

Commando VM — атакующий дистрибутив Windows

 innostage-group.ru/press/blog/technical/commandovm



Митенёв Всеволод,
инженер отдела
средств защиты
информации

Commando VM — атакующий дистрибутив Windows

Введение

В среде пентестеров своеобразным стандартом тестовой платформы на базе Linux является стабильная и поддерживаемая Kali. Однако, если вы предпочитаете использовать ОС семейства Windows, то вероятно заметили, что подходящей платформы для пентестеров нет. Поддержание пользовательского окружения Windows при сохранении актуальности всего набора инструментов для пентеста многим может показаться сущим мучением. Вероятно, многие потратили не мало часов, настраивая под себя рабочую среду Windows, при этом все используют в работе одни и те же инструменты, утилиты и техники. Осознавая это, компания Mandiant, входящая в FireEye, создала отдельный дистрибутив Windows. Дистрибутив, разработанный на базе другого популярного специализированного дистрибутива компании, предназначенного для анализа вредоносного ПО и реверсинга – FLARE VM, получил название «Complete Mandiant Offensive VM» (Commando VM). В него включены автоматизированные скрипты, призванные помочь каждому пентестеру создать свою собственную рабочую среду и облегчить процесс развертывания и настройки виртуальной машины для пентеста.

Что же такое Commando VM? Это виртуальная машина, от рождения готовая стать «дежурной» машиной для внутренних пентестов в типичной корпоративной инфраструктуре на базе Active Directory. Использование операционной системы Windows дает «врожденную» поддержку Windows и Active Directory, легкий и интерактивный просмотр общих ресурсов, возможность использования виртуальной машины в качестве командного центра тестовой бот-сети и позволяет работать с такими инструментами, как PowerView и BloodHound не заботясь о том, куда поместить выходные файлы на клиентских компьютерах.

Commando VM использует скрипты для установки всего необходимого ПО и добавляет большой набор инструментов и утилит для поддержки пентеста. Список содержит более 140 инструментов, включая: Nmap, Wireshark, Covenant, Python, Go, Remote Server Administration Tools, Sysinternals, Mimikatz, BurpSuite, x64dbg, Hashcat.

С такой комплектацией Commando VM претендует на роль настоящей «Dream Windows Machine» каждого пентестера и редтимера. Если на работе вы чаще носите футболку с надписью «Blue Team», то будьте спокойны: Commando VM также хорошо упакована и для вас. Универсальный набор инструментов, входящий в ее состав обеспечит вас всем необходимым для аудита сетей и повысит ваши возможности по выявлению вредоносных. Библиотека наступательных инструментов позволит синей команде не отстать в гонке средств нападения и защиты. Рассмотрим на примере процесс работы с ней.

Установка Commando VM

Создаем виртуальную машину минимум с 2 ГБ памяти и 60 ГБ диском (рекомендуется не менее 4 ГБ памяти, 80 ГБ диск и 2 сетевых карты). Устанавливаем Windows 7 Service Pack 1 или Windows 10 (последняя дает больше возможностей по установке дополнительного функционала). Желательно установить также гостевые инструменты виртуальной машины (например, VMware Tools) – это предоставит дополнительные возможности – копирования/вставки и изменения размера экрана.

Устанавливаем все обновления с помощью Windows Update. Процедуру обновления нужно повторить несколько раз после каждой перезагрузки, пока Windows Update не покажет, что доступных обновлений нет.

Сохраняем снимок «чистой» виртуальной машины. Скачиваем файл `install.ps1` по адресу github.com/fireeye/commando-vm и копируем его на созданную виртуальную машину. Запускаем PowerShell от имени администратора.

Разрешаем исполнение скриптов командой `Set-ExecutionPolicy Unrestricted`. Переходим в каталог со скриптом и запускаем его командой `.install.ps1` (Рис. 14).

По приглашению скрипта вводим пароль администратора.

Оставшийся процесс установки полностью автоматизирован. Во время установки машина несколько раз перезагрузится. Процесс установки будет каждый раз автоматически возобновляться. Установка продолжается примерно 3-4 часа.

```
PS C:\Users\kevin\Downloads\commandovm> .\install.ps1  
[+] Beginning install...
```



COMPLETE MANDIANT
OFFENSIVE VM

Version 1.0

Developed by
Jake Barteaux
Proactive Services
Blaine Stancill
FireEye Labs Advanced Reverse Engineering
Nhan Huynh
FireEye Labs Advanced Reverse Engineering

Рис. 14. Запуск скрипта установки Commando VM



Рис. 15. Рабочий стол Commando VM

Тест-драйв Commando VM

Commando VM ориентирована в первую очередь на тестирование внутренних сетей. Рассмотрим на примере внутренней сети способ работы с дистрибутивом. Просканируем сеть с помощью Nmap (Рис. 16).

```
C:\Users\kevin\assessements\windomain>nmap -sTV -top-ports 100 192.168.38.0/24 -oA test.domain
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-19 16:55 Mountain Daylight Time
Nmap scan report for 192.168.38.104
Host is up (0.00s latency).
Not shown: 95 filtered ports
PORT      STATE SERVICE        VERSION
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
3389/tcp  open  ms-wbt-server  Microsoft Terminal Services
8080/tcp  open  http           Jetty 9.4.z-SNAPSHOT
MAC Address: 00:0C:29:8E:D9:DD (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Рис. 16. Сканирование сети с помощью Nmap

Порт 8080 часто используется для административных веб-интерфейсов. Проверим какое приложение через него работает. Запускаем Firefox, вводим адрес сервера и порт. Видим приглашение ввода имени и пароля сервера Jenkins (Рис. 17).

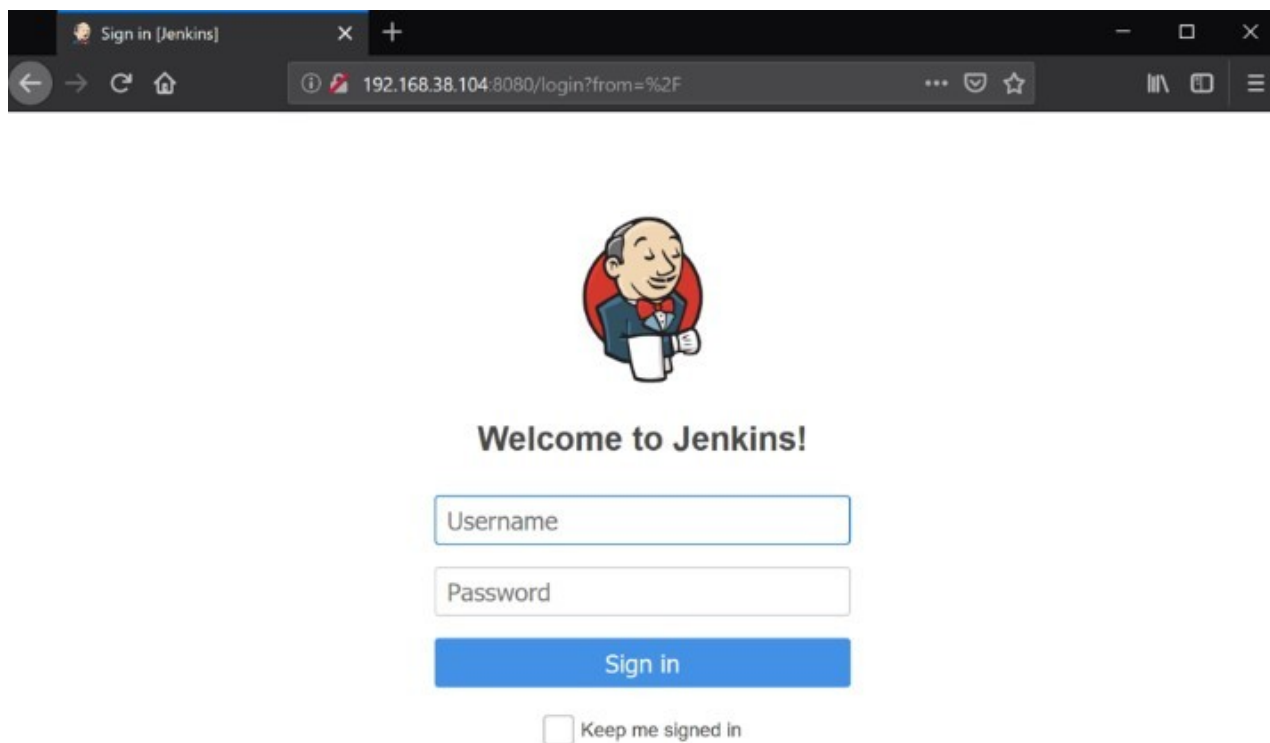


Рис. 17. Страница входа сервера Jenkins

Цель определена. Выбираем оружие. Для таких случаев в арсенале CommandoVM есть Burp Suite Intruder. В качестве боеприпаса возьмем произвольный файл паролей от OWASP SecLists Project в папке Wordlists на рабочем столе. После настройки Burp Suite Intruder и анализа откликов видим, что пароль «admin» дает доступ к консоли Jenkins (Рис. 18).

11	admin	302			398
12	welcome	302			438
13	monkey	302			438
14	login	302			437

Request

Response

RawHeadersHex

```
HTTP/1.1 302 Found
Connection: close
Date: Tue, 12 Mar 2019 20:10:28 GMT
X-Content-Type-Options: nosniff
Set-Cookie: JSESSIONID.4f5e0dc5=node0tp55pea2gwa4lr0usqtkjme6j93.node0;Path=/;HttpOnly
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Set-Cookie: JSESSIONID.4f5e0dc5=node014alb66brb8e314mn3wpss2r2v94.node0;Path=/;HttpOnly
Location: http://192.168.38.104:8080/
Server: Jetty(9.4.z-SNAPSHOT)
```

Рис. 18. Подбор пароля с помощью Burp Suite Intruder

Хорошо известно, что сервер Jenkins в среде Windows по умолчанию устанавливается со Script Console, и запускается под учетной записью NT AUTHORITY\SYSTEM. Разумеется, мы воспользуемся этим преимуществом для повышения привилегий, но сперва проверим, так ли это. Переходим в каталог script на целевом сервере и запускаем простой скрипт для определения под какой учетной записью работает Script Console (Рис. 19).

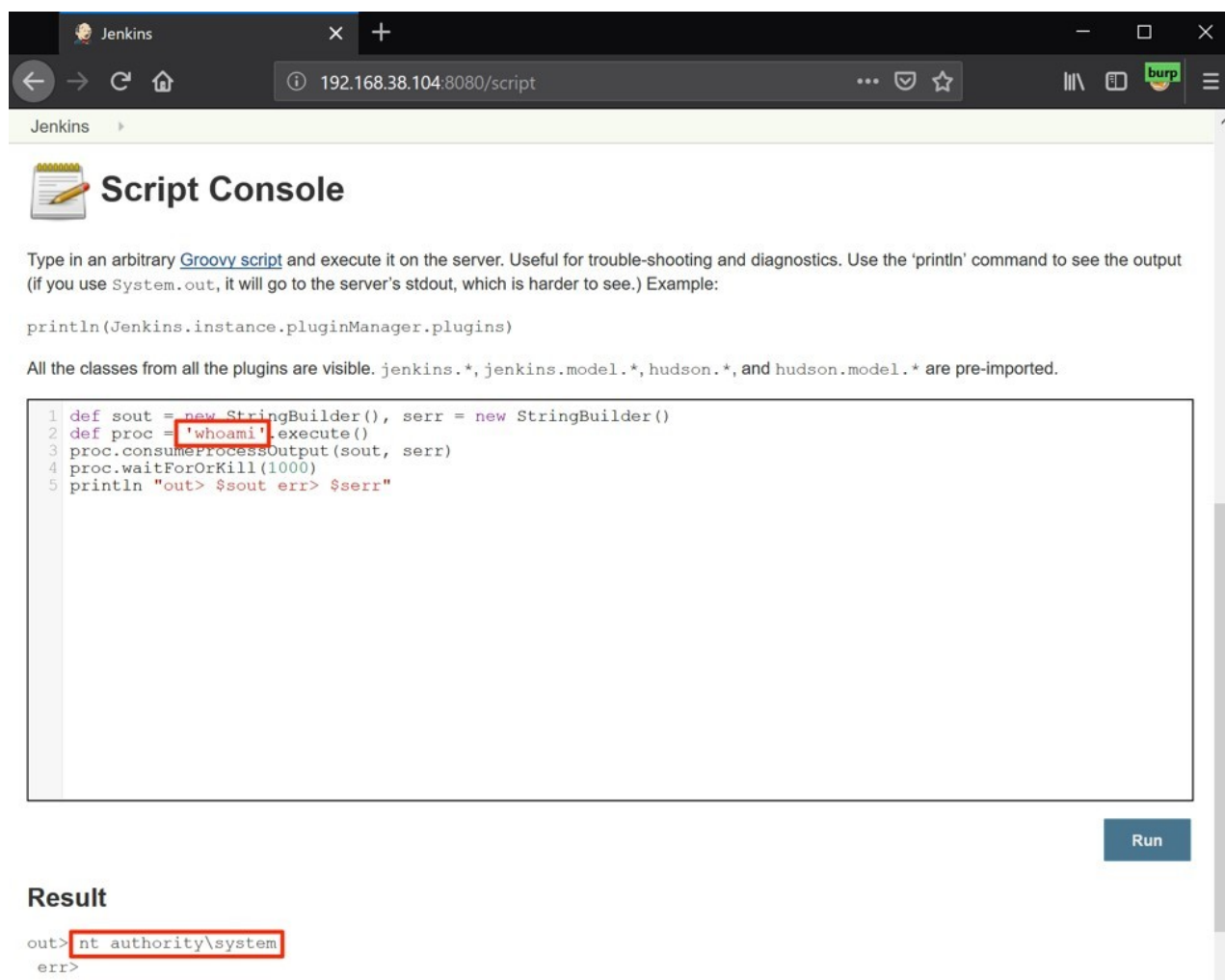


Рис. 19. Script Console сервера Jenkins

Командная консоль с системными привилегиями открывает большой выбор дальнейших действий; но мы не станем никуда спешить и для начала посмотримся на месте: проверим нет ли на сервере файлов с полезной информацией. В каталоге пользователя «Niso Sepersky» нашелся закрытый ключ SSH и файл «pass.txt» с самоутверждающим паролем «!mth3best!» (Рис 20).

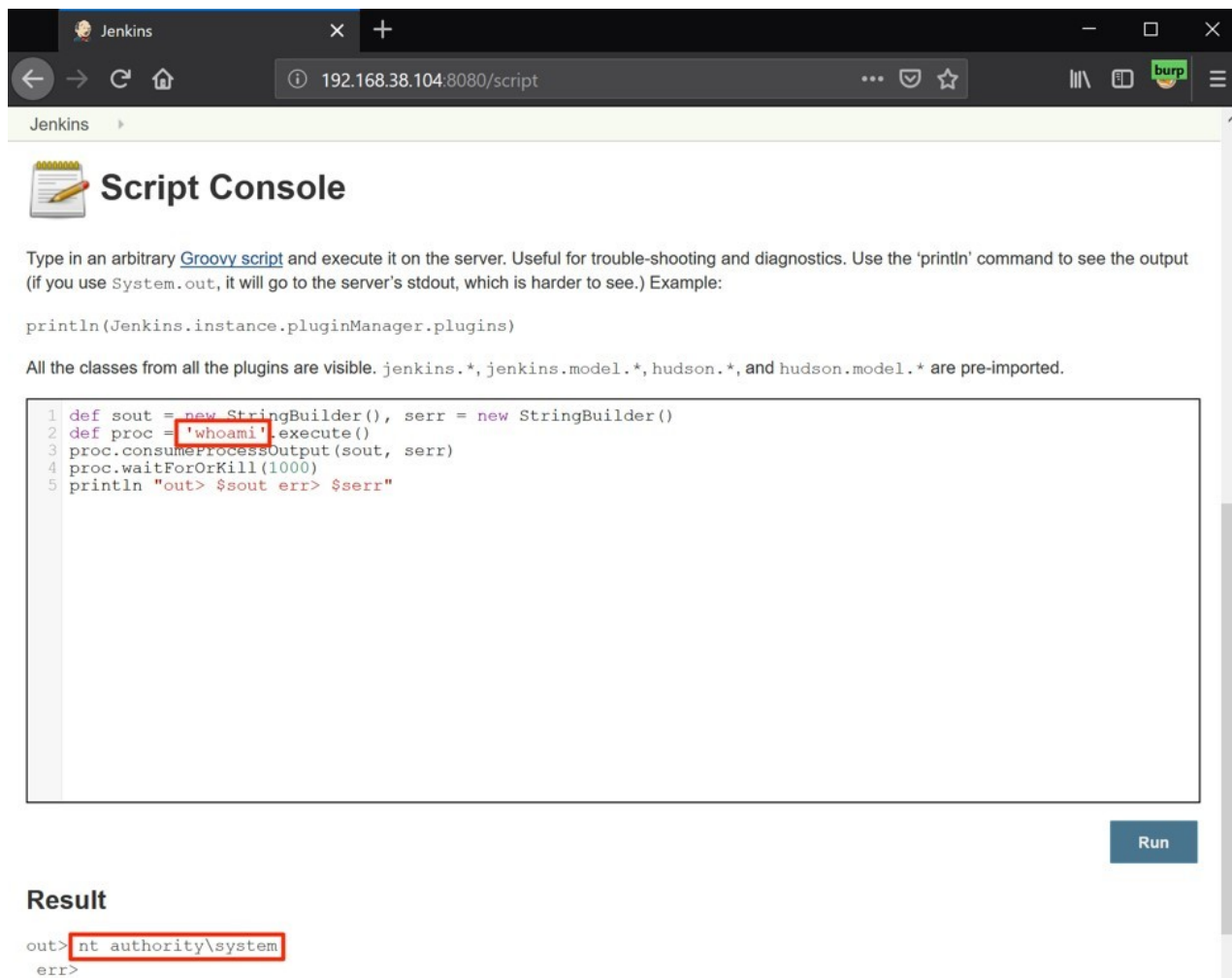


Рис. 20. Файл с паролем пользователя, найденный на сервере Jenkins

Самое время вспомнить о главной цели – корпоративной инфраструктуре на базе Active Directory. Проверим полученную учетную запись на контроллере домена. Инструмент CredNinja из набора CommandoVM прекрасно подойдет для этого (Рис. 21).

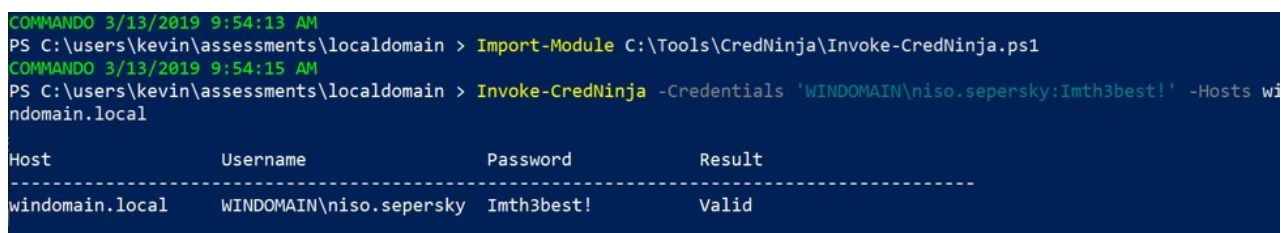


Рис. 21. Проверка учетной записи с помощью CredNinja на контроллере домена

А какие права на других узлах? С помощью Nmap мы получили файл 445hosts.txt со списком узлов, на которых открыт порт 445 TCP. Проверим права учетной записи на них (Рис. 22).


```

COMMANDO 3/13/2019 10:08:40 AM
PS C:\users\kevin\assessments\localdomain > Invoke-CredNinja -Credentials 'WINDOMAIN\niso.sepersky:Imth3best!' -Hosts $(
Get-Content .\445hosts.txt)

```

Host	Username	Password	Result
192.168.38.102	WINDOMAIN\niso.sepersky	Imth3best!	Valid
192.168.38.103	WINDOMAIN\niso.sepersky	Imth3best!	Valid
192.168.38.104	WINDOMAIN\niso.sepersky	Imth3best!	LOCAL ADMIN!

Рис. 22. Проверка учетной записи с помощью CredNinja на узлах по списку из файла

Похоже камрад Niso Sepersky имеет административные права только на сервере Jenkins 192.168.38.104. С такого плацдарма можно начать разведку домена.

Простая команда `runas /netonly /user:windomain.local\niso.sepersky cmd.exe` и ввод пароля позволит получить командную строку с правами Niso Sepersky в домене windomain, в чем можно убедиться, выведя список файлов общего ресурса sysvol на контроллере домена (Рис. 23).

```

C:\Users\kevin\assessments\localdomain>runas /netonly /user:windomain.local\niso.sepersky cmd.exe
Enter the password for windomain.local\niso.sepersky:
Attempting to start cmd.exe as user "windomain.local\niso.sepersky" ...

```

```

cmd.exe (running as windomain.local\niso.sepersky)
Microsoft Windows [Version 10.0.17763.348]
(c) 2018 Microsoft Corporation. All rights reserved.

COMMANDO Wed 03/13/2019 9:58:59.72
C:\WINDOWS\system32>dir \\windomain.local\sysvol
Volume in drive \\windomain.local\sysvol is Windows 2016
Volume Serial Number is 00BB-1F7B

Directory of \\windomain.local\sysvol

02/15/2019 12:01 AM <DIR> .
02/15/2019 12:01 AM <DIR> ..
02/15/2019 12:01 AM <JUNCTION> windomain.local [C:\Windows\SYSTEM\sysvol\domain]
0 File(s) 0 bytes
3 Dir(s) 39,479,476,224 bytes free

COMMANDO Wed 03/13/2019 10:00:19.10
C:\WINDOWS\system32>

```

Рис. 23. Запуск командной строки от имени найденной учетной записи

Запустим PowerShell и поищем общие ресурсы с помощью PowerView (Рис. 24)

```

COMMANDO 3/13/2019 10:05:50 AM
PS C:\users\kevin\assessments\localdomain > Import-Module C:\Tools\PowerSploit\Recon\PowerView.ps1
COMMANDO 3/13/2019 10:06:09 AM
PS C:\users\kevin\assessments\localdomain > Invoke-ShareFinder -ExcludeStandard -CheckShareAccess -NoPing -Threads 20 |
Out-File shares.txt
COMMANDO 3/13/2019 10:15:25 AM
PS C:\users\kevin\assessments\localdomain > cat .\shares.txt
\\dc.windomain.local\NETLOGON - Logon server share
\\wef.windomain.local\Engineering -
\\dc.windomain.local\SYSTEM - Logon server share
\\wef.windomain.local\Software$ -
COMMANDO 3/13/2019 10:15:35 AM
PS C:\users\kevin\assessments\localdomain >

```

Рис. 24. Поиск общих ресурсов с помощью PowerView

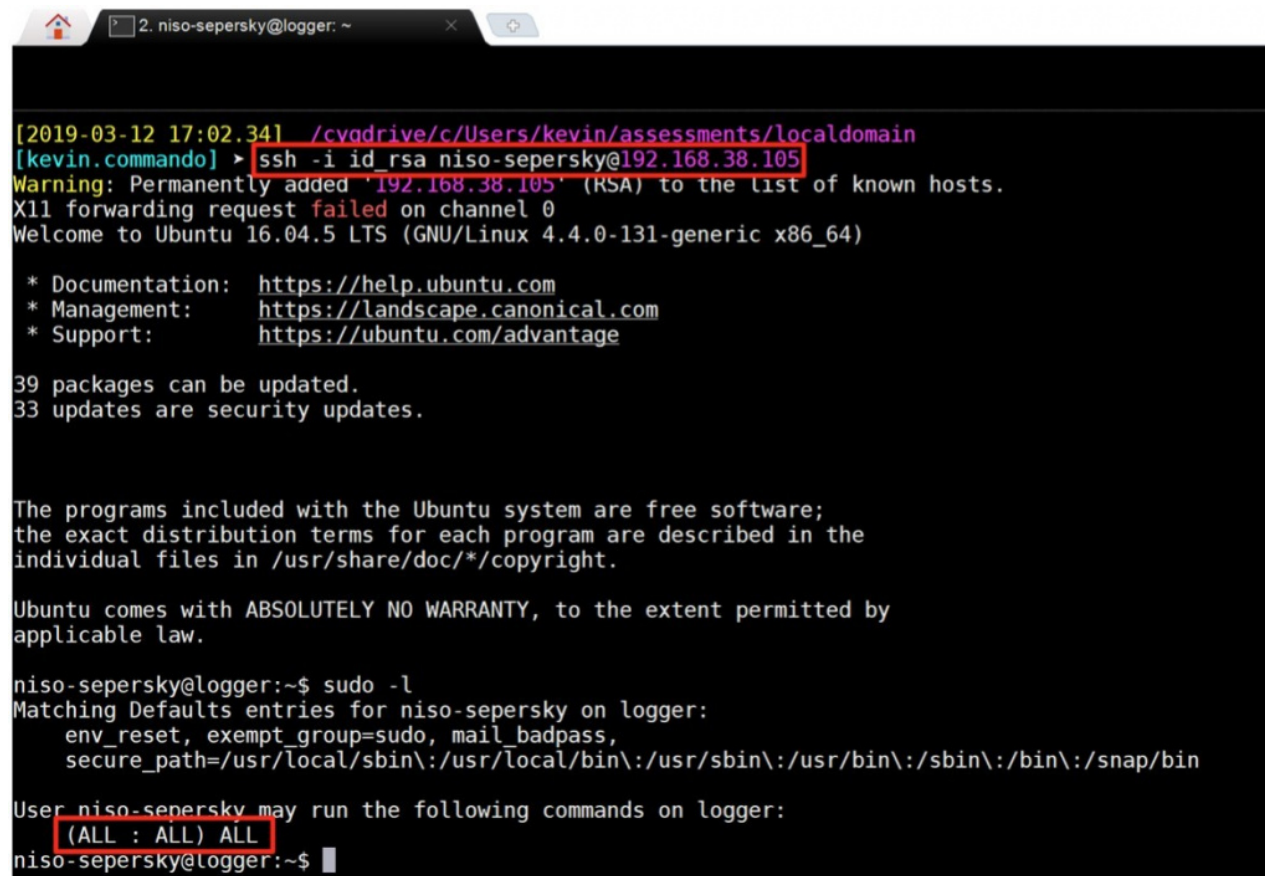
Нужно узнать о том в какие группы входит доступная нам учетная запись и ее права. Применим модуль GetDomainUser, чтобы поближе познакомиться с нашим другом Niso Sepersky. Обратите внимание на то, что CommandoVM по умолчанию использует ветку «dev» платформы PowerView (Рис. 25).

```
COMMANDO 3/13/2019 10:25:04 AM
PS C:\users\kevin\assessments\localdomain > Import-Module C:\Tools\PowerSploit\Recon\PowerView_dev.ps1
COMMANDO 3/13/2019 10:25:30 AM
PS C:\users\kevin\assessments\localdomain > Get-DomainUser niso.sepersky -Domain windomain.local 2>$null

company           : WinDomain
logoncount         : 7
badpasswordtime    : 12/31/1600 5:00:00 PM
st                : CO
mail              : Niso.Sepersky@windomain.local
department        : Engineering
objectclass        : {top, person, organizationalPerson, user}
displayname        : Niso Sepersky
lastlogontimestamp : 3/12/2019 2:22:23 PM
userprincipalname  : niso.sepersky@windomain.local
name              : Niso Sepersky
l                 : Highlands Ranch
primarygroupid     : 513
objectsid          : S-1-5-21-1708028330-1629023850-3525407807-2250
samaccountname     : niso.sepersky
```

Рис. 25. Получение информации об учетной записи с помощью Get-DomainUser

Осталось еще проверить не поможет ли нам продвинуться дальше найденный закрытый ключ SSH. При сканировании портов нашелся хост 192.168.38.105 с открытым портом 22 TCP. Попробуем установить с ним SSH-соединение с помощью MobaXterm (Рис. 26).



```
2. niso-sepersky@logger: ~
[2019-03-12 17:02.34] /cyqdrive/c/Users/kevin/assessments/localdomain
[kevin.commando] > ssh -i id_rsa niso-sepersky@192.168.38.105
Warning: Permanently added '192.168.38.105' (RSA) to the list of known hosts.
X11 forwarding request failed on channel 0
Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.4.0-131-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

39 packages can be updated.
33 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

niso-sepersky@logger:~$ sudo -l
Matching Defaults entries for niso-sepersky on logger:
  env_reset, exempt_group=sudo, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User niso-sepersky may run the following commands on logger:
(ALL : ALL) ALL
niso-sepersky@logger:~$
```

Рис. 26. SSH-соединение с помощью MobaXterm

Есть доступ к SSH-серверу с правами root. Увы, он не поможет нам повысить привилегии в домене. Придется вернуться назад и поискать полезную информацию на общем ресурсе Software\$, который мы нашли раньше с помощью Invoke-ShareFinder. Для этого отлично подойдет обычный проводник Windows (Рис. 27).

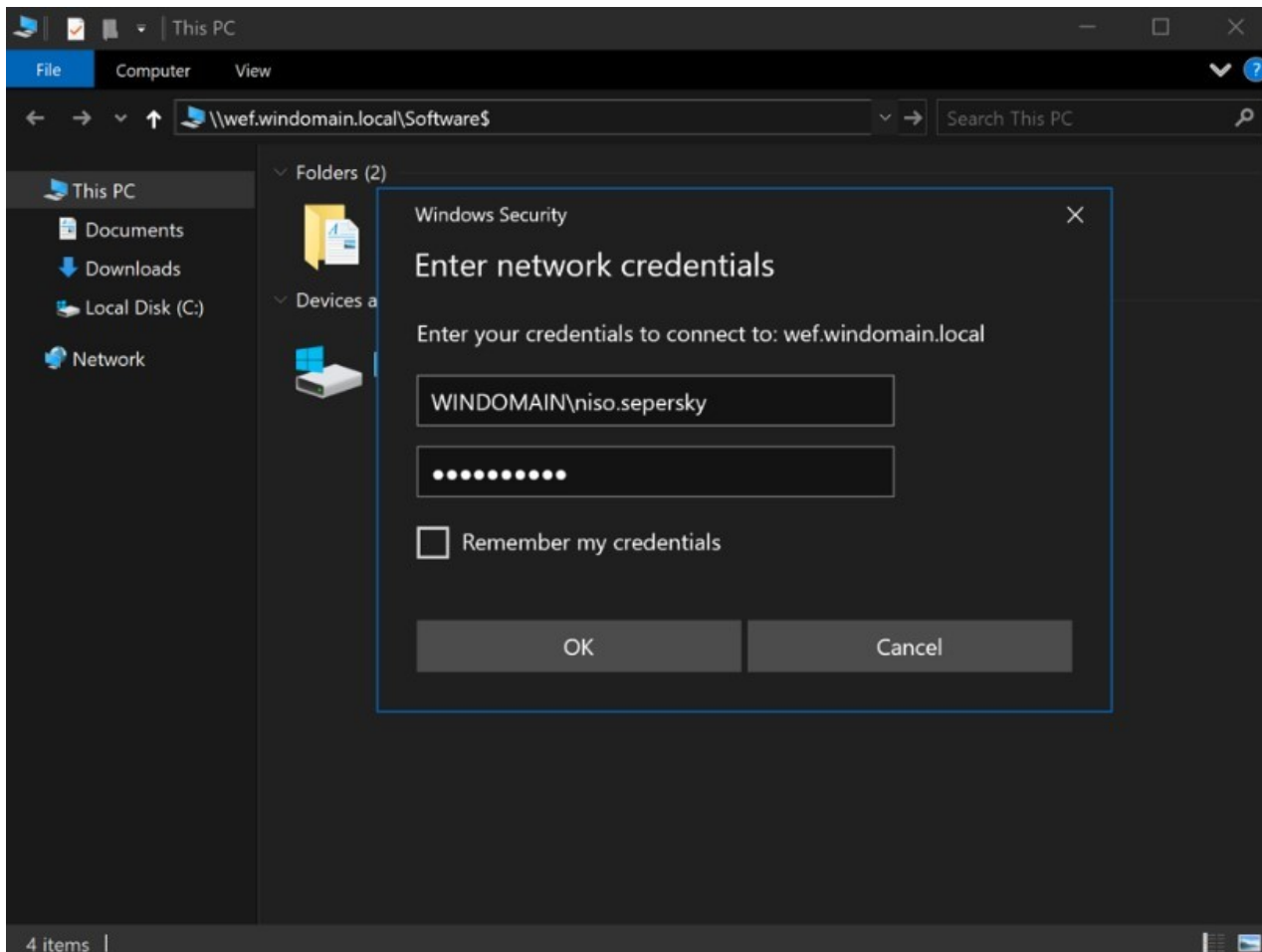


Рис. 27. Подключение в общему ресурсу с использованием полученной учетной записи

После просмотра множества файлов наше терпение было наконец вознаграждено: мы нашли конфигурационный файл с записанными открытым текстом учетными данными сервисной учетной записи (Рис. 28).

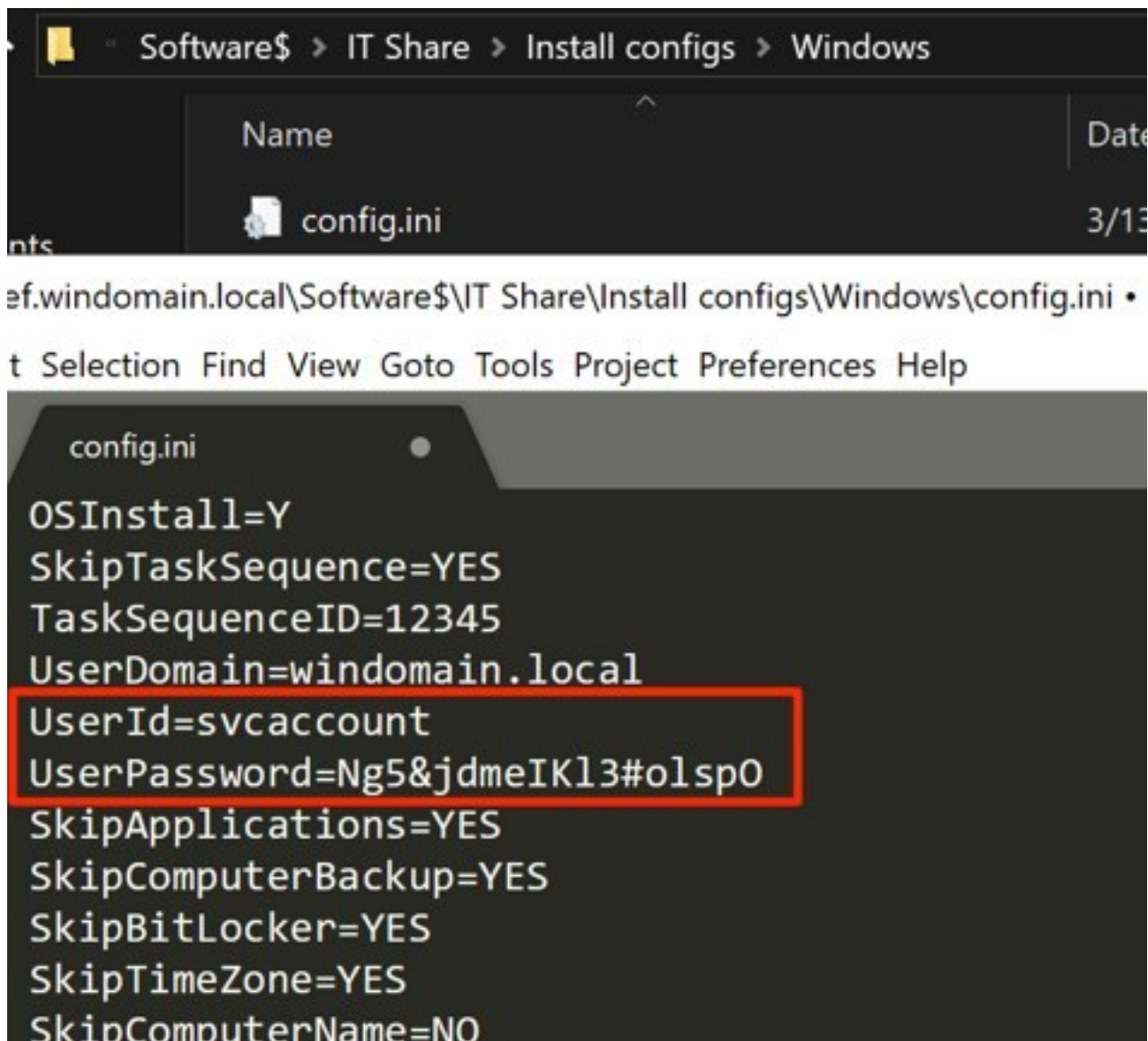


Рис. 28. Конфигурационный файл с учетными данными

Проверка найденной учетной записи на контроллере домена с помощью CredNinja показала, что она имеет права локального администратора (Рис. 29).

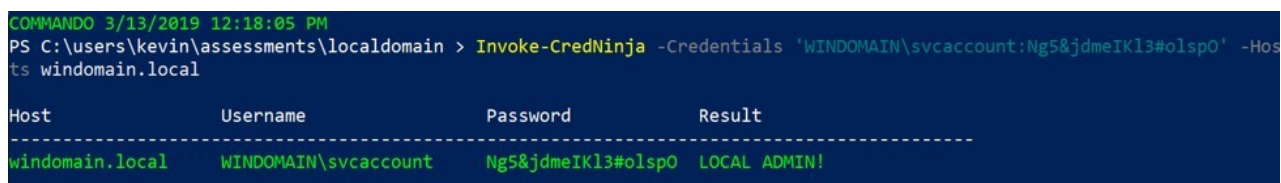


Рис. 29. Проверка сервисной учетной записи с помощью CredNinja на контроллере домена

Проверим в какие группы входит учетная запись. Для этого снова используем модуль GetDomainUser (Рис. 30).

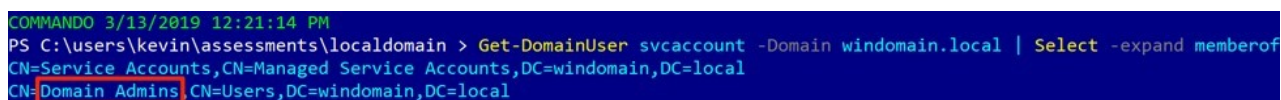


Рис. 30. Получение информации о сервисной учетной записи с помощью Get-DomainUser

Поздравляю! Мы в группе администраторов домена! Конечно, сеть, которую мы проверяли была вымышленной (тестовой); но все использованные инструменты – настоящие, и они, как и многие другие установлены на Commando VM по умолчанию. Полный список инструментов и установочные скрипты можно найти в репозитории Commando VM в Github по [ссылке](#).

В августе 2019 года, вышла обновлённая версия дистрибутива Commando VM 2.0.