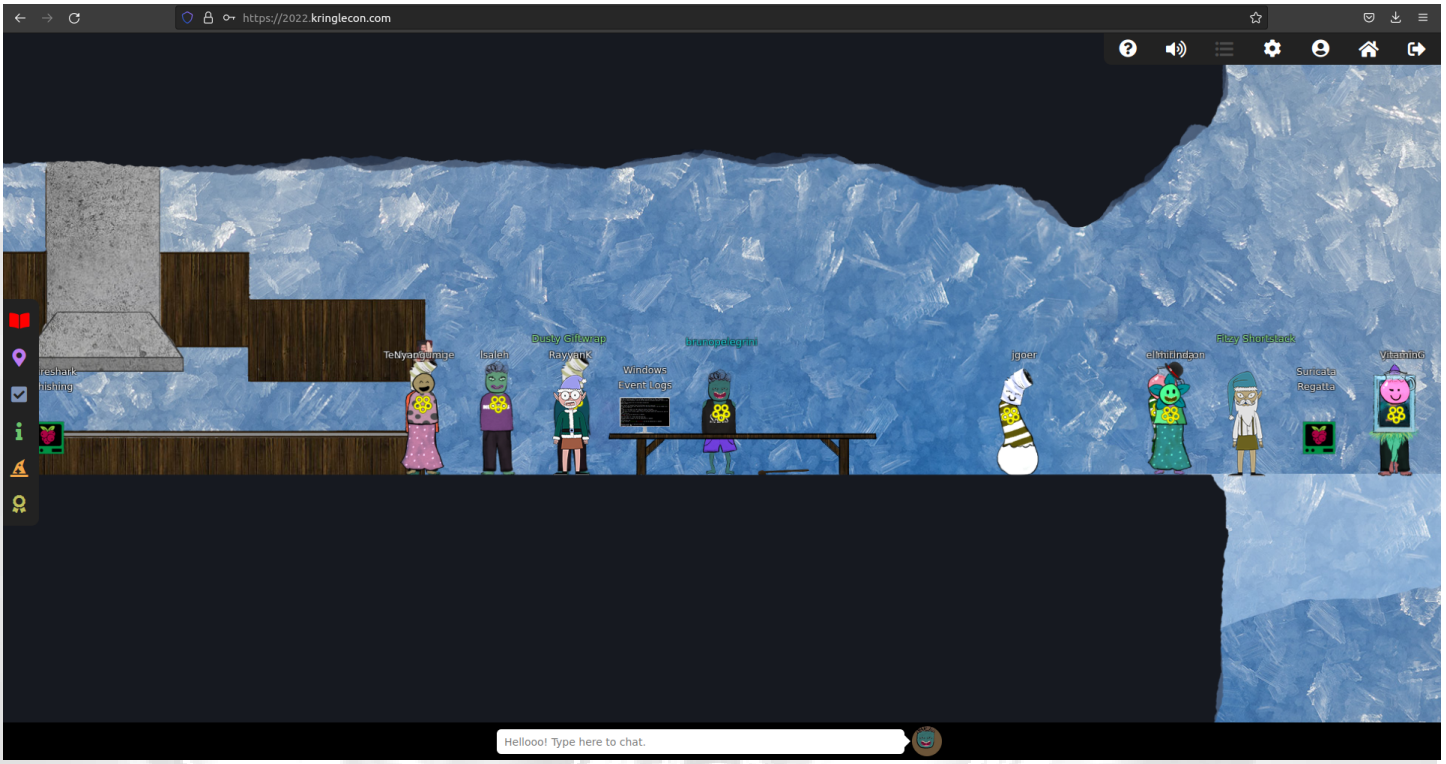
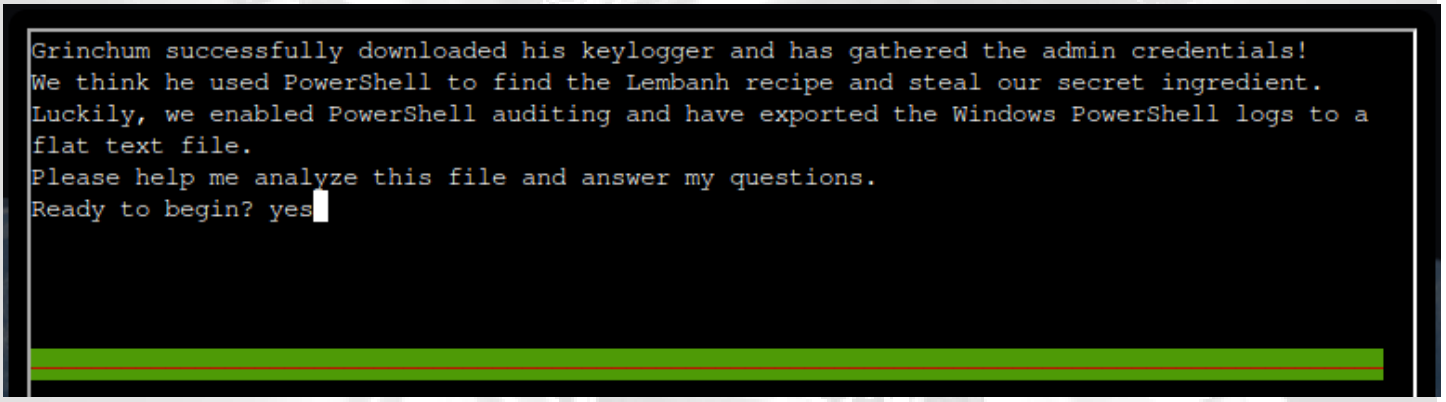
Write-up CTF
SANS - Holiday Hack Challenge 2022
Challenge: Windows Event Logs
Difficulty: Easy
https://github.com/brunopelegrini

First of all, open the Objectives session in the left menu. For this challenge, we have the event log file to analyze. Download this file.

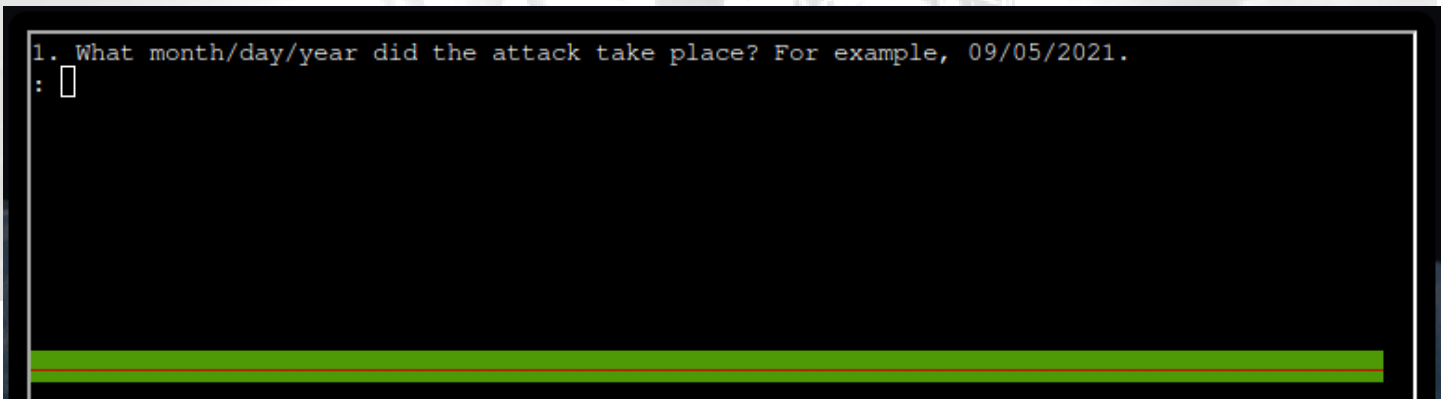
In the Kringlecon game, go to Tokien Ring tunnels and search for Wireshark Phishing Terminal, then connect.



The Terminal will show two sessions. In the above session is where you'll insert your answers.
Then type **“Yes”** to continue.



Now the first question about the challenge is shown.



@badposeidon1
https://github.com/brunopelegrini

Looking for a directory, I found the “Powershell.evtx.log”, we’ll look for it!

```
elf@4965d68bad74:~$ ls -lah
total 3.0M
drwxr-xr-x 1 elf  elf  4.0K Dec 21 21:29 .
drwxr-xr-x 1 root root 4.0K Dec 21 21:29 ..
-rw-r--r-- 1 elf  elf   220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 elf  elf  3.9K Dec 21 21:29 .bashrc
-rw-r--r-- 1 elf  elf   807 Feb 25  2020 .profile
-rw-r--r-- 1 root root  814 Dec  9 00:55 HELP
-rw-r--r-- 1 root root 3.0M Nov 28 22:21 powershell.evtx.log
elf@4965d68bad74:~$
```

Opening the log, I was faced with a lot of garbage.
I used the command grep to find any actions to evidence that the endpoint is compromised, so then I searched for simple commands involved in the enumeration phase, example ipconfig, hostname, whoami.
In this case I used the parameters -A and -B to specify the number of lines after and before string search.

```
elf@e2a942e8780b:~$ grep "whoami" -A 10 -B 10 powershell.evtx.log


User Data:

"
Verbose 12/24/2022 2:56:27 AM   Microsoft-Windows-PowerShell    4106    Stopping Command  "
Completed invocation of ScriptBlock ID: c8b1e019-beab-49cd-8281-51e1207b5a78
Runspace ID: 4181eda9-20e6-4eb9-8869-fe5fa6d5e663"
Verbose 12/24/2022 2:56:27 AM   Microsoft-Windows-PowerShell    4105    Starting Command  "
Started invocation of ScriptBlock ID: c8b1e019-beab-49cd-8281-51e1207b5a78
Runspace ID: 4181eda9-20e6-4eb9-8869-fe5fa6d5e663"
Verbose 12/24/2022 2:56:27 AM   Microsoft-Windows-PowerShell    4104    Execute a Remote Co
mmand   "Creating Scriptblock text (1 of 1):
whoami
```

we can see the command “whoami” was performed in powershell on 12/24/2022, so then I type this in terminal.

```
1. What month/day/year did the attack take place? For example, 09/05/2021.
: 12/24/2022
```

Now, we have question number 2.

```
2. An attacker got a secret from a file. What was the original file's name?
:
```

For the next question we have the hint:

```
Hint 1: https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.management
/add-content?view=powershell-7.3
2. An attacker got a secret from a file. What was the original file's name?
:
```

Based in the hint, I decided to look for the command “Add-”, so I have the return below.

```
elf@529c13add73c:~$ grep "Add-" powershell.evtx.log | sort -u                    [80/1232]
        Command Name = Add-Content
        Command Name = Add-Member
$foo = Get-Content .\Recipe| % {$_ -replace 'honey', 'fish oil'} $foo | Add-Content -Path '
recipe_updated.txt'
$foo = Get-Content .\Recipe| % {$_-replace 'honey','fish oil'} $foo | Add-Content -Path 're
cipe_updated.txt'
$foo | Add-Content -Path 'Recipe'
$foo | Add-Content -Path 'Recipe.txt'
$foo | Add-Content -Path 'recipe_updated.txt'
```

Based on the results, I typed in the terminal the value “Recipe”.

```
Hint 1: https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.management
/add-content?view=powershell-7.3
2. An attacker got a secret from a file. What was the original file's name?
: Recipe
```

Now, we have question number 3.

```
3. The contents of the previous file were retrieved, changed, and stored to a variable by t
he attacker. This was done multiple times. Submit the last full PowerShell line that perfor
med only these actions.
:
```

Looking at the same result it is possible to find the command.

```
$foo = Get-Content .\Recipe| % {$_-replace 'honey','fish oil'} $foo | Add-Content [75/1232]
cipe_updated.txt'
```

I type it in my terminal.

```
3. The contents of the previous file were retrieved, changed, and stored to a variable by t
he attacker. This was done multiple times. Submit the last full PowerShell line that perfor
med only these actions.
: $foo = Get-Content .\Recipe| % {$_ -replace 'honey', 'fish oil'} $foo | Add-Content -Path
 'recipe_updated.txt'
```

Now, we have question number 4.

```
4. After storing the altered file contents into the variable, the attacker used the variabl
e to run a separate command that wrote the modified data to a file. This was done multiple
times. Submit the last full PowerShell line that performed only this action.
:
```

At this moment, I get the variable set by the attacker, looking at this first line, it is a reference to the last command executed.

```
elf@529c13add73c:~$ grep "\$foo" powershell.evtx.log
$foo | Add-Content -Path 'Recipe'
$foo | Add-Content -Path 'Recipe.txt'
$foo = Get-Content .\Recipe| % {$_ -replace 'honey', 'fish oil'}
$foo | Add-Content -Path 'Recipe.txt'
$foo = Get-Content .\Recipe| % {$_-replace 'honey','fish oil'}
$foo | Add-Content -Path 'Recipe.txt'
$foo | Add-Content -Path 'recipe_updated.txt'
$foo = Get-Content .\Recipe| % {$_-replace 'honey','fish oil'}
$foo = Get-Content .\Recipe| % {$_-replace 'honey','fish oil'} $foo | Add-Content -Path 're
cipe_updated.txt'
$foo = Get-Content .\Recipe| % {$_ -replace 'honey', 'fish oil'} $foo | Add-Content -Path '
recipe_updated.txt'
elf@529c13add73c:~$
```

Then, I type it in my terminal.

```
4. After storing the altered file contents into the variable, the attacker used the variabl
e to run a separate command that wrote the modified data to a file. This was done multiple
times. Submit the last full PowerShell line that performed only this action.
: $foo | Add-Content -Path 'Recipe'
```

Now, we have question number 5.

```
5. The attacker ran the previous command against one file multiple times. What is the name
of this file?
:
```

Looking at the results, I tried to type Recipe.txt in my terminal.

```
elf@529c13add73c:~$ grep "\$foo" powershell.evtx.log
$foo | Add-Content -Path 'Recipe'
$foo | Add-Content -Path 'Recipe.txt'
$foo = Get-Content .\Recipe| % {$_ -replace 'honey', 'fish oil'}
$foo | Add-Content -Path 'Recipe.txt'
$foo = Get-Content .\Recipe| % {$_-replace 'honey','fish oil'}
$foo | Add-Content -Path 'Recipe.txt'
$foo | Add-Content -Path 'recipe_updated.txt'
$foo = Get-Content .\Recipe| % {$_-replace 'honey','fish oil'}
$foo = Get-Content .\Recipe| % {$_-replace 'honey','fish oil'} $foo | Add-Content -Path 're
cipe_updated.txt'
$foo = Get-Content .\Recipe| % {$_ -replace 'honey', 'fish oil'} $foo | Add-Content -Path '
recipe_updated.txt'
elf@529c13add73c:~$
```

```
5. The attacker ran the previous command against one file multiple times. What is the name
of this file?
: Recipe.txt
```

Now, we have question number 6.

```
6. Were any files deleted? (Yes/No)
:
```

For question number 6, I searched the string “Remove”, then I found some lines about this.

```
elf@529c13add73c:~$ grep "Remove" powershell.evtx.log
ParameterBinding(Out-Default): name=""InputObject""; value=""\\DESKTOP-R65OKRB\ROOT\cimv2:W
in32_RemoveIniAction""
ParameterBinding(Out-Default): name=""InputObject""; value=""\\DESKTOP-R65OKRB\ROOT\cimv2:W
in32_RemoveFileAction""
Information     12/24/2022 3:05:51 AM   Microsoft-Windows-PowerShell    4103    Executing P
ipeline "CommandInvocation(Remove-Item): ""Remove-Item""
ParameterBinding(Remove-Item): name=""Path""; value="".\recipe_updated.txt""
        Command Name = Remove-Item
Information     12/24/2022 3:05:42 AM   Microsoft-Windows-PowerShell    4103    Executing P
ipeline "CommandInvocation(Remove-Item): ""Remove-Item""
ParameterBinding(Remove-Item): name=""Path""; value="".\Recipe.txt""
```

Then I answered “yes”.

```
6. Were any files deleted? (Yes/No)
: Yes
```

Now, we have question number 7.

```
7. Was the original file (from question 2) deleted? (Yes/No)
: 
```

Looking at this block of logs, I can't see the Recipe file, so I insert in my terminal the option "No".

```
in32_RemoveFileAction""
Information     12/24/2022 3:05:51 AM   Microsoft-Windows-PowerShell    4103    Executing P
ipeline "CommandInvocation(Remove-Item): ""Remove-Item""
ParameterBinding(Remove-Item): name=""Path""; value="".\recipe_updated.txt""
        Command Name = Remove-Item
Information     12/24/2022 3:05:42 AM   Microsoft-Windows-PowerShell    4103    Executing P
ipeline "CommandInvocation(Remove-Item): ""Remove-Item""
ParameterBinding(Remove-Item): name=""Path""; value="".\Recipe.txt""
        Command Name = Remove-Item
```

```
7. Was the original file (from question 2) deleted? (Yes/No)
: NO
```

Now, we have question number 8.

```
8. What is the Event ID of the logs that show the actual command lines the attacker typed a
nd ran?
: 
```

To the file Recipe.txt the last command in the log refers to event 4104.
So, I type it in my terminal.

```
8. What is the Event ID of the logs that show the actual command lines the attacker typed a
nd ran?
: 4104
```

Now, we have question number 9.

```
9. Is the secret ingredient compromised (Yes/No)?
: 
```

Looking at the results, we found the sequence below.

```
Completed invocation of ScriptBlock ID: 8e5b9d7d-e1ff-40bc-8727-49ae9530af02       [10/924]
Runspace ID: 4181eda9-20e6-4eb9-8869-fe5fa6d5e663"
Information     12/24/2022 3:03:56 AM   Microsoft-Windows-PowerShell    4103    Executing P
ipeline "CommandInvocation(Add-Content): ""Add-Content""
ParameterBinding(Add-Content): name=""Path""; value=""Recipe.txt""
ParameterBinding(Add-Content): name=""Value""; value=""Recipe from Mixolydian, the Queen of
 Dorian""
ParameterBinding(Add-Content): name=""Value""; value=""Lembanh Original Recipe""
ParameterBinding(Add-Content): name=""Value""; value="" ""
ParameterBinding(Add-Content): name=""Value""; value=""2 1/2 all purpose flour""
ParameterBinding(Add-Content): name=""Value""; value=""1 Tbsp baking powder""
ParameterBinding(Add-Content): name=""Value""; value=""1/4 tsp salt""
ParameterBinding(Add-Content): name=""Value""; value=""1/2 c  butter""
ParameterBinding(Add-Content): name=""Value""; value=""1/3 c brown sugar""
ParameterBinding(Add-Content): name=""Value""; value=""1 tsp cinnamon""
ParameterBinding(Add-Content): name=""Value""; value=""1/2 tsp fish oil (secret ingredient)
""
--
        Connected User =
        Shell ID = Microsoft.PowerShell
```

Then, my answer is “Yes”.

```
9. Is the secret ingredient compromised (Yes/No)?
: Yes
```

Now, we have question number 10.

```
10. What is the secret ingredient?
:
```

Using the command grep to find the string “secret” I found the ingredient honey.

```
elf@70ffa8812da8:~$ grep "secret" -A 10 -B 10 powershell.evtx.log
ParameterBinding(ForEach-Object): name=""InputObject""; value=""1/4 tsp salt""
ParameterBinding(ForEach-Object): name=""InputObject""; value=""1/2 c  butter""
ParameterBinding(ForEach-Object): name=""InputObject""; value=""1/3 c brown sugar""
ParameterBinding(ForEach-Object): name=""InputObject""; value=""1 tsp cinnamon""
ParameterBinding(ForEach-Object): name=""InputObject""; value=""1/2 tsp honey (secret ingre
dient)""
ParameterBinding(ForEach-Object): name=""InputObject""; value=""2/3 c heavy whipping cream"
"
```

So, I type it in my terminal.

```
10. What is the secret ingredient?
: honey
```

And finally, we finished this challenge.