Windows Active Directory Certificate Services (ADCS): методы компрометации, эскалации привилегий и защиты

Пентест. Инструменты и методы проникновения в действии

Windows Active Directory Certificate Services (ADCS): методы компрометации, эскалации привилегий и защиты

Дмитрий Антонов

https://dant.pro

https://t.me/dantpro

https://github.com/dantpro

Цель и задачи

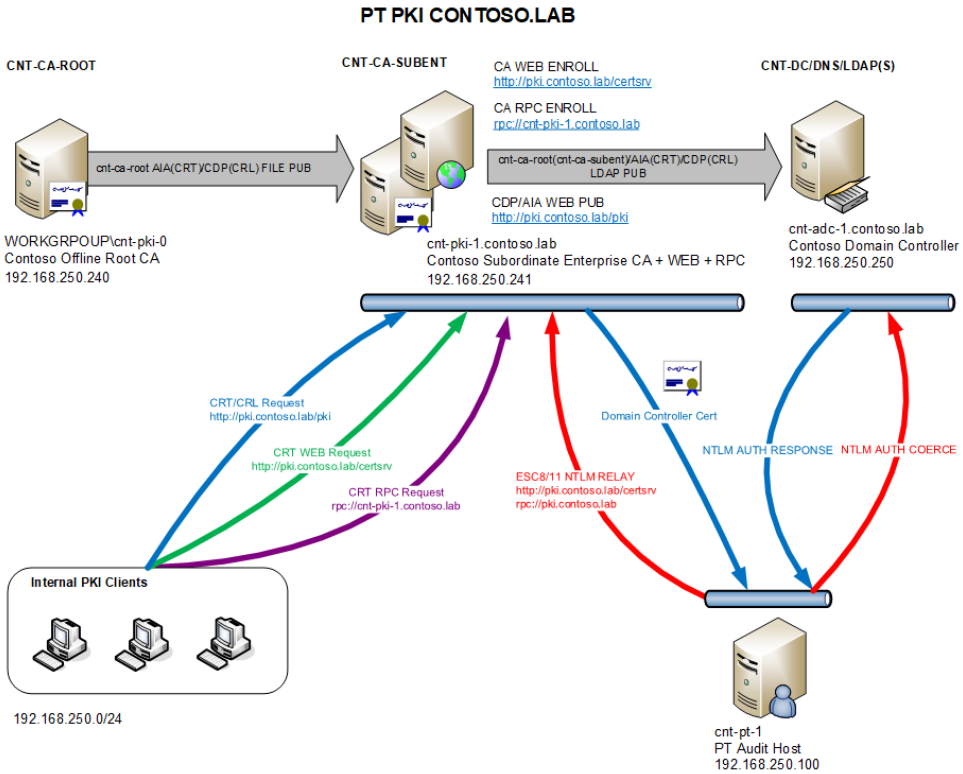
Цель: продемонстрировать основные методы компрометации домена AD и эскалации привилегий в инфраструктуре PKI Windows Active Directory Certificate Services (ADCS), предложить методы защиты

1. Развернуть виртуальную инфраструктуру PKI ADCS в домене AD Windows
2. Подготовить инструментарий для аудита этой инфраструктуры
3. Рассказать об основных методах эскалации ESC ADCS и продемонстрировать их в развёрнутой в п.1 инфраструктуре, используя инструментарий из п.2
4. Систематизировать информацию об ESC ADCS, дать рекомендации для безопасной настройки службы

Какие технологии использовались

1. Система виртуализации – Proxmox Virtual Environment (PVE)
2. Инфраструктура PKI – Windows Server 2022 ADCS
3. Операционная система для аудита инфраструктуры - Kali Linux
4. Инструмент аудита - Python-утилита Certipy

Схема лабораторного стенда



Имя компьютера	Описание
CNT-ADC-1	Контроллер домена CONTOSO.LAB
CNT-PKI-0	Корневой центр сертификации ADCS – недоменный компьютер, который должен быть выключен и физически отключен от сети после выполнения первоначальной настройки
CNT-PKI-1	Основной доменный выпускающий центр сертификации с веб-службами для запроса сертификатов и сопровождения их жизненного цикла
CNT-PT-1	Kali Linux с которого выполняем аудит

Результаты

ЧТО	ГДЕ
Документ ***Windows Active Directory Certificate Services (ADCS): методы компрометации, эскалации привилегий и защиты***	https://github.com/dantpro/_lab_pki/blob/main/contoso_adcs/windows_adcs_esc.pdf
Скрипты для развёртывания инфраструктуры PKI ADCS	https://github.com/dantpro/_lab_pki

Методы повышения доменных прививилегий с использованием ADCS, рассмотренные в работе

Повышение привилегий через уязвимые шаблоны и настройки, разрешающие указать альтернативное имя в запросе сертификата

Эскалация	Описание
ESC1	Базовая уязвимость: при запросе сертификата по уязвимому шаблону, можно указать дополнительное имя пользователя SAN, с которым возможно аутентифицироваться в домене
ESC4	Доступен на изменение и запрос сертификата любой шаблон, модифицировав который, можно сделать его уязвимым к ESC1
ESC6	Уязвимая конфигурация сервера CA, которая позволяет задать SAN в запросе сертификата по любому шаблону, сделав его уязвимым к ESC1. Возможность прямой эксплуатации исправлена в майском обновлении Windows в 2022 году, но в комбинации с уязвимыми конфигурациями ESC9 и ESC16 все ещё представляет собой серьёзную угрозу

Повышение привилегий через права на сервере CA, разрешающие выпускать сертификаты на имя других пользовталей

Эскалация	Описание
ESC2	Доступен шаблон с EKU Any Purpose, получение сертификата по которому разрешает выпустить другой сертификат клиентской аутентификации на имя любого пользователя по доступному шаблону
ESC3	Доступен шаблон с EKU Certificate Request Agent, получение сертификата по которому разрешает выпустить другой сертификат клиентской аутентификации на имя любого пользователя по доступному шаблону. ESC3 – это частный случай ESC2. т.к. EKU CRA это частный случай EKU Any Purpose

Повышение привилегий через права на сервере CA или в службах CA

Эскалация	Описание
ESC5	Права администратора на сервере CA позволяют получить закрытый ключ сертификата самого CA, которым подписываются все выпущенные сертификаты, что позволяет сгенерировать сертификат на имя любого пользователя. Выпуск такого сертификата никак не отслеживается на самом сервере CA и он будет валидным до тех пор, пока не обновился сертификат самого CA, срок жизни которого обычно большой, например 10 лет. Поэтому такой сертификат называют **Golden Certificate**
ESC7	Эскалация через права Manage CA на сервере CA, которые позволяют включить встроенный шаблон SubCA, уязвимый к ESC1, затем дать себе права Manage and Issue Certificates, которые позволяют утвердить сертификат по отклонённому запросу, получить сертификат и эскалировать права по методике ESC1

Повышения привилегий, возможные в следствие небезопасных настроек сервиса CertSvc на сервере CA

Эскалация	Описание
ESC6	Уязвимая конфигурация сервера CA, которая позволяет задать SAN в запросе сертификата по любому шаблону, сделав его уязвимым к ESC1 – **неактуально после обновления Windows, вышедшего в мае 2022 года,** однако представляет опасность в комбинации с другими небезопасными настройками
ESC11	Уязвимая конфигурация сервера CA, разрешающая нешифрованные RPC-запросы сертификатов, что делает службу выпуска сертификатов уязвимой к NTLM RELAY
ESC16	Уязвимая конфигурация сервера CA, полностью отключающая поддержку SID-расширения szOID_NTDS_CA_SECURITY_EXT OID 1.3.6.1.4.1.311.25.2, которое добавляется в сертификаты после майского обновления Windows от 2022 года

Повышения привилегий, возможные в следствие отсутствия в сертификатах расширения szOID_NTDS_CA_SECURITY_EXT

Эскалация	Описание
ESC9	Уязвимая конфигурация шаблона, когда в нем отключено SID-расширение szOID_NTDS_CA_SECURITY_EXT После **сентября 2025** года эскалация станет неактуальной, так как она требует совместимый режим работы сервиса KDC на контроллере домена, включить который будет нельзя. Однако, такая конфигурация открывает возможность использовать уязвимую конфигурацию CA ESC6, даже в полностью обновлённой инфраструктуре, эскалация по которой стала невозможной после майского обновления 2022 года
ESC16	Уязвимая конфигурация сервера CA полностью отключающая на уровне сервера, а не шаблонов, поддержку SID-расширения szOID_NTDS_CA_SECURITY_EXT, которое добавляется в сертификаты после майского обновления Windows от 2022 года. После сентября 2025 может использоваться только в комбинации с ESC6 по аналогии с ESC9

Повышения привилегий, возможные в следствие уязвимости служб выдачи сертификатов к NTLM RELAY

Эскалация	Описание
ESC8	Уязвимая к NTLM RELAY конфигурация службы запроса сертификатов через WEB-интерфейс CA Web Enrollment, что позволяет получить сертификат контроллера домена, перенаправив запрос NTLM от него на подконтрольный нам хост и, затем, на сервер CA WEB, используя один из методов принудительной аутентификации. Принуждение к аутентификации возможно, если, например, на контроллере домена работает служба Print Spooler
ESC11	Уязвимая конфигурация сервера CA, разрешающая нешифрованные RPC-запросы сертификатов, что делает службу выпуска сертификатов через RPC уязвимой к NTLM RELAY

Выводы

1. В работе наглядно показано, что сервер CA ADCS/WEB - это очень критичная система Tier 0 уровня контроллеров домена, любая ошибка в конфигурировании которой приводит к полной компрометации домена
2. После внедрения службы ADCS нужен постоянный контроль и мониторинг её работы, регулярный аудит конфигурации и выпущенных сертификатов
3. Для безопасной настройки служб ADCS CA/WEB необходимо внимательно изучить представленный документ)