



目 次

1. 試験にログイン
2. Running windows Script
3. VM接続
4. report 提出

1. 試験にログイン

- 試験前日にIDとMD5は送られる。
- ログインは試験開始の15分にログイン可能
- ログイン後試験管とチャットが可能ですぐに準備に入ることが出来た。
- その後は <https://help.offsec.com/hc/en-us/articles/360050299352-Proctoring-ToolManual> の資料の通り実施（画面共有）

ステップ1：ログイン

次のURLにログインしてください: <https://proctoring.offensive-security.com/Student/login>

LOGIN

OSID

MD5

LOGIN

Please enter only the numeric portion of your OSID. If you are unable to login and it is 15 minutes or less before your exam start time, please contact proctoring@offensive-security.com

OSIDを入力してください

- MD5を入力してください
- ログインをクリック
- ログインできない場合は、OSIDを添えてproctoring@offensive-security.comまでご連絡ください。

2. Running windows Script

- 試験開始時に、担当の試験監督官からホスト端末のOSを聞かれ、「windows」と回答したら、Windowsスクリプトのリンクが送信される。Windowsスクリプトを実行するには、送信されたリンクをclick
- スクリプト/コードをコピーする。

The screenshot shows a web browser window with the URL <https://paste.offsec.com/?d7b3bedd63fda290#5QHriaMeX9K2o5oDLMGVz3SxR9976n2vJkRh...>. The page displays a PowerShell script with a warning message: "🔥 このドキュメントは2日後に失効します。". Below the message, it says "To copy document press on the copy button or use the clipboard shortcut **Ctrl + c / Cmd + c**". A red box highlights the copy icon (a clipboard icon with a 'C') on the right side of the code area. The script itself is a multi-line PowerShell command.

```
$output = Get-NetTCPConnection | Select-Object LocalAddress, LocalPort, RemoteAddress, RemotePort, State, OwningProcess, @n='ProcessName';e={(Get-Process -Id $_.OwningProcess).ProcessName} | format-table
$output += Get-Process
$output += Get-WmiObject -Class Win32_product | format-table
$output += Get-WmiObject -Class win32_physicalmemory | format-table
$output += Get-WmiObject Win32_VideoController
$output += systeminfo | format-table
$output += Get-ItemProperty "HKCU:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store"
Write-Output $output |clip
Write-Host "Data Copied to your clipboard, please paste this data in a new paste at paste.offse.com (don't copy the url!)" -ForegroundColor Green
```

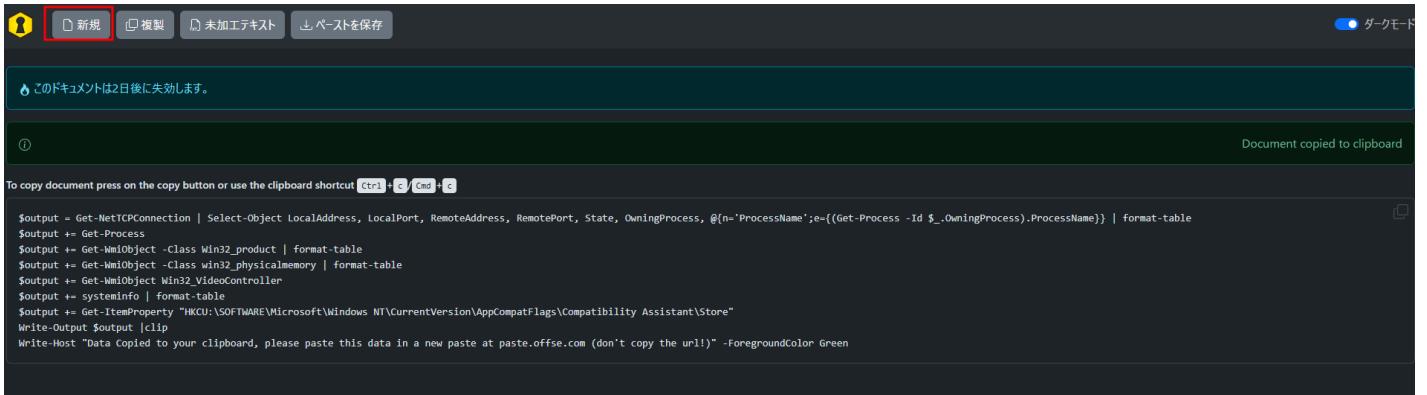
- copyしたらPowerShellを起動させ、scriptを実行

The screenshot shows a PowerShell terminal window with the following command history:
PS C:\Windows\system32> \$output = Get-NetTCPConnection | Select-Object LocalAddress, LocalPort, RemoteAddress, RemotePort, State, OwningProcess, @n='ProcessName';e={(Get-Process -Id \$_.OwningProcess).ProcessName} | format-table
>> \$output += Get-Process
>> \$output += Get-WmiObject -Class Win32_product | format-table
>> \$output += Get-WmiObject -Class win32_physicalmemory | format-table
>> \$output += Get-WmiObject Win32_VideoController
>> \$output += systeminfo | format-table
>> \$output += Get-ItemProperty "HKCU:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store"
>> Write-Output \$output |clip
>> Write-Host "Data Copied to your clipboard, please paste this data in a new paste at paste.offse.com (don't copy the url!)" -ForegroundColor Green
>>
Data Copied to your clipboard, please paste this data in a new paste at paste.offse.com (don't copy the url!)
PS C:\Windows\system32>
PS C:\Windows\system32>

⚠※※※ 重要 ※※※

出力は自動的にクリップボードにコピーされる。

4. 新規を選択する



このドキュメントは2日後に失効します。

To copy document press on the copy button or use the clipboard shortcut **Ctrl + C / Cmd + C**

```
$output = Get-NetTCPConnection | Select-Object LocalAddress, LocalPort, RemoteAddress, RemotePort, State, OwningProcess, @{n='ProcessName';e={(Get-Process -Id $_.OwningProcess).ProcessName}} | format-table
$output += Get-Process
$output += Get-WmiObject -Class Win32_product | format-table
$output += Get-WmiObject -Class win32_physicalemmory | format-table
$output += Get-WmiObject Win32_VideoController
$output += systeminfo | format-table
$output += Get-ItemProperty "HKCU:\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store"
Write-Output $output |clip
Write-Host "Data Copied to your clipboard, please paste this data in a new paste at paste.offse.com (don't copy the url!)" -ForegroundColor Green
```

5. この画面にscriptの実行結果を **Ctrl + V** で張り付ける。



エディター プレビュー

6. 貼り付けたら作成を選択

LocalAddress	LocalPort	RemoteAddress	RemotePort	State	OwningProcess	ProcessName
::	61200	::	0	Bound	41128	vmware
::	54354	::	0	Bound	26320	SupportAssistAgent
::1	61200	::1	61199	Established	41128	vmware
::1	61199	::1	61200	Established	41128	vmware
::	49681	::	0	Listen	1656	services
::1	49669	::	0	Listen	5848	jhi.service
::	49668	::	0	Listen	5016	spoolsv

7. このリンクをcopyして、試験官にchatに送信したらラボに接続可能

Copy link

ペースト: <https://paste.offsec.com/?5d5832946e2ce994#9Aj9RrKZ2furHqGstC8SXQFPmxniv8ce3Ht62CMcpjZm> です (コピーするには Ctrl + C / Cmd + C を押してください)

To copy document press on the copy button or use the clipboard shortcut Ctrl + C / Cmd + C

LocalAddress	LocalPort	RemoteAddress	RemotePort	State	OwningProcess	ProcessName
::	49669	::	0	Listen	660	services
::	49668	::	0	Listen	2476	spoolsv
::	49667	::	0	Listen	1180	svchost
::	49666	::	0	Listen	1172	svchost
::	49665	::	0	Listen	516	wininit
::	49664	::	0	Listen	688	lsass
::1	42050	::	0	Listen	6044	OneDrive.Sync.Service
::	7688	::	0	Listen	2160	svchost
::	5357	::	0	Listen	4	System

総 括

- 途中で画面共有が上手くいかず時間がかかった。
- このスクリプトに一番時間がかかった冷静になることが重要
- 時間の延長を交渉したら30分延長してくれた。

3. VM接続

ここではすでにsplunkに接続しているためご了承下さい。

自分は背景と同化していて最初は気がつかなかった。

1. 下記の画面を選択したらsplunkとwindowsに接続できる。

The screenshot shows a web-based exam interface for 'OSTH Exam'. On the left, there's a sidebar with 'Instructions' (radio button), 'Labs' (list including 'Exercise X5', 'Exercise I7' (selected), 'Exercise N5', 'Exercise U3', 'Exercise L8', 'Exercise Z4', 'Exercise A4'), and 'Next Steps' (radio button). The main area is titled 'Exercise I7' and contains a large QR code. Below the QR code is a text input field labeled 'Answer' and a 'Submit' button. To the right of the QR code is a 'MACHINES' section with a table:

MACHINES	OSTH - VM	+ 192.168.123.132	Group
OSTH - VM	+ 192.168.123.132	Group	(refresh icon)

At the bottom of the screen, there's a progress bar indicating '6 / 7' completed and a timer showing '7h 41m / 8h 33m'. There are 'Back' and 'Next' buttons, along with a circular navigation icon.

splunk & windows に接続できる。

Credentials Objectives

192.168.123.132

Splunk OS Credentials:

splunk / Qwerty09!

192.168.123.131

DEV OS Credentials:

offsec / Qwerty09!

- LABと同じく IOCがあるのでしっかり確認すること、またDLしておかないと試験終了後は見ることが出来ない。
- 問題文の後に下にある次のボタンを押すと試験問題になる。
- LABと違い試験問題毎に回答欄がある。(LAB同様)
- 問題毎に回答したかどうかは左側の○が●に変わるので分かる。
- 回答後も変更は可能
- 試験環境のスタートは右側にあるので押すことで環境をスタートできる。
- 試験自体は自分のペースで進められる。
- 休憩やトイレはチャットで報告した。

4. report 提出

1. 受験者は試験終了後24時間以内にレポートを提出
2. 期限を守れなかった場合、試験は自動的に不合格

Upload Your Osth Exam Files

Important: The documentation requirements are very strict and failure to provide sufficient documentation will result in reduced or zero points being awarded.

Please note that once your report is submitted, your submission is final. If any screenshots or other information is missing, you will not be allowed to send them and we will not request them. For more information, please [visit our help center](#).

Your Report

 No file chosen

7z format only. Maximum size of 100MB

[Cancel](#)

[Submit Exam Files](#)

report提出: https://help.offsec.com/hc/en-us/articles/29141776768148-Osth-Exam-Guide#h_01J6YFXFQ95ARF9JXXR15FVZ9B

⚠ 提出チェックリスト

- 試験レポートはPDF形式
- PDFファイル名
- 「OSTH-OS-XXXXX-Exam-Report.pdf」には以下の形式を使用「OS-XXXXX」はOSID
- PDFは .7z ファイルにアーカイブする。(パスワードを付けてアーカイブしない)
- .7zファイル名には「OSTH-OS-XXXXX-Exam-Report.7z」という形式が使用「OS-XXXXX」はOSID
- アーカイブが100MBを超えていないことを確認

提出されたら、Submittedになりcheckされる。



Course OSTH

Foundational Threat Hunting (TH-200)

Level ●● ● | Text Video Lab 41h

Progress: 23.0%

Access will end on March 8th 2026, 09:00 AM. [Extend](#)

[Save](#)

[Continue](#)

TH-200 (Foundational Threat Hunting) introduces core threat hunting techniques and methodologies to proactively detect and mitigate threat actors in enterprise environments. Learners gain practical experience with tools such as CrowdStrike Falcon and Splunk while exploring network data analysis, endpoint hunting, and hunting without IoCs.

[Overview](#) [Syllabus](#) [Challenge Labs](#) [Exam](#)

[Buy new exam attempt](#)

#	CERTIFICATION	DURATION	EXPIRATION DATE	START TIME	STATUS	SUBMIT BY	
1	OSTH Exam	8 hours	Jul 06, 2026, 09:00	Jan 20, 2026, 10:00	Grading	Submitted	