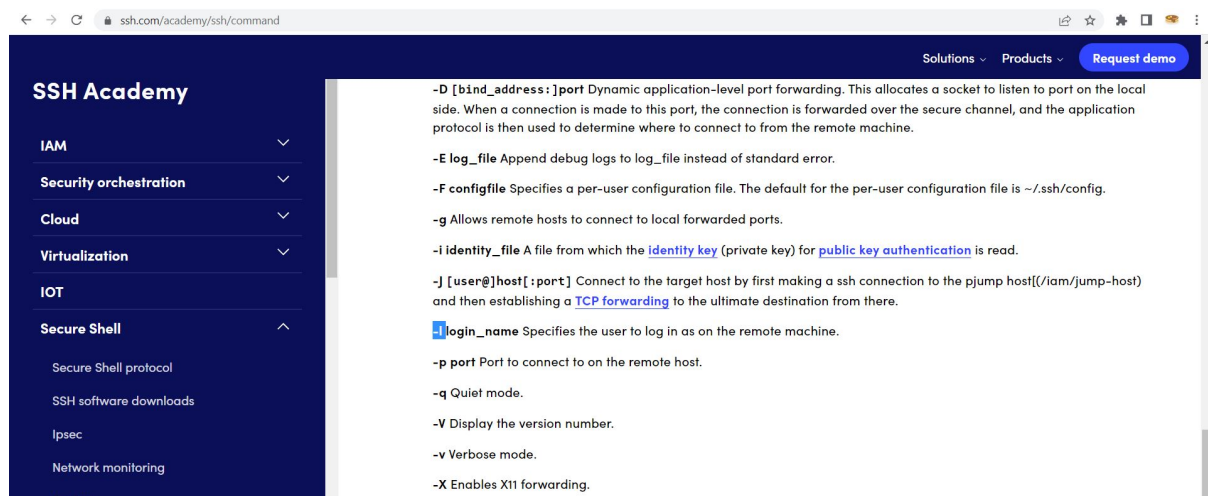


Day 20 - [Blue Teaming] Powershell to the rescue

Tool Used: Kali Linux, firefox, PowerShell

Solution/walkthrough:

Q1

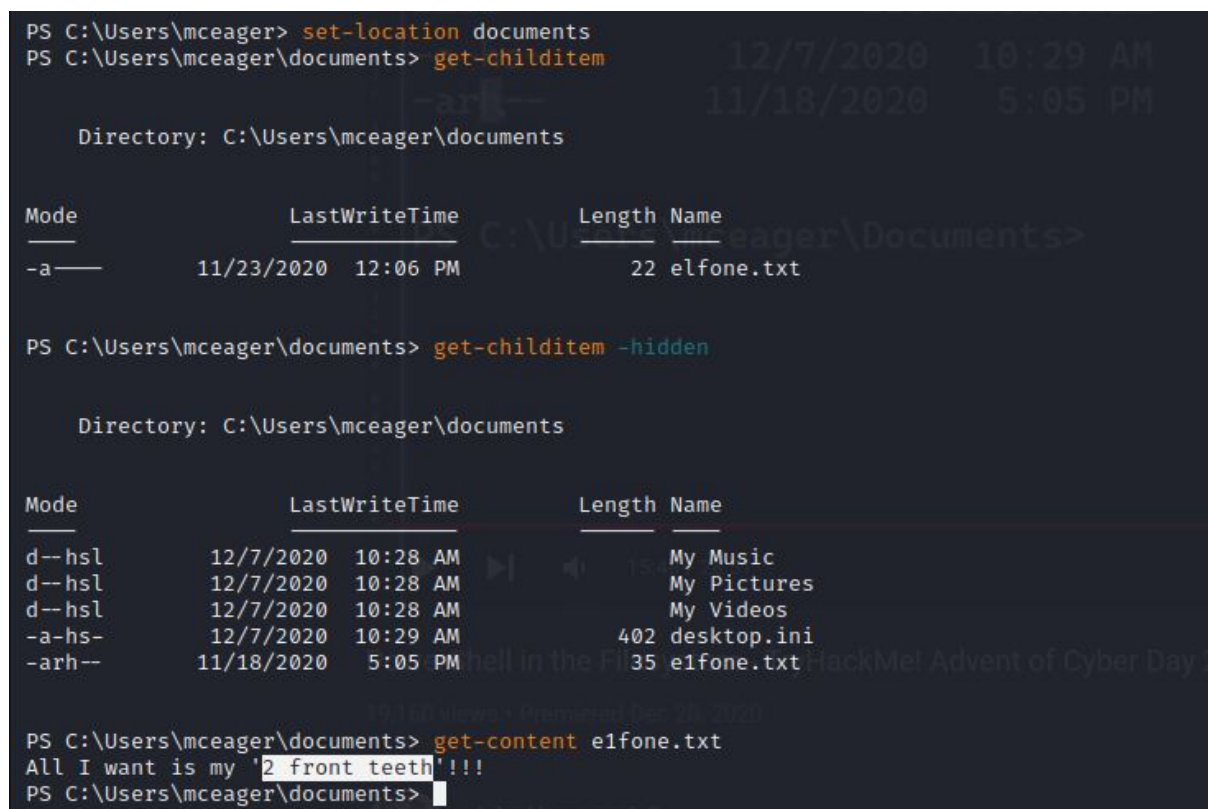


The screenshot shows the SSH Academy website. On the left is a navigation menu with categories: IAM, Security orchestration, Cloud, Virtualization, IOT, and Secure Shell (expanded). Under Secure Shell, there are links for Secure Shell protocol, SSH software downloads, Ipsec, and Network monitoring. The main content area lists SSH command options:

- D [bind_address:]port Dynamic application-level port forwarding. This allocates a socket to listen to port on the local side. When a connection is made to this port, the connection is forwarded over the secure channel, and the application protocol is then used to determine where to connect to from the remote machine.
- E log_file Append debug logs to log_file instead of standard error.
- F configfile Specifies a per-user configuration file. The default for the per-user configuration file is ~/.ssh/config.
- g Allows remote hosts to connect to local forwarded ports.
- i identity_file A file from which the identity key (private key) for public key authentication is read.
- J [user@]host[:port] Connect to the target host by first making a ssh connection to the jump host[/iam/jump-host] and then establishing a TCP forwarding to the ultimate destination from there.
- l login_name Specifies the user to log in as on the remote machine.
- p port Port to connect to on the remote host.
- q Quiet mode.
- V Display the version number.
- v Verbose mode.
- X Enables X11 forwarding.

search from google.

Q2



```
PS C:\Users\mceager> set-location documents
PS C:\Users\mceager\documents> get-childitem

Directory: C:\Users\mceager\documents

Mode                LastWriteTime         Length Name
----                -
-a-----         11/23/2020   12:06 PM             22 elfone.txt

PS C:\Users\mceager\documents> get-childitem -hidden

Directory: C:\Users\mceager\documents

Mode                LastWriteTime         Length Name
----                -
d--hsl             12/7/2020   10:28 AM             My Music
d--hsl             12/7/2020   10:28 AM             My Pictures
d--hsl             12/7/2020   10:28 AM             My Videos
-a-hs-             12/7/2020   10:29 AM           402 desktop.ini
-arh--             11/18/2020    5:05 PM           35 elfone.txt

PS C:\Users\mceager\documents> get-content elfone.txt
All I want is my '2 front teeth'!!!
PS C:\Users\mceager\documents>
```

connect to the machine. get into the document folder with [set-location]command. then, use [get-childitem] command with [-hidden]parameter to view the hidden file. then use [get-content] command to read the contents of e1fone.txt. then we can know what elf 1 wants.

Q3

```

PS C:\Users\mceager\Desktop> get-childitem
PS C:\Users\mceager\Desktop> get-childitem -hidden

Directory: C:\Users\mceager\Desktop

Mode                LastWriteTime         Length Name
----                -
d--h--             12/7/2020 11:26 AM              elf2wo
-a-hs-             12/7/2020 10:29 AM          282 desktop.ini

PS C:\Users\mceager\Desktop> cd elf2wo
PS C:\Users\mceager\Desktop\elf2wo> cat e70smw10Y4k.txt
movie: Scrapped - 31

PS C:\Users\mceager\Desktop\elf2wo> get-childitem

Directory: C:\Users\mceager\Desktop\elf2wo

Mode                LastWriteTime         Length Name
----                -
-a--              11/17/2020 10:26 AM           64 e70smw10Y4k.txt

PS C:\Users\mceager\Desktop\elf2wo> get-content *.txt
PS C:\Users\mceager\Desktop\elf2wo> get-content e70smw10Y4k.txt
I want the movie Scrapped - 31
PS C:\Users\mceager\Desktop\elf2wo>

```

get into the desktop using [set-location]command. then search for a hidden folder with [get-childitem] command with [-hidden]parameter. After that, get into the hidden folder, and read the contents, then we can know what elf 2 wants.

Q4

```

PS C:\windows> get-childitem -filter '*3*'

Directory: C:\windows

Mode                LastWriteTime         Length Name
----                -
d-----             7/16/2022  9:09 AM              System32
d-----             9/15/2018 12:19 AM              twain_32
-a-----             9/15/2018 12:13 AM          64512 twain_32.dll
-a-----             9/15/2018 12:13 AM          11776 winhlp32.exe

PS C:\windows> set-location system32

PS C:\windows\system32> get-childitem -hidden -directory -filter '*3*'

Directory: C:\windows\system32

Mode                LastWriteTime         Length Name
----                -
d--h--             11/23/2020  3:26 PM              3lfthr3e

```

get into the Windows directory. search for the directory containing '3' . Then we get into the system32, and do further search with [-filter] command to filter out the folder containing 3. we successfully found it on our first search.

Q5

```
PS C:\windows\system32\3lfthr3e> get-childitem -hidden
Directory: C:\windows\system32\3lfthr3e

Mode                LastWriteTime         Length Name
----                -
-arh-- the re 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
```

in the folder we have found, search for hidden files. Then we can do word count with [Get-Content -Path file.txt | Measure-Object -Word] command from Try Hack Me, modify it to match our use. we can get the number of words after running the command.

Q6

```
PS C:\windows\system32\3lfthr3e> (Get-Content 1.txt)[551]
Red
PS C:\windows\system32\3lfthr3e> (Get-Content 1.txt)[6991]
Ryder
PS C:\windows\system32\3lfthr3e>
```

We use (Get-Content -Path file.txt)[index] command from Try Hack Me to find the exact position of a string in the file. Replace the [index] with the index provided in the question to find out the string.

Q7

```
PS C:\windows\system32\3lfthr3e> (Get-Content 1.txt)[551]
Red
PS C:\windows\system32\3lfthr3e> (Get-Content 1.txt)[6991]
Ryder
PS C:\windows\system32\3lfthr3e> Select-String 2.txt -Pattern 'redryder'

2.txt:558704:redryderbbgun
```

with the 2 strings found from the previous question, we follow the guide from the question. we search the 2nd file with the 'redryder' string, and we can find out the elf 3 wants.