

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет экономический

Кафедра экономико-математического моделирования

ЛАБОРАТОРНАЯ РАБОТА №1

на тему

«Защита данных файлового сервера»

38.03.05 — Кибербезопасность в экономике

Выполнили

Студенты группы НБИбд-02-22

Студенческий билет №: 1132229056

_____ Д.Д. Панченко

(подпись)

Студенческий билет №: 1132222827

_____ П.А. Савурская

(подпись)

Студенческий билет №: 1132221541

_____ Н.Р. Кочарян

(подпись)

Студенческий билет №: 1132220820

_____ Д.В. Чистякова

(подпись)

Студенческий билет №: 1132229527

_____ А.В. Захаренко

(подпись)

Студенческий билет №: 1132220826

_____ В.В. Щербакова

(подпись)

Студенческий билет №: 1032228104

_____ Е. Кроитору

(подпись)

«___» _____ 2024 г.

Проверил

к.ф.-м.н., доцент кафедры теории
вероятностей и кибербезопасности,

_____ В.А. Бесчастный

(подпись)

Москва 2024

Оглавление

Список сокращений	3
Введение.....	4
Ход работы.....	5
1. Простой пароль пользователя веб-приложения предприятия.....	5
2.1. Служба RDP на порту установлена по умолчанию	9
2.2. Последствие Manager meterpreter	11
3.1. Служба RDP на порту установлена по умолчанию	13
3.2. Последствие FS Backdoory	17
Вывод.....	19

Список сокращений

Русскоязычные сокращения

БД	База данных
ПО	Программное обеспечение

Англоязычные сокращения

CVE	Demilitarized Zone
DMZ	Demilitarized Zone
OWA	Outlook Web Access
RDP	Remote Desktop Protocol

Введение

Внешний злоумышленник находит в интернете сайт Компании и решает провести атаку на него с целью получения доступа к внутренним ресурсам. На сайте был обнаружен раздел для входа в личный кабинет, который не содержит защитных механизмов от атаки перебора учетных данных. Нарушитель смог успешно подобрать параметры входа для одного из пользователей.

Использование одинаковых паролей для различных сервисов позволило нарушителю получить доступ к почтовому ящику сотрудника и далее успешно подключиться к его рабочей станции, с которой он атаковал внутренний файловый сервис с помощью уязвимости в windows-реализации SMB-протокола.

Квалификация нарушителя средняя. Он умеет использовать инструментарий для проведения атак, а также знает техники постэксплуатации.

Ход работы

1. Простой пароль пользователя веб-приложения предприятия

На узле Web Server PHP обслуживается веб-сайт предприятия. В веб-приложении существует механизм аутентификации пользователей.

С помощью ViPNet IDS NS детектируем инструмент перебора паролей hydra, атака происходит на порт 10.10.1.20 (Рисунок 1).

Ур...	Дата и время	Код события	Ко...	Название правила	Класс	Протокол	IP-адрес источн...	Порт источ...	IP-адрес получат...	Порт пол...	Направл...
...	20:27:28.220 20.02...	2010935	1	ET SCAN Suspicious inbound to ...	bad-known...	TCP	195.239.174.11	37432	10.10.1.24	1433	→ ←
...	20:27:28.922 20.02...	3227008	1	ET SCAN Potential SSH Scan	attempted-recon	TCP	195.239.174.11	37437	10.10.1.24	22	→ ←
...	20:27:30.167 20.02...	2010936	1	ET SCAN Suspicious inbound to ...	bad-known...	TCP	195.239.174.11	37430	10.10.1.24	1521	→ ←
...	20:27:30.292 20.02...	2010936	1	ET SCAN Suspicious inbound to ...	bad-known...	TCP	195.239.174.11	37432	10.10.1.24	1521	→ ←
...	20:27:32.505 20.02...	2010939	1	ET SCAN Suspicious inbound to ...	bad-known...	TCP	195.239.174.11	37430	10.10.1.24	5432	→ ←
...	20:27:32.601 20.02...	2010939	1	ET SCAN Suspicious inbound to ...	bad-known...	TCP	195.239.174.11	37432	10.10.1.24	5432	→ ←
...	20:27:44.066 20.02...	2101877	1	GPL WEB_SERVER printenv access	web-application-activity	TCP	195.239.174.11	38823	10.10.1.20	80	→ ←
...	20:27:49.508 20.02...	3061281	1	AM USER_AGENTS Suspicious U...	bad-known...	TCP	195.239.174.11	53862	10.10.1.20	80	→ ←
...	20:28:00.086 20.02...	2001330	1	ET INFO RDP - Res...	AM USER_AGENTS Suspicious User-Agent -	TCP	10.10.4.11	3389	195.239.174.11	58118	→ ←
...	20:28:00.086 20.02...	2001330	1	ET INFO RDP - Res...	Hydra	TCP	10.10.4.11	3389	195.239.174.11	58118	→ ←
...	20:28:04.451 20.02...	3007339	1	AM TROJAN TrojanDownloader...	trojan-activity	TCP	10.10.4.11	58009	195.239.174.11	8081	→ ←

Рисунок 1. Сканирование серверов из Интернета

Передаем данные группе реагирование (Рисунок 2).

Основная информация Чат Закрытый

Дата и время события 02.02.2025 20:27

Описание Правило обнаруживает нестандартный клиент (UserAgent) в HTTP запросах

Индикаторы компрометации Простой пароль пользователя веб-приложения предприятия.

Рекомендации Изменить пароль пользователя веб-приложения на более сложный, который не содержится в словаре rockyou.txt.

Оценка ★ ★ ★ ★ ★

Автор Панченко Денис @1132229056

Ответственный Панченко Денис @1132229056

Источник 195.239.174.11

Поражённые активы 10.10.1.20

Рисунок 2. Передача данных

Аутентифицируемся на узле Web Server PHP, воспользовавшись учетной записью user и SSH 10.10.1.20 (Рисунок 3), через Bitvise SSH Client (Рисунок 4).

Access to virtual infrastructure from the response team VM			
Edge Gateway	WEB: https://10.10.1.254	admin	qweGWE
Internal Gateway	WEB: https://10.10.2.254	admin	qweGWI
Web Portal PHP	SSH: 10.10.1.20	user	qwe123!@#
	MySQL DB	root	qwe123asd
CMS Drupal	SSH: 10.10.1.21	user	qwe123!@#
	WEB: http://10.10.1.21	admin	qwe123!@#
Apache Tomcat	SSH: 10.10.1.24	user	qwe123!@#
	WEB: http://10.10.1.24:8080	admin	qwe123!@#
MS Active Directory	RDP: 10.10.2.10	ampire\administrator	qwe123!@#
MS Exchange Server	RDP: 10.10.2.11	ampire\administrator	qwe123!@#
MS FileServer	RDP: 10.10.2.12	ampire\administrator	qwe123!@#

Рисунок 3. Данные для входа в виртуальные среды

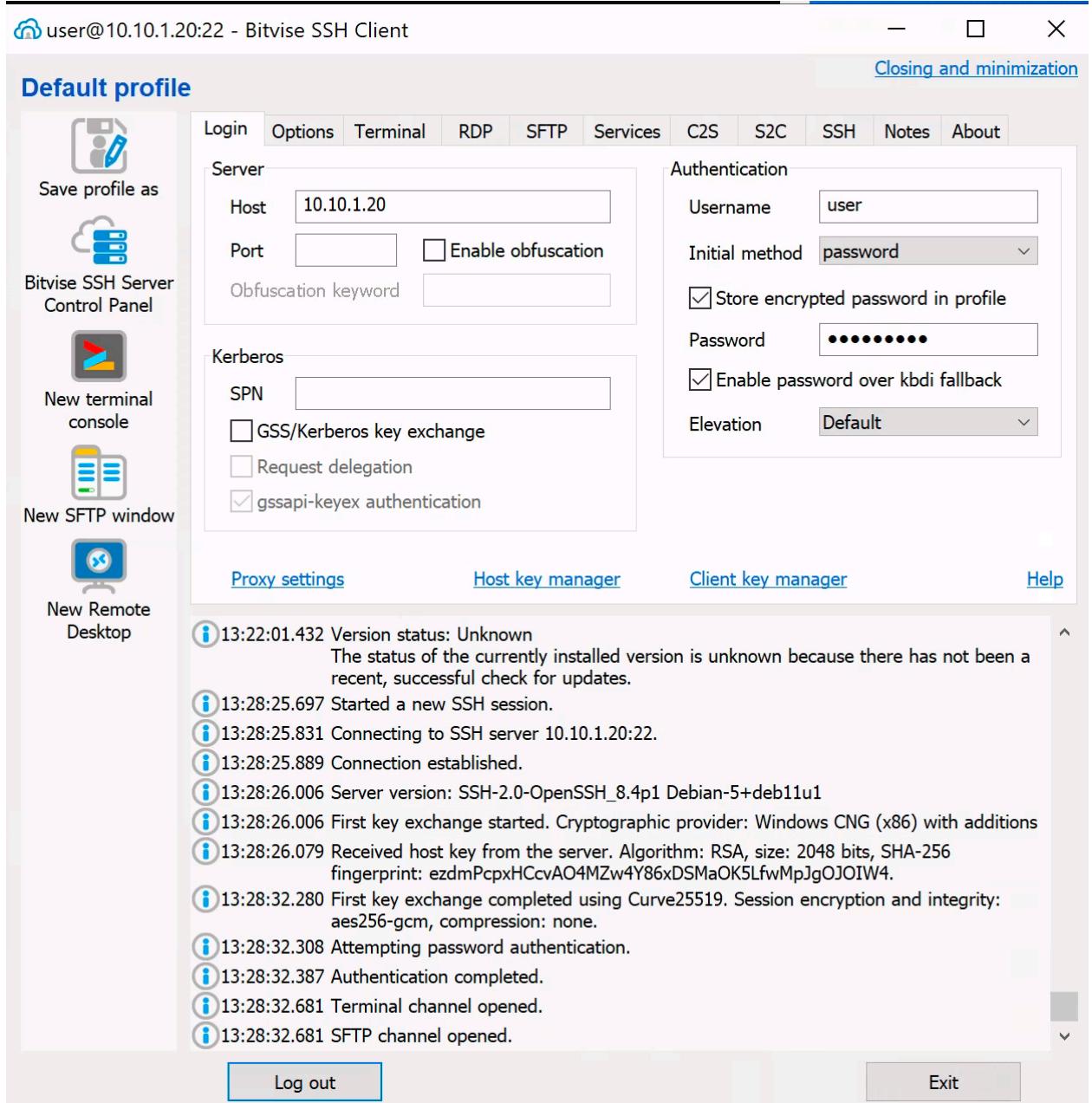


Рисунок 4. Переход в учетную запись user через клиент SSH

Авторизуемся в MySQL, используя логин и пароль. Для вывода всех таблиц БД выполним команды show databases; use topro; show tables; (Рисунок 5).

```

user@webportal1:~$ mysql -uroot -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 269813
Server version: 10.1.45-MariaDB-0+deb9u1 Debian 9.12

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show databases;
+-----+
| Database      |
+-----+
| information_schema |
| msgdb          |
| mysql          |
| performance_schema |
| topro          |
+-----+
5 rows in set (0.00 sec)

MariaDB [(none)]> use topro;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
Database changed
MariaDB [topro]> show tables;
+-----+
| Tables_in_topro |
+-----+
| comment         |
| news            |
| user            |
+-----+
3 rows in set (0.00 sec)

```

Рисунок 5. Авторизация и вывод таблиц БД «topro»

Для вывода всех данных в таблице воспользуемся командой SELECT * FROM user;. В конце таблицы мы видим скомпрометированный пароль пользователя «Manager1» (Рисунок 6).

MariaDB [toppro]> SELECT * FROM user;		email	password	role
id name				
1	Лисин Дмитрий Сергеевич	dlisin@toppro.com	Dk04_12!	user
2	Жуков Андрей Никитич	azhukov@toppro.com	Hj50@1k!	user
3	Харитонова Светлана Дмитриевна	sharitonova@toppro.com	Vk1k\$09_	user
4	Мурзаев Ильдар Арсенович	imurzaev@toppro.com	Gvc!678@	user
5	Стройнов Павел Антонович	pstroinov@toppro.com	Kb#980!&	user
6	Сухарев Артемий Петрович	asuharev@toppro.com	Kp09!f=2	user
7	Ковалёв Валерий Дмитриевич	vkovalev@toppro.com	1k_Rt35!	user
8	Цициулина Ксения Павловна	kciculina@toppro.com	Gh%yu12+	user
9	Петров Иван Семёнович	ispetrov@toppro.com	Bn12#hj!	user
10	Мирошина Дарья Анатольевна	dmiroshina@toppro.com	We!789\$n	user
11	Колобов Вячеслав Владимирович	vkolobov@toppro.com	Fg@84h!j	user
12	Петренко Александр Алексеевич	apetrenko@toppro.com	Kjg#@124	user
13	Пугачёв Пётр Иванович	ppugachev@toppro.com	Fgn!67#0	user
14	Зарубин Александр Григорьевич	azarubin@toppro.com	\$S\$156!jd	user
15	Гатауллина Динара Булатовна	dgataullina@toppro.com	Nv456!=1	user
16	Дёмина Наталья Сергеевна	ndemina@toppro.com	Hfv#671_	user
17	Куприянова Анжела Викторовна	akupriyanova@toppro.com	dsK13%b_	user
18	Иванченко Владислава Константиновна	vivanchenko@toppro.com	nCxh1234	user
19	Лихачёва Людмила Андреевна	llihacheva@toppro.com	Xj*s!1789	user
20	Прохина Антонина Владимировна	aproch이나@toppro.com	Jk!23vc)	user
21	Гуров Евгений Матвеевич	egurov@toppro.com	Kfd+lw43	user
22	Ноготков Сергей Петрович	snogotkov@toppro.com	Yu0_l2@%	user
23	Шилина Алина Дмитриевна	ashilina@toppro.com	Er12+09!	user
24	Белова Светлана Ильинична	sbelova@toppro.com	K3_2#nfa	user
25	Иванова Анжелика Ивановна	aivanova@toppro.com	Ls!24_rt	user
26	Лысенко Дарья Александровна	dlisenko@toppro.com	Y#89&f0q	user
27	Петров Иван Александрович	ipetrov@toppro.com	mX13)_1*	user
28	Силин Алексей Георгиевич	asilin@toppro.com	Fki!28_@	user
29	Усачев Дмитрий Игоревич	dusachev@toppro.com	Jkdl2joq	user
30	Зорин Игорь Радионович	izorin@toppro.com	Kcf!287%	user
31	Немцов Александр Михайлович	anemcov@toppro.com	p!D134_%	user
32	Зяглина Наталья Тимофеевна	nzvyagina@toppro.com	KLp!29_#	user
33	Машук Анна Юрьевна	amashyuk@toppro.com	IHty12_5	user
34	UserOne	user1@mail.local	qwe123!@#	user
35	Manager1	manager1@ampire.corp	qwe123!@#	user

Рисунок 6. Вывод таблицы user

Выполним команду update user set password = ‘YOUR PASSWORD’ where name = ‘Manager1’ и сменим пароль для пользователя (Рисунок 7).

```
MariaDB [toppro]> update user set password = 'ckjgfh123' where name = 'Manager1';
Query OK, 1 row affected (0.01 sec)
Rows matched: 1  Changed: 1  Warnings: 0
```

Рисунок 7. Успешное изменение пароля пользователя

Перейдём в Ampire и убедимся в успешном устранении уязвимости (Рисунок 8).



Рисунок 8. Успешное устранение уязвимости Web1 MySQL Password

2.1. Служба RDP на порту установлена по умолчанию

На узле менеджера Manager Workstation 1 для внешней сети открыт порт 3389, обслуживающий соединения по протоколу RDP.

С помощью ViPNet IDS NS детектируем этап атаки на внутренний хост 10.10.4.11 (Рисунок 9).

● 20:28:04.451 20.02.... 3007339 1 AM TROJAN TrojanDownloader.... trojan-activity	TCP	10.10.4.11	58009	195.239.174.11	8081
● 20:28:04.451 20.02.... 3007339 1 AM TROJAN TrojanDownloader.... trojan-activity	TCP	10.10.1.253	17331	195.239.174.11	8081
● 20:28:05.379 20.02.... 2035480 1 ET INFO PE EXE Download over r... misc-activity	TCP	195.239.174.11	4445	10.10.1.253	55356
● 20:28:05.379 20.02.... 2035480 1 ET INFO PE EXE Download over r... misc-activity	TCP	195.239.174.11	4445	10.10.4.11	58013
● 20:28:05.413 20.02.... 2025644 1 ET TROJAN Possible Metasploit ... trojan-activity	TCP	195.239.174.11	4445	10.10.1.253	55356
● 20:28:05.414 20.02.... 2025644 1 ET TROJAN Possible Metasploit ... trojan-activity	TCP	195.239.174.11	4445	10.10.4.11	58013
● 20:28:14.623 20.02.... 3227012 1 ET SCAN Behavioral Unusual Por... misc-activity	TCP	10.10.4.11	58101	10.10.2.3	445
● 20:28:43.712 20.02.... 2102465 1 GPL NETBIOS SMB-DS IPC\$ shar... protocol-command-decode	TCP	10.10.4.11	59716	10.10.2.10	445
● 20:28:43.712 20.02.... 2102465 1 GPL NETBIOS SMB-DS IPC\$ shar... protocol-command-decode	TCP	10.10.2.254	57004	10.10.2.10	445
● 20:28:43.818 20.02.... 3201433 1 ET EXPLOIT Possible ETERNALBL... trojan-activity	TCP	10.10.4.11	59716	10.10.2.10	445
● 20:28:43.818 20.02.... 3204835 1 ET EXPLOIT Possible ETERNALBL... trojan-activity	TCP	10.10.4.11	59716	10.10.2.10	445
● 20:28:43.819 20.02.... 3201433 1 ET EXPLOIT Possible ETERNALBL... trojan-activity	TCP	10.10.2.254	57004	10.10.2.10	445
● 20:28:43.819 20.02.... 3204835 1 ET EXPLOIT Possible ETERNALBL... trojan-activity	TCP	10.10.2.254	57004	10.10.2.10	445

Рисунок 9. События атаки на внутренний хост

Передаем данные группе реагирование (Рисунок 10).

AM TROJAN TrojanDownloader.JTTH

Основная информация Чат Закрытый

Дата и время события ①
20.02.2025 20:28

Описание ①
Правило обнаруживает сетевую активность вредоносного ПО

Индикаторы компрометации ①
служба RDP на порту установлена по умолчанию

Рекомендации ①
Отключить доступ по RDP для узла

Оценка ★ ★ ★ ★ ★
Автор ПД Панченко Денис @1132229056
Ответственный ПД Панченко Денис @1132229056
Источник 10.10.4.11
Поражённые активы 195.239.174.11

Рисунок 10. Передача данных

Для закрытия уязвимости отключим доступ по RDP для узла Manager Workstation 1.

Для этого подключимся к узлу менеджера Manager Workstation 1, находящейся во внутренней сети, по протоколу RDP (Рисунок 11).

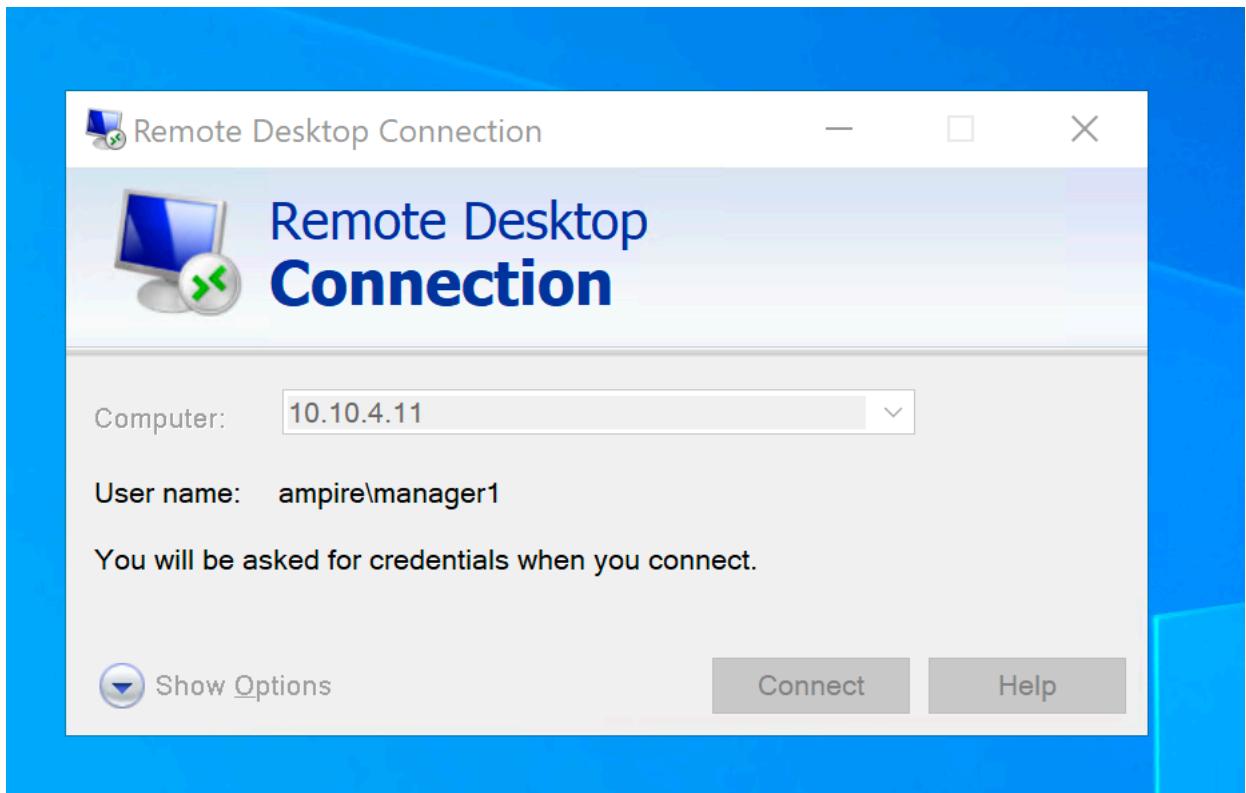


Рисунок 11. Подключение к узлу Manager Workstation 1

Зайдем на EdgeGW (WEB: <https://10.10.1.254>). Введем данные и нажмем sign in (Рисунок 12).

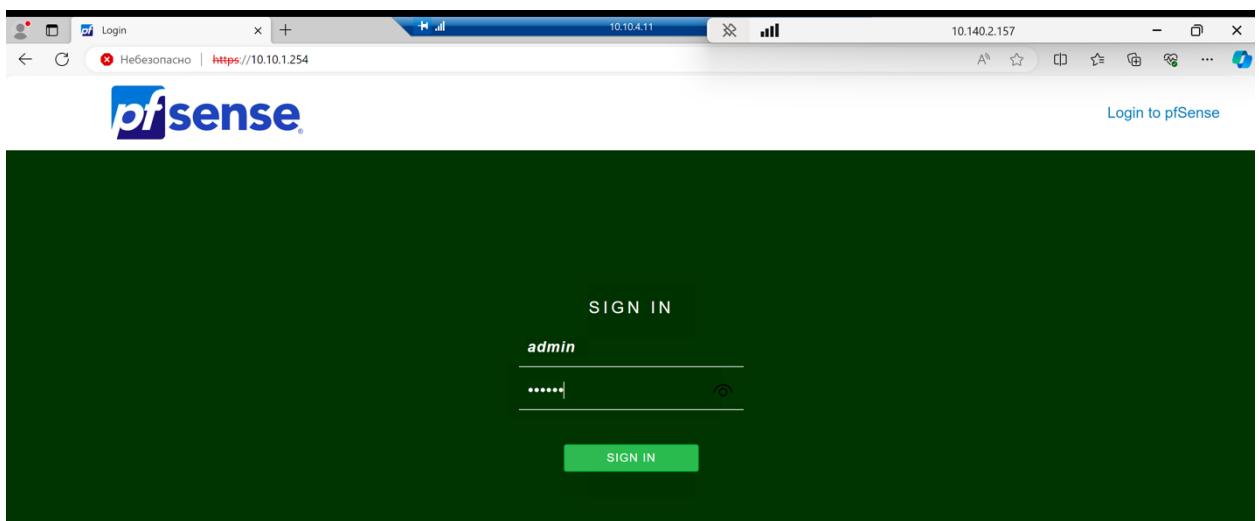


Рисунок 12. EdgeGW

Отключим доступ по RDP для виртуальной машины менеджера Manager1 (Рисунок 13).

<input type="checkbox"/>	<input checked="" type="checkbox"/>	3 /1.10 MIB	IPv4 TCP/UDP	*	*	Manager	3389 (MS RDP)	*	none	Temp to Manager1
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0 /424 B	IPv4 TCP	*	*	InternalGW	25 (SMTP)	*	none	NAT To mail srv

Рисунок 13. Отключение правил проброса RDP портов

Перейдём в Ampire и убедимся в успешном устранении уязвимости (Рисунок 14).

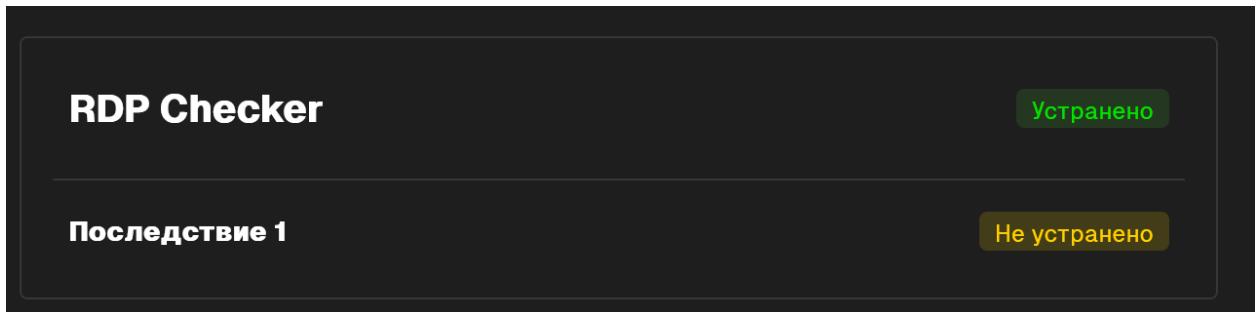


Рисунок 14. Успешное устраниние уязвимости RDP Checker

2.2. *Последствие Manager meterpreter*

Нарушитель устанавливает shell соединение с машиной Manager1.

Подключимся к узлу администратора Administrator Workstation, находящейся во внутренней сети, по протоколу RDP (Рисунок 15).

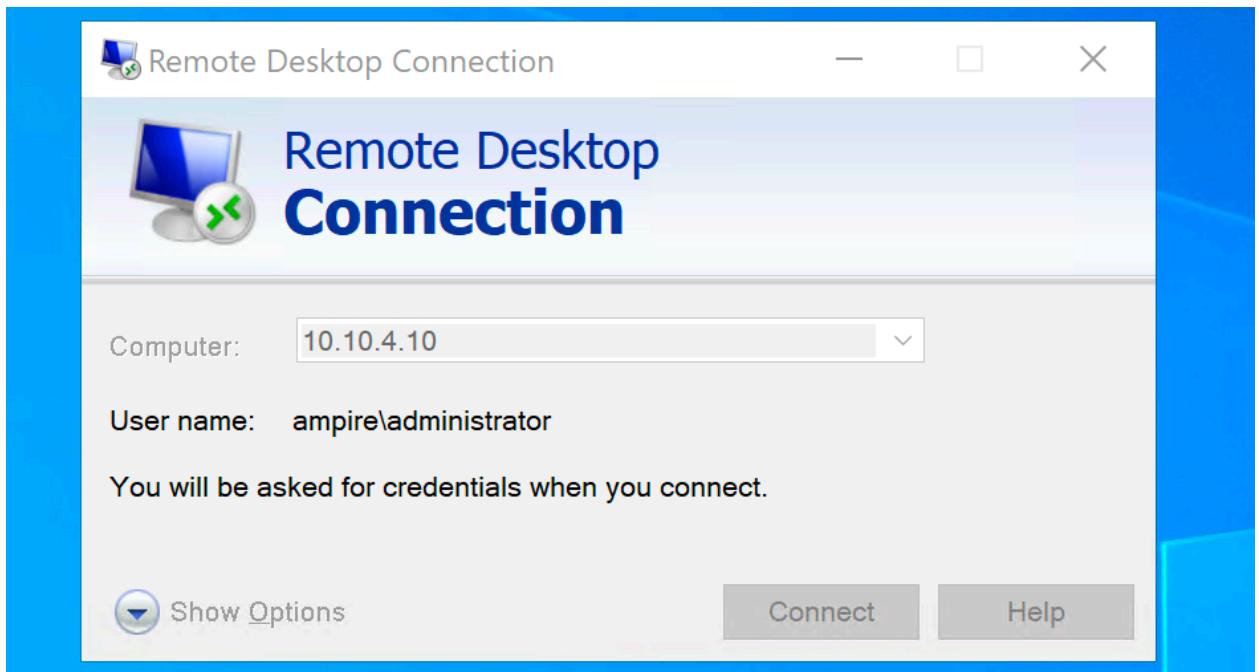
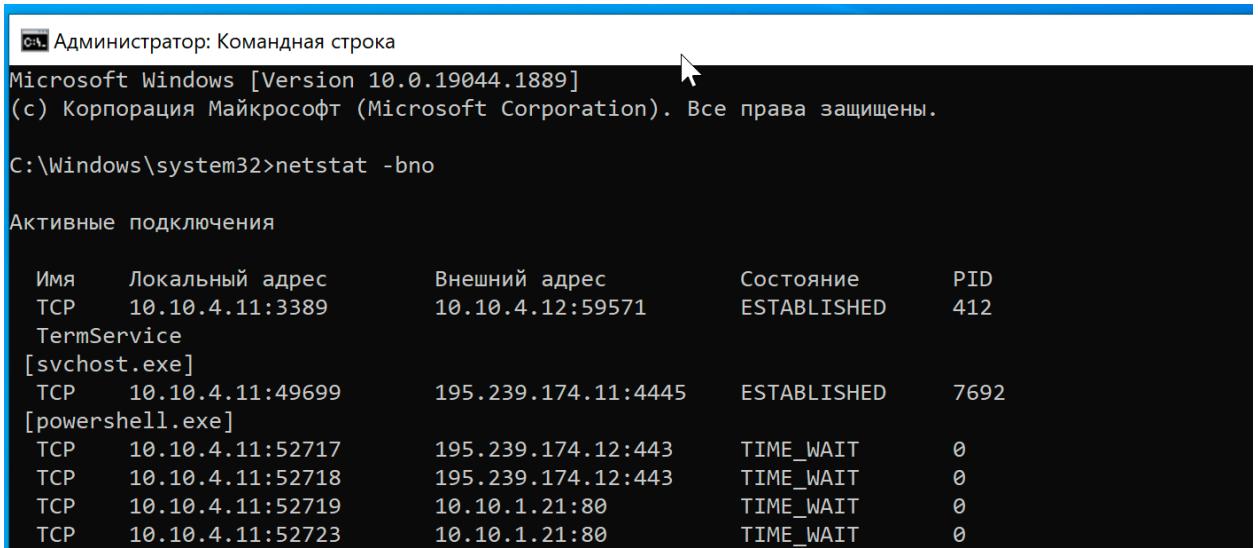


Рисунок 15. Подключение к узлу Administrator Workstation

Установленную сессию с нарушителем и имя процесса обнаруживаем с помощью утилиты netstat с ключами -bno (Рисунок 16).



```

Administrator: Командная строка
Microsoft Windows [Version 10.0.19044.1889]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Windows\system32>netstat -bno

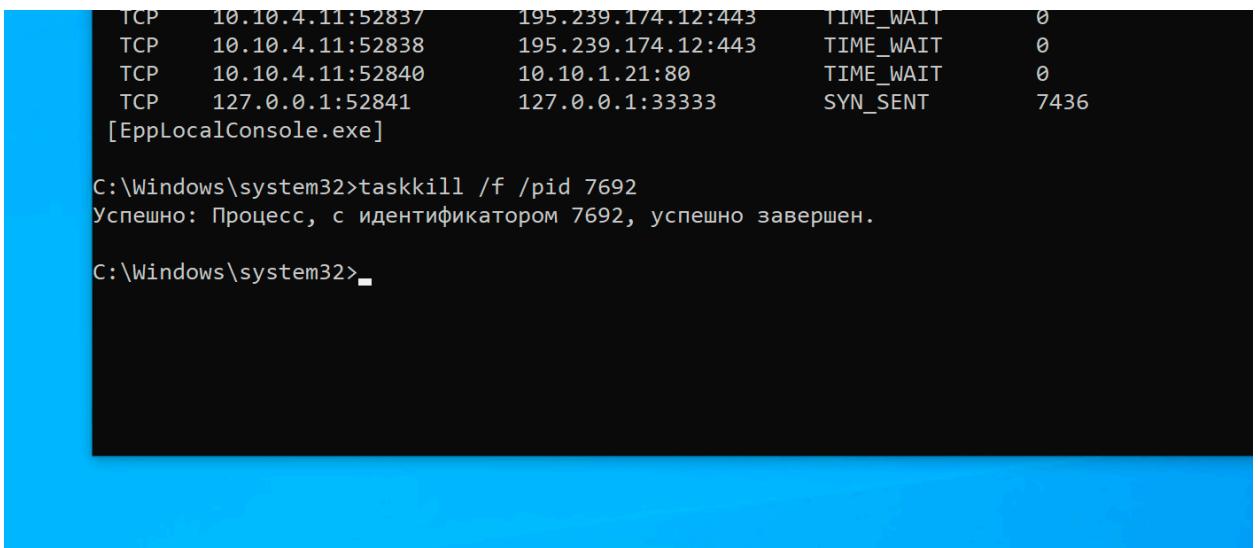
Активные подключения

Имя      Локальный адрес        Внешний адрес        Состояние      PID
TCP      10.10.4.11:3389          10.10.4.12:59571    ESTABLISHED   412
TermService
[svchost.exe]
TCP      10.10.4.11:49699        195.239.174.11:4445  ESTABLISHED   7692
[powershell.exe]
TCP      10.10.4.11:52717        195.239.174.12:443   TIME_WAIT     0
TCP      10.10.4.11:52718        195.239.174.12:443   TIME_WAIT     0
TCP      10.10.4.11:52719        10.10.1.21:80       TIME_WAIT     0
TCP      10.10.4.11:52723        10.10.1.21:80       TIME_WAIT     0

```

Рисунок 16. Список установленных соединений

Мы видим активное соединение веб-портала с IP-адресом нарушителя (195.239.174.11). Для устранения завершаем соединение с помощью команды taskkill /f /pid <PID> (Рисунок 17).



```

C:\Windows\system32>taskkill /f /pid 7692
Успешно: Процесс, с идентификатором 7692, успешно завершен.

C:\Windows\system32>

```

Рисунок 17. Остановка процесса

Последствие Manager meterpreter успешно устранило, meterpreter-сессия с нарушителем (195.239.174.11) завершена. Перейдём в Ampire и убедимся в успешном устраниении последствия (Рисунок 18).

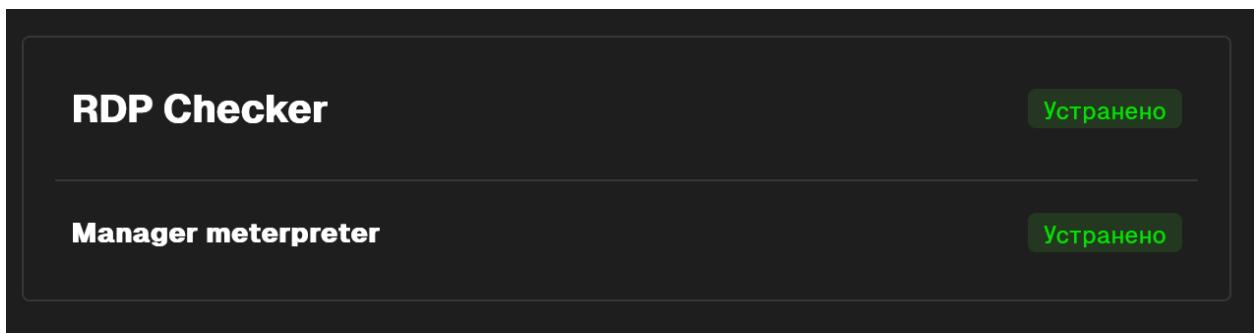


Рисунок 18. Успешное устранение последствия Manager meterpreter

3.1. Служба RDP на порту установлена по умолчанию

Узел MS FileServer является файловым сервером сети предприятия. Файловый сервер предоставляет центральный ресурс в сети для хранения и обеспечения совместного доступа к файлам пользователям сети.

С помощью ViPNet IDS NS детектируем эксплуатацию уязвимости MS17-010 по 445 порту (наиболее распространенный SMB порт) с помощью Metasploit Framework. Обнаруживается анализатором сетевых пакетов (Рисунок 19).

The screenshot displays two windows from the ViPNet TIAS application. The left window is a list of network events over the last 24 hours, showing various SMB-related activity. The right window is a detailed view of a specific event from 2028:43.821 20.02.2025, which is identified as an 'ET EXPLOIT ETERNALBLUE Probe Vulnerable System Response MS17-010 (CVE-2017-0144)' attempt. The detailed view includes sections for 'Общая информация', 'Правило анализа', and the raw 'Текст' of the alert message.

Рисунок 19. Факт эксплуатации Eternalblue

Изучив цепочку атак, обнаруживаем, что атака адресована файловому серверу (ip: 10.10.2.12). Это подтверждает анализ событий в ViPNet TIAS (Рисунок 18).

<input type="checkbox"/> Не обработан	20.02.2025 22:01:00	10	10.10.2.12	FS	Нарушение це...	Вредоносная акти...	Создание нов...	У службы в качестве ...
<input type="checkbox"/> Не обработан	20.02.2025 22:01:00	10	10.10.2.12	FS	Нарушение це...	Подозрительная...	Добавление р...	Выявлено добавлени...

Рисунок 20. Атака на узел 10.10.2.12

Передаем данные группе реагирование (Рисунок 21).

ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (Generic Flags)

Основная информация Чат Закрытый

Дата и время события ①
20.02.2025 20:28

Описание ①
Правило обнаруживает в сетевом трафике программный код, предназначенный для эксплуатации уязвимости

Индикаторы компрометации ①
Уязвимость MS17-010 файлового сервера

Рекомендации ①
На узле MS FileServer отключить протокол SMBv1

Оценка
☆ ☆ ☆ ☆ ☆

Автор
Панченко Денис
@1132229056

Ответственный
Панченко Денис
@1132229056

Источник
10.10.4.11

Поражённые активы
10.10.2.10

Рисунок 21. Передача данных

Для устранения данной уязвимости для начала подключимся к RDP файлового сервера (Рисунок 22).

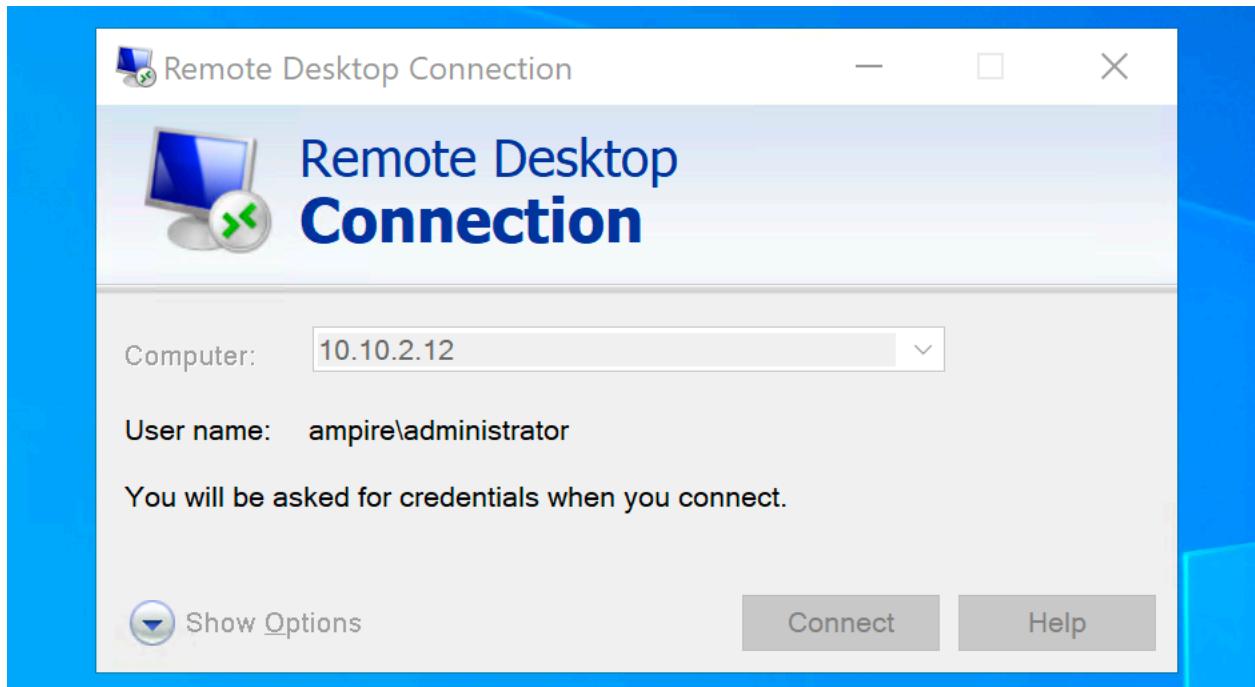


Рисунок 22. Подключение к RDP файлового сервера

Для закрытия уязвимости отключим SMB (Server Message Block) – сетевой протокол для удаленного доступа к файлам и принтерам (Рисунок 23).

```

Administrator: Windows PowerShell
PS C:\Users\administrator.AMPIRE> Get-SmbServerConfiguration

AnnounceComment : False
AnnounceServer   : 512
AsynchronousCredits : False
AuditSmb1Access  : 15
AutoDisconnectTimeout : True
AutoShareServer   : True
AutoShareWorkstation : True
CachedOpenLimit    : 10
DurableHandleV2TimeoutInSeconds : 180
EnableAuthenticateUserSharing : False
EnableDownlevelTimewarp : False
EnableForcedLogoff  : True
EnableLeasing      : True
EnableMultiChannel  : True
EnableOplocks       : True
EnableSecuritySignature : False
EnableSMB1Protocol : True
EnableSMB2Protocol : True
EnableStrictNameChecking : True
EncryptData        : False
IrpStackSize       : 15
KeepAliveTime     : 2
MaxChannelPerSession : 32
MaxMpxCount       : 50
MaxSessionPerConnection : 16384
MaxThreadsPerQueue : 20
MaxWorkItems       : 1
NullSessionPipes   : IPC$ 
Nullsessionshares : 35
OplockBreakWait   : 120
PendingClientTimeoutInSeconds : True
RejectUnencryptedAccess : False
RequireSecuritySignature : True
ServerHidden       : 8192
Smb2CreditsMax    : 512
Smb2CreditsMin    : 0
SmbServerNameHardeningLevel : False
TreatHostAsStableStorage : True
ValidateAliasNotCircular : True
ValidateShareScope  : True
ValidateShareScopeNotAliased : True
ValidateTargetName  : True

```

Рисунок 23. Подключение к RDP файлового сервера

Для его отключения выполним команду Set-SmbServerConfiguration - EnableSMB1Protocol \$false в Windows PowerShell (Рисунок 24).

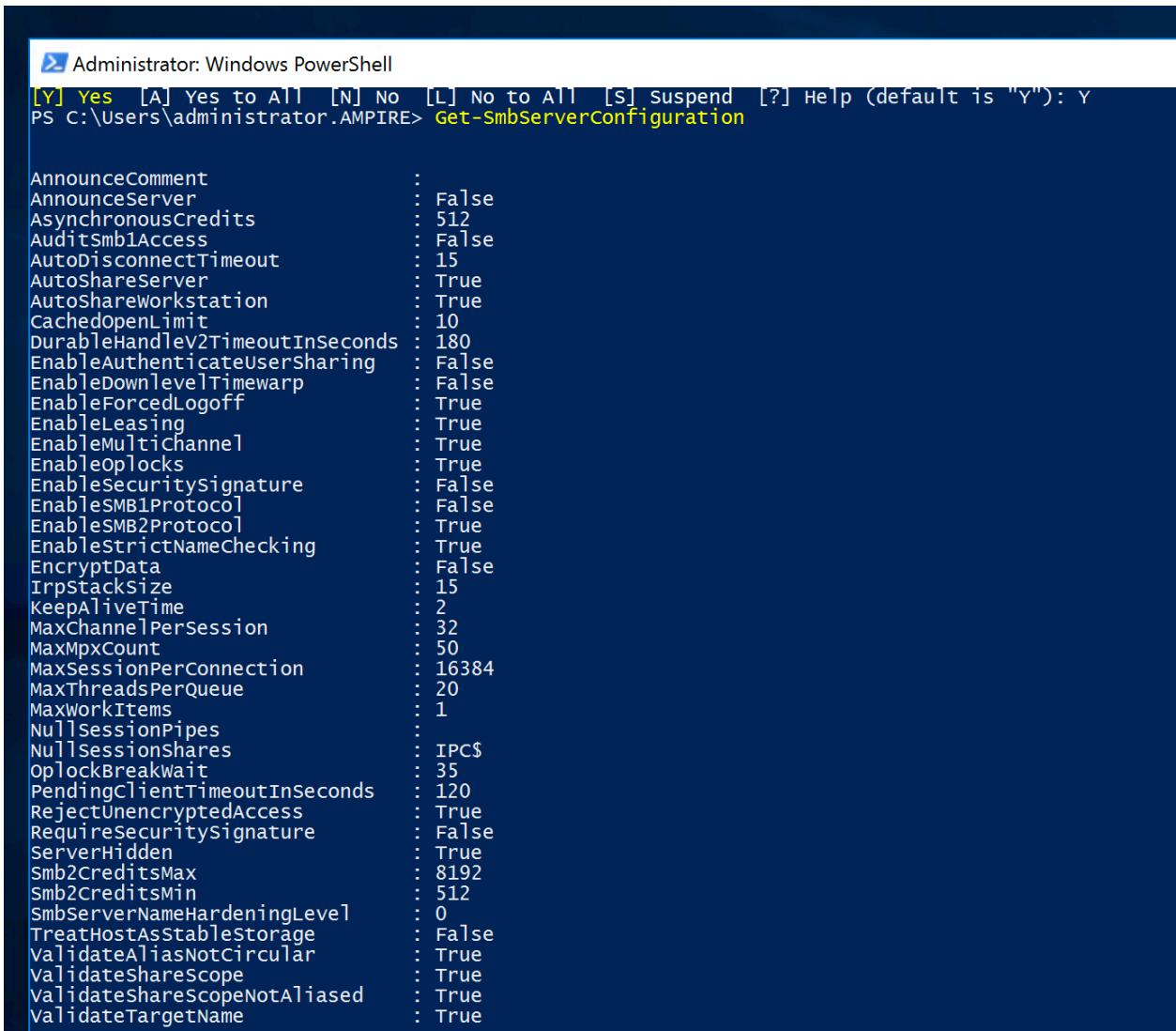
```

PS C:\Users\administrator.AMPIRE> Set-SmbServerConfiguration -EnableSMB1Protocol $false
Confirm
Are you sure you want to perform this action?
Performing operation 'Modify' on Target 'SMB Server Configuration'.
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): Y

```

Рисунок 24. Отключение протокола SMBv1

Проверим отключение данного протокола (Рисунок 25).



```
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): Y
PS C:\Users\administrator.AMPIRE> Get-SmbServerConfiguration

AnnounceComment          : False
AnnouncesServer          : 512
AsynchronousCredits      : False
AuditSmb1Access          : 15
AutoDisconnectTimeout    : True
AutoShareServer           : True
AutoShareWorkstation      : True
CachedOpenLimit            : 10
DurableHandlev2TimeoutInSeconds : 180
EnableAuthenticateUserSharing : False
EnableDownlevelTimewarp   : False
EnableForcedLogoff        : True
EnableLeasing              : True
EnableMultichannel         : True
EnableOplocks              : True
EnableSecuritySignature    : False
EnableSMB1Protocol         : False
EnableSMB2Protocol         : True
EnableStrictNameChecking   : True
EncryptData                : False
IrpStackSize               : 15
KeepAliveTime              : 2
MaxChannelPerSession       : 32
MaxMpxCount                : 50
MaxSessionPerConnection    : 16384
MaxThreadsPerQueue          : 20
MaxWorkItems                : 1
NullSessionPipes           : IPC$ 
NullSessionShares          : 35
OplockBreakWait            : 120
PendingClientTimeoutInSeconds : True
RejectUnencryptedAccess    : False
RequiresecuritySignature    : True
ServerHidden                 : True
Smb2CreditsMax              : 8192
Smb2CreditsMin              : 512
SmbServerNameHardeningLevel : 0
TreatHostAsStableStorage     : False
ValidateAliasNotCircular    : True
ValidateShareScope           : True
ValidateShareScopeNotAliased : True
ValidateTargetName           : True
```

Рисунок 25. Проверка статуса на сервере

Уязвимость MS17-010 файлового сервера успешно устранена (Рисунок 26).

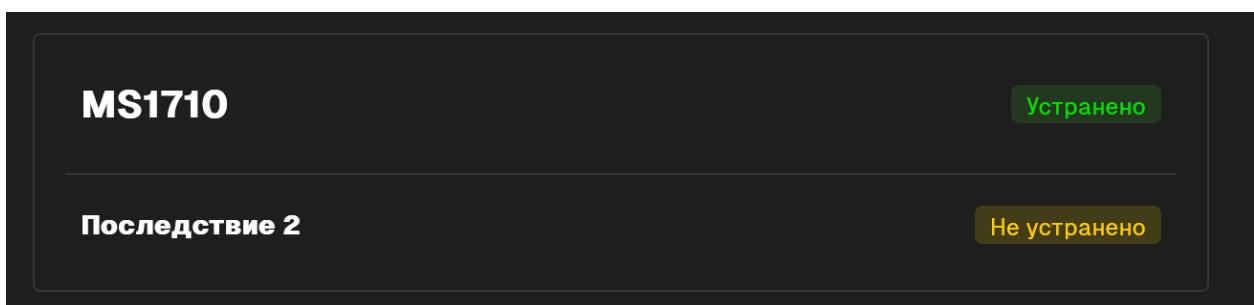
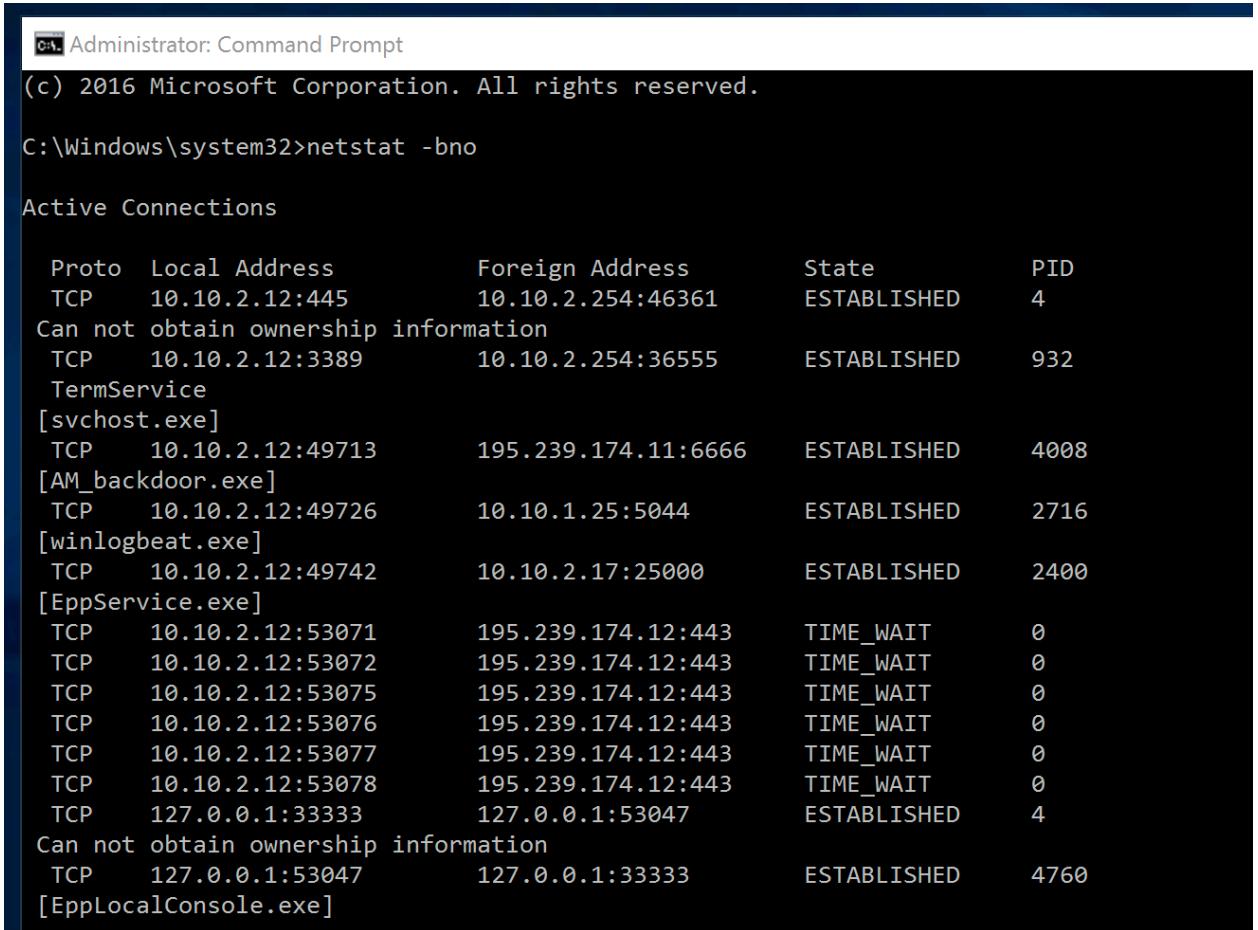


Рисунок 26. Успешное устранение уязвимости MS1710

3.2. Последствие FS Backdoory

Частым способом закрепления в скомпрометированной системе является создание вредоносного сервиса. Нарушитель может создать сервис, автоматически запускающий исполняемый файл, который устанавливает reverse shell подключение.

Установленную сессию файлового сервера с IP-адресом нарушителя (195.239.174.11) и имя запущенного процесса детектируем с помощью утилиты netstat с ключами -bno (Рисунок 27).



```

Administrator: Command Prompt
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>netstat -bno

Active Connections

  Proto  Local Address          Foreign Address        State      PID
  TCP    10.10.2.12:445        10.10.2.254:46361    ESTABLISHED  4
Can not obtain ownership information
  TCP    10.10.2.12:3389       10.10.2.254:36555    ESTABLISHED  932
  TermService
  [svchost.exe]
  TCP    10.10.2.12:49713      195.239.174.11:6666   ESTABLISHED  4008
  [AM_backdoor.exe]
  TCP    10.10.2.12:49726      10.10.1.25:5044     ESTABLISHED  2716
  [winlogbeat.exe]
  TCP    10.10.2.12:49742      10.10.2.17:25000    ESTABLISHED  2400
  [EppService.exe]
  TCP    10.10.2.12:53071      195.239.174.12:443   TIME_WAIT    0
  TCP    10.10.2.12:53072      195.239.174.12:443   TIME_WAIT    0
  TCP    10.10.2.12:53075      195.239.174.12:443   TIME_WAIT    0
  TCP    10.10.2.12:53076      195.239.174.12:443   TIME_WAIT    0
  TCP    10.10.2.12:53077      195.239.174.12:443   TIME_WAIT    0
  TCP    10.10.2.12:53078      195.239.174.12:443   TIME_WAIT    0
  TCP    127.0.0.1:33333       127.0.0.1:53047     ESTABLISHED  4
Can not obtain ownership information
  TCP    127.0.0.1:53047       127.0.0.1:33333    ESTABLISHED  4760
  [EppLocalConsole.exe]

```

Рисунок 27. Соединения, вызванные backdoor в netstat

В диспетчере задач детектируем имя процесса и узнаём расположение исполняемого файла (Рисунок 28).

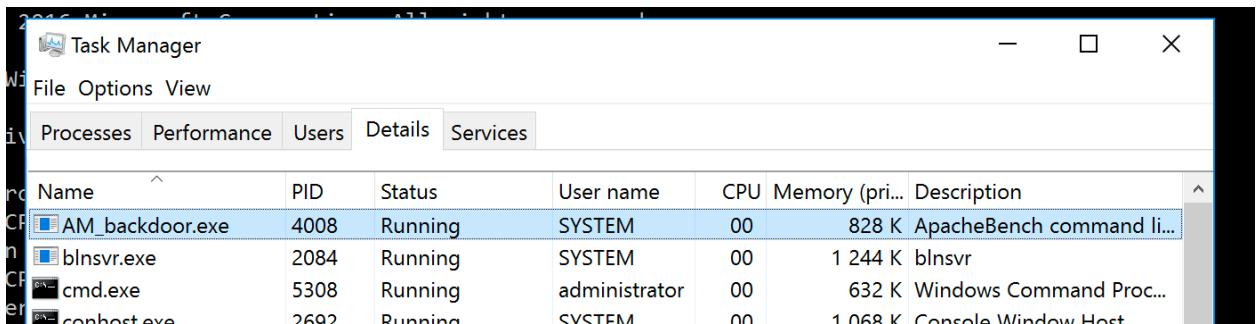


Рисунок 28. Исполняемый файл в диспетчере задач

Для устранения полезной нагрузки завершим работу исполняемого файла в диспетчере задач, удалим данный файл из директории C:\Windows\Temp (Рисунок 29).

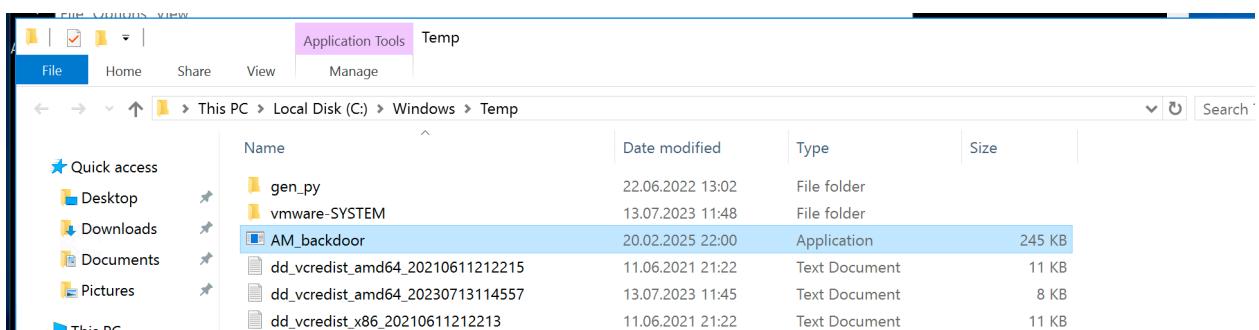


Рисунок 29. Расположение AM_backdoor.exe

После удаления исполняемого файла и остановки последствие FS Backdoor успешно устранено (Рисунок 30).

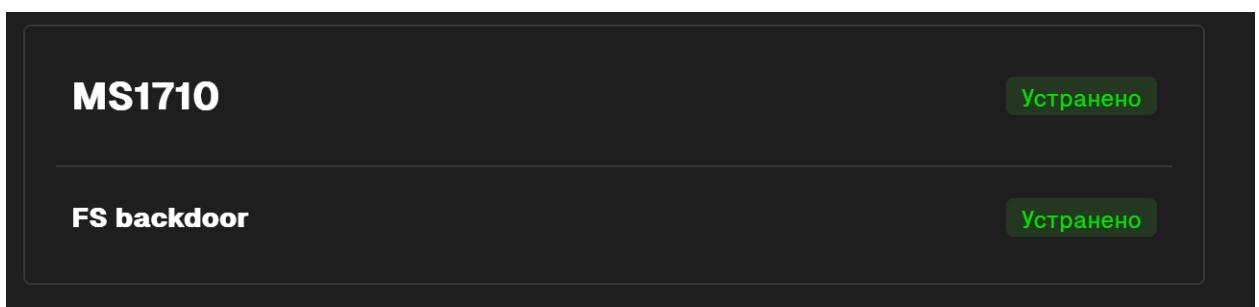


Рисунок 30. Успешное устранение последствия FS Backdoor

Вывод

В данной лабораторной работе мы успешно устранили три уязвимости и два последствия (Рисунок 31–32):

- 1) Уязвимость 1. Простой пароль пользователя веб-приложения предприятия.
- 2) Уязвимость 2. Служба RDP на порту установлена по умолчанию.

Последствие. Meterpreter-сессия.

- 3) Уязвимость 3. MS17-010 файлового сервера (CVE-2017–0144).

Последствие. FS backdoor.

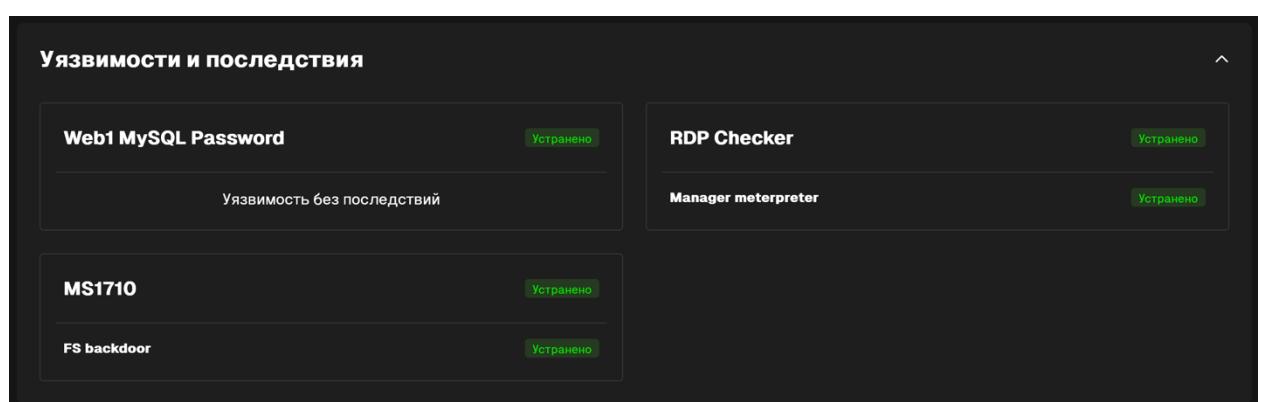


Рисунок 31. Успешное устранение уязвимостей и последствий

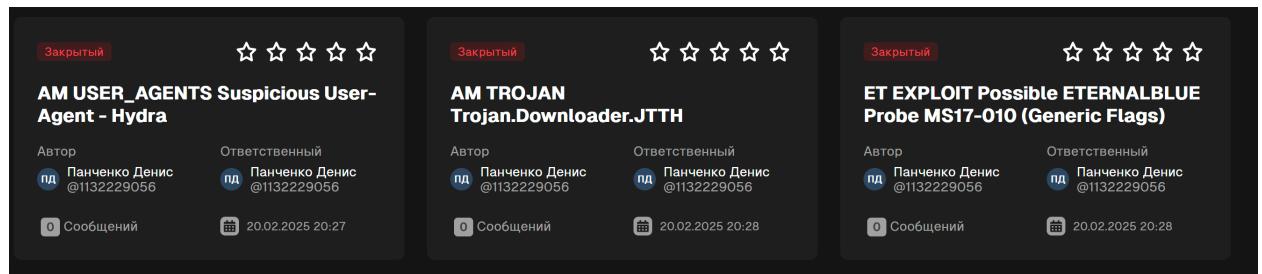


Рисунок 32. Успешное устранение уязвимостей и последствий

Кроме этого, мы выстроили примерную схему атаки, где красными линиями обозначены вредоносные действия нарушителя (Рисунок 33).

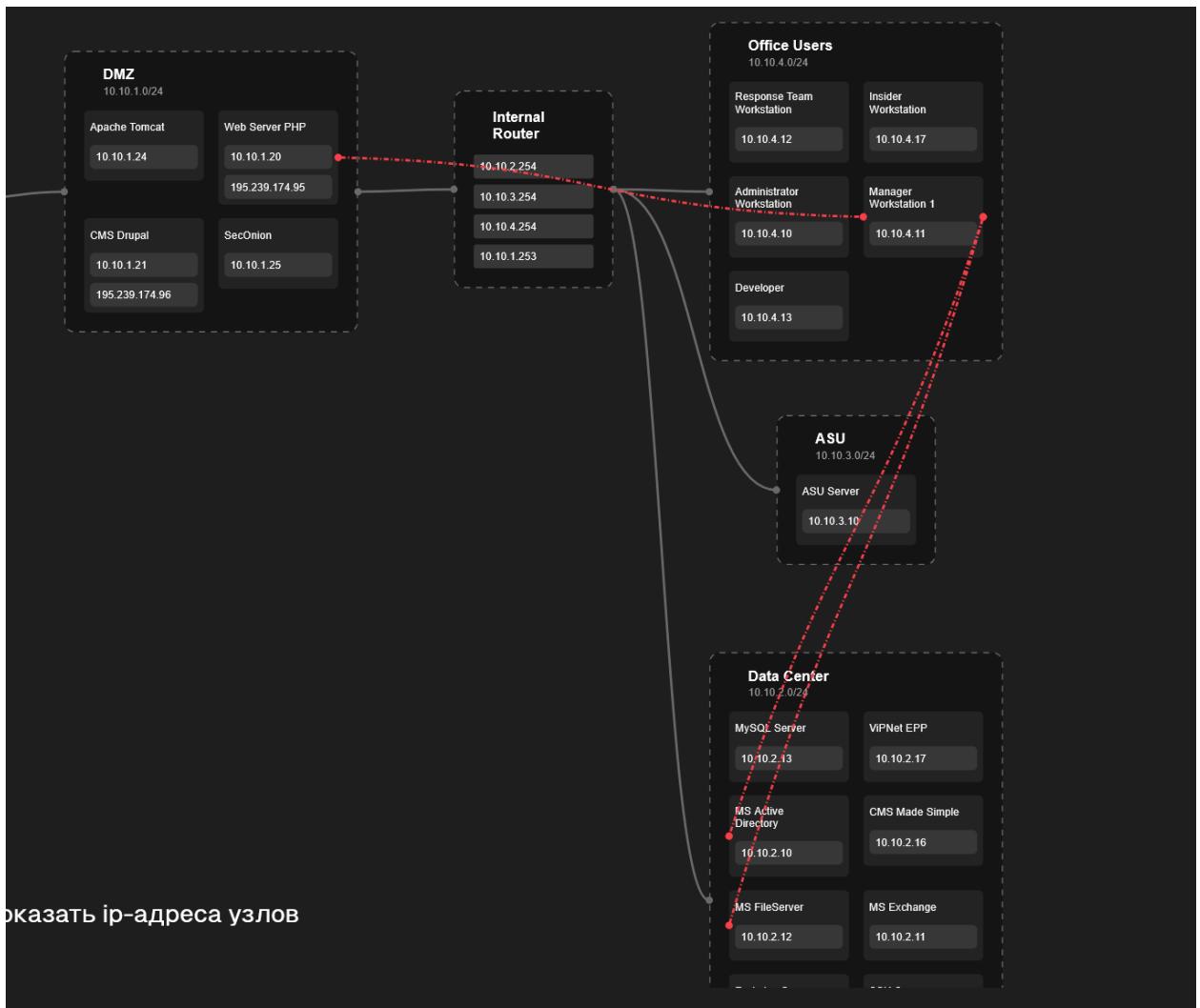


Рисунок 33. Схема атаки