

Planning Stage

Daan Van Winkel



Inhoud

1. CONTEXT & PROBLEEMSTELLING	3
1.1. Wat is de organisatiecontext?	3
1.1.1. Context	3
1.1.2. Probleemstelling	3
2. DOELSTELLING	5
2.1. Hoofddoel	5
2.2. Subdoelen	5
2.3. Eindresultaat	5
3. SCOPE	6
3.1. Binnen scope	6
3.2. Buiten scope	6
4. DELIVERABLES	7
4.1. Technisch	7
4.2. Documentatie	7
4.3. Tooling (optioneel)	7
5. PLANNING	8
5.1. Fase 1: Onderzoek en lab opzet	8
5.2. Fase 2: Analyse en reproductie van ESC-aanvalspaden	8
5.3. Fase 3: Living-off-the-Land technieken	9
5.4. Fase 4: Tooling en automatisatie	9
5.5. Fase 5: Trust attacks en aanvullende Active Directory-aanvallen	9
5.6. Fase 6: Detectieanalyse en mitigaties	10
5.7. Fase 7: Documentatie en finalisatie	10
6. RISICOANALYSE	11
6.1. Technisch	11
6.2. Inhoudelijk	11
6.3. Planning	11
7. PROJECTMANAGEMENT AANPAK	12
7.1. Bewijsstukken	12

1. Context & Probleemstelling

1.1. Wat is de organisatiecontext?

1.1.1. Context

Refracted Security is een cybersecuritybedrijf gevestigd in Lier dat onder andere **penetration testing** uitvoert voor organisaties. Tijdens deze pentests worden regelmatig omgevingen aangetroffen waarin **Active Directory Certificate Services (AD CS)** aanwezig is. AD CS wordt binnen veel Windows-omgevingen gebruikt voor certificaatbeheer, authenticatie en identiteitsvalidatie. Hierdoor vormt het een fundamenteel onderdeel van de interne beveiligingsarchitectuur van een organisatie.

In de praktijk blijkt echter dat AD CS vaak **complex is om correct te configureren en te beheren**. Veel organisaties implementeren het één keer en laten het vervolgens jarenlang ongewijzigd draaien. Hierdoor blijven configuratiefouten onopgemerkt bestaan. Wanneer deze misconfiguraties aanwezig zijn, kunnen ze worden misbruikt door een aanvaller om **privilege escalation uit te voeren of zelfs volledige controle over een Active Directory-domein te verkrijgen**.

Binnen de pentestingactiviteiten van Refracted Security worden dergelijke kwetsbaarheden steeds vaker aangetroffen. De afgelopen jaren heeft onderzoek van securitybedrijven zoals SpecterOps aangetoond dat er **verschillende specifieke aanvalspaden bestaan binnen AD CS**, vaak aangeduid als **ESC-misconfiguraties (Enterprise Security Controls)**. Elk van deze paden beschrijft een manier waarop een aanvaller certificaatfunctionaliteit kan misbruiken om privileges te verhogen.

Hoewel deze technieken bekend zijn binnen de securitycommunity, is de kennis erover vaak **verspreid over blogs, onderzoeksartikelen en technische documentatie**. Hierdoor is het moeilijk om snel een volledig overzicht te hebben van alle mogelijke aanvalspaden en hun detectiemogelijkheden.

Tijdens pentests bij Refracted Security wordt AD CS dus regelmatig aangetroffen, maar het is niet realistisch dat elke consultant **alle ESC-technieken volledig uit het hoofd kent**. Daardoor ontstaat de behoefte aan een **centrale en gestructureerde kennisbron** die consultants kunnen raadplegen wanneer ze met AD CS-omgevingen werken.

Dit stageproject speelt in op die nood door een **technische kennisbasis op te bouwen rond AD CS-aanvallen en hun detectie**, gebaseerd op zowel onderzoek als praktische reproductie.

1.1.2. Probleemstelling

Hoewel AD CS een kritische component kan zijn binnen een Active Directory-omgeving, is de beschikbare kennis over misconfiguraties vaak gefragmenteerd en moeilijk toegankelijk. Binnen Refracted Security bestaat momenteel geen interne documentatie die alle bekende AD CS-aanvalspaden systematisch beschrijft.

Dit leidt tot verschillende uitdagingen:

- AD CS is een **complex systeem** met veel configuratiemogelijkheden en afhankelijkheden.
- De verschillende **ESC-aanvalspaden zijn verspreid over meerdere externe bronnen**.
- Er bestaat geen **interne, gestructureerde documentatie** die consultants snel kunnen gebruiken tijdens pentests.
- Sommige technieken zijn moeilijk te reproduceren zonder een **labomgeving waarin de aanvallen getest kunnen worden**.
- Mogelijk ontbreken er interne scripts of tooling om **AD CS-misconfiguraties efficiënt te enumereren of te detecteren**.

Het gevolg is dat waardevolle kennis niet altijd **consistent gedeeld of hergebruikt wordt** binnen het team. Door deze informatie te centraliseren kan de efficiëntie van pentests verhoogd worden en kunnen consultants sneller kwetsbaarheden identificeren.

Het stageproject richt zich daarom op het **systematisch onderzoeken, reproduceren en documenteren van AD CS-aanvalspaden**, zodat deze kennis beschikbaar wordt binnen de interne kennisbank van Refracted Security.

2. Doelstelling

2.1. Hoofddoel

Het hoofddoel van dit project is het **technisch documenteren en structureren van Active Directory Certificate Services (AD CS) en de bijhorende ESC-aanvalspaden**, inclusief praktische reproductie van deze technieken in een gecontroleerde testomgeving.

De resultaten moeten gebruikt kunnen worden als **interne referentie voor pentesters** binnen Refracted Security.

2.2. Subdoelen

Om dit doel te bereiken worden meerdere deeldoelen uitgewerkt:

- Een **duidelijke technische uitleg van de AD CS-architectuur**
- Een **praktische analyse en documentatie van de verschillende ESC-aanvalspaden**
- Het uitwerken van **Living-off-the-Land varianten**, waarbij waar mogelijk gebruik wordt gemaakt van native Windows-tools en PowerShell
- Onderzoeken hoe deze aanvallen **gedetecteerd kunnen worden via logs en security monitoring**
- Eventueel ontwikkelen van **ondersteunende scripts of tooling** voor enumeratie en detectie
- Onderzoek naar **andere Active Directory-aanvallen**, zoals trust attacks, die relevant kunnen zijn in combinatie met AD CS

2.3. Eindresultaat

Het project moet resulteren in:

- **Professionele technische documentatie** die gebruikt kan worden binnen de interne knowledge base
- **Reproduceerbare aanvalsscenario's** in een labomgeving
- Eventuele **scripts of tools** die het analyseren van AD CS-omgevingen ondersteunen

3. Scope

3.1. Binnen scope

Binnen dit project vallen de volgende onderdelen:

- Analyse van de **Active Directory Certificate Services (AD CS) architectuur**
- Uitleg van belangrijke AD CS componenten zoals **Certificate Authorities, certificate templates en enrollment processen**
- Onderzoek en documentatie van **ESC1 tot en met ESC16**
- **ESC12 en ESC13** krijgen minder prioriteit omdat deze minder vaak voorkomen in praktijkcases
- **Opzetten van een AD CS labomgeving** met Domain Controller, Certificate Authority en testaccounts
- **Praktische reproductie van aanvalspaden** in deze labomgeving
- Documenteren van **volledige aanvalsstappen**, inclusief enumeratie, exploitatie en privilege escalation
- Gebruik van tooling zoals **Certipy en Rebeus** voor het demonstreren van de verschillende aanvalspaden
- Analyse van **detectiemogelijkheden**, bijvoorbeeld via Windows Event Logs en andere security telemetry
- Structureren van alle resultaten in **technische documentatie voor de interne knowledge base van Refracted Security**
-

3.2. Buiten scope

De volgende onderwerpen vallen buiten het project:

- **Implementatie van oplossingen in productieomgevingen bij klanten**
- Aanpassingen aan **live infrastructuren of bedrijfsomgevingen**
- **Volledige herontwerpen van enterprise PKI-architecturen**
- Ontwikkelen van **volwaardige enterprise security tools of frameworks**
- **Opzetten van een volledige Security Operations Center (SOC) infrastructuur**
- Implementatie van **complete SIEM monitoring of detectieregels**
- Analyse van **Active Directory aanvalstechnieken die geen relatie hebben met AD CS of Trusts**
- **Security awareness trainingen of workshops voor eindgebruikers**
- Juridische of compliance analyse rond **PKI governance**
- Integratie van ontwikkelde scripts in **bestaande enterprise securityplatformen**

4. Deliverables

4.1. Technisch

- Gedetailleerde documentatie van **ESC-aanvalspaden**
- **PowerShell-varianten** van aanvalstechnieken waar mogelijk
- Eventuele **scripts of tools** ontwikkeld tijdens het project

4.2. Documentatie

- Theoretische uitleg van **Active Directory Certificate Services**
- **Technische handleidingen per ESC-aanvalspad**
- Analyse van **detectiemogelijkheden**, bijvoorbeeld via Windows Event Logs of SIEM-systemen
- **Mitigatieadvies** voor het beveiligen van AD CS-omgevingen

4.3. Tooling (optioneel)

Indien haalbaar kan aanvullende tooling worden ontwikkeld, bijvoorbeeld voor:

- AD CS enumeratie
- Detectie van mogelijke misconfiguraties
- Rapportage van kwetsbaarheden

5. Planning

Het project loopt over een periode van **14 weken** en volgt een gefaseerde aanpak. In plaats van strikt per week te werken, wordt het project opgesplitst in **logische onderzoeks- en implementatiefases**. Elke fase bouwt verder op de vorige en heeft een duidelijke technische focus.

Deze aanpak sluit beter aan bij een onderzoeksproject waarin sommige onderdelen meer tijd kunnen vragen dan initieel verwacht.

5.1. Fase 1: Onderzoek en lab opzet

In de eerste fase wordt een **labomgeving opgezet waarin AD CS-aanvallen veilig kunnen worden getest en gereproduceerd**. Deze omgeving bestaat uit een Domain Controller, een Certificate Authority en verschillende testaccounts.

Parallel met de technische setup wordt een **grondige studie van Active Directory Certificate Services** uitgevoerd. Hierbij wordt gekeken naar de architectuur, certificaattemplates, enrollmentmechanismen en de rol van certificaten binnen Active Directory-authenticatie.

Tijdens deze fase wordt ook gestart met de **eerste ESC-aanvalspaden**, zodat de basis van de documentatiestructuur meteen duidelijk wordt.

Resultaten van deze fase:

- Werkende **AD CS labomgeving**
- Basiskennis van **AD CS architectuur**
- Eerste documentatie van **ESC-aanvalspaden**

5.2. Fase 2: Analyse en reproductie van ESC-aanvalspaden

In deze fase ligt de focus op het **systematisch analyseren en reproduceren van de verschillende ESC-misconfiguraties** die binnen AD CS kunnen voorkomen.

Voor elk aanvalspad wordt een vaste structuur gevolgd:

- Technische uitleg van de kwetsbaarheid
- Reproductie van de misconfiguratie in de labomgeving
- Praktische exploitatiestappen
- Validatie van het aanvalsscenario

Omdat sommige ESC-technieken in de praktijk vaker voorkomen dan andere, wordt prioriteit gegeven aan de paden die **het meest relevant zijn tijdens pentests**. Minder voorkomende paden worden later uitgewerkt.

Resultaten van deze fase:

- Technische documentatie van **ESC1 t.e.m. ESC16**
- Werkende **labscenario's per aanvalspad**
- Praktische exploitatiestappen en command workflows

5.3. Fase 3: Living-off-the-Land technieken

Veel aanvallen binnen Active Directory kunnen worden uitgevoerd met **native Windows-tools** in plaats van externe tooling. Dit wordt vaak aangeduid als **Living-off-the-Land (LotL)**.

In deze fase wordt onderzocht hoe AD CS-aanvallen kunnen worden uitgevoerd met:

- **PowerShell**
- **Native Windows utilities**
- Bestaande functionaliteit binnen Active Directory

Het doel is om alternatieve aanvalsmethoden te documenteren die minder afhankelijk zijn van gespecialiseerde tools.

Resultaten van deze fase:

- PowerShell-varianten van aanvalstechnieken
- LotL-workflows voor AD CS-aanvallen
- Documentatie van alternatieve aanvalsmethoden

5.4. Fase 4: Tooling en automatisatie

Na het analyseren van de aanvalspaden wordt onderzocht of bepaalde stappen **geautomatiseerd kunnen worden**.

In deze fase kan een **PowerShell-script ontwikkeld worden dat AD CS-omgevingen analyseert** en mogelijke misconfiguraties identificeert. Het script kan bijvoorbeeld:

- AD CS componenten enumereren
- Certificaattemplates analyseren
- Mogelijke ESC-misconfiguraties detecteren

Het doel is niet om een volledig product te ontwikkelen, maar eerder een **technische demonstratie van automatisatie binnen AD CS-analyse**.

Resultaten van deze fase:

- Prototype **enumeratie- of detectiescript**
- Documentatie van de gebruikte technieken

5.5. Fase 5: Trust attacks en aanvullende Active Directory-aanvallen

Naast AD CS-aanvalspaden worden ook **andere Active Directory-aanvallen onderzocht die relevant kunnen zijn in combinatie met certificaatgebaseerde authenticatie**.

Een belangrijk voorbeeld hiervan zijn **trust attacks**, waarbij relaties tussen verschillende domeinen of forests misbruikt kunnen worden.

Tijdens deze fase wordt onderzocht:

- Hoe trustrelaties werken binnen Active Directory

- Hoe deze relaties misbruikt kunnen worden
- Of er mogelijke interacties zijn met AD CS
- Andere aanvallen die in optie zijn:
- GoldenGSMA
- Aanvallen met C2 server

Resultaten van deze fase:

- Documentatie van **trust attacks**
- Analyse van mogelijke link met **AD CS-aanvallen**

5.6. Fase 6: Detectieanalyse en mitigaties

In deze fase wordt gekeken naar **defensieve aspecten** van de onderzochte aanvalspaden.

Voor elke aanval wordt onderzocht:

- Welke **Windows Event Logs** worden gegenereerd
- Welke sporen zichtbaar zijn in **security monitoring**
- Hoe organisaties deze aanvallen kunnen **detecteren of voorkomen**

Daarnaast worden **mitigaties en best practices** uitgewerkt voor het beveiligen van AD CS-omgevingen.

Resultaten van deze fase:

- Detectieanalyse per aanvalspad
- Overzicht van relevante **security events**
- Mitigatie- en hardeningrichtlijnen

5.7. Fase 7: Documentatie en finalisatie

In de laatste fase worden alle resultaten samengebracht tot een **gestructureerd technisch einddocument**.

Alle aanvalspaden worden opnieuw gevalideerd in de labomgeving en voorzien van:

- Screenshots
- Logs
- Scriptoutputs
- Praktische bewijsstukken

De uiteindelijke documentatie wordt zo opgesteld dat deze **bruikbaar is als interne kennisbron voor pentesters** binnen Refracted Security.

Resultaten van deze fase:

- Volledige technische documentatie
- Reproduceerbare labscenario's
- Eventuele scripts of tooling
- Gestructureerde knowledge base content.

6. Risicoanalyse

6.1. Technisch

- Problemen met **AD CS configuratie in de labomgeving**
- Beperkingen van de testomgeving

6.2. Inhoudelijk

- Overlap tussen verschillende **ESC-aanvalspaden**
- Afhankelijkheid van **externe onderzoeksbronnen**

6.3. Planning

- Onderschatting van de **technische complexiteit**
- Ontwikkeling van tooling kan **meer tijd vragen dan voorzien**

7. Projectmanagement aanpak

Het project volgt een **iteratieve aanpak per aanvalspad**.

Voor elke techniek wordt dezelfde workflow toegepast:

- Analyse
- Exploitatie
- Detectie
- Mitigatie

Daarnaast wordt gewerkt met:

- **Wekelijkse feedbackmomenten met de stagebegeleider bij Refracted Security**
- Een **strikte documentatiestructuur in Markdown**
- Systematische verzameling van bewijsstukken

7.1. Bewijsstukken

- Screenshots
- Logs
- Scriptversies
- Testresultaten



THOMAS
MORE