

AD CS Security *Research Internship*

Reflectie

Daan Van Winkel

Student Bachelor in de Elektronica-ICT – Cloud & Cyber Security Ethical Hacking Traject

Inhoudsopgave

1. INLEIDING _____ ERROR! BOOKMARK NOT DEFINED.
2. INHOUDELIJKE REFLECTIE _____ ERROR! BOOKMARK NOT DEFINED.
3. PERSOONLIJKE REFLECTIE _____ ERROR! BOOKMARK NOT DEFINED.

1. Inleiding

Tijdens deze stage kreeg ik de kans om mij verder te verdiepen in Active Directory Certificate Services (AD CS), privilege escalation technieken en detectie binnen een Windows-omgeving. Het doel van de stage was om verschillende AD CS ESC attack paths te onderzoeken, deze praktisch uit te werken in een labo-omgeving en te analyseren hoe detecteerbaar deze aanvallen zijn binnen een monitoringplatform zoals Wazuh.

Deze reflectie kijkt terug op zowel de inhoudelijke als persoonlijke groei tijdens de stageperiode. In het eerste deel bespreek ik de gerealiseerde resultaten, de huidige status van het project en mogelijke aanbevelingen voor de toekomst. Daarna volgt een persoonlijke reflectie waarin ik terugblik op wat ik geleerd heb, welke uitdagingen ik ben tegengekomen en hoe ik hierin gegroeid ben.

2. Inhoudelijke reflectie

Tijdens deze stage heb ik gewerkt rond het onderzoeken en documenteren van verschillende Active Directory Certificate Services (AD CS) ESC attack paths. Het project bestond uit zowel een offensief als defensief luik. Enerzijds lag de focus op het begrijpen en reproduceren van privilege escalation technieken binnen AD CS, anderzijds op het onderzoeken hoe deze activiteiten zichtbaar gemaakt kunnen worden binnen een SIEM-oplossing zoals Wazuh.

Een groot deel van de stage bestond uit research en praktische testing binnen een eigen labo-omgeving. Ik heb verschillende ESC attack paths onderzocht, waaronder onder andere ESC1 tot ESC13. Voor elk attack path heb ik documentatie opgesteld waarin de werking, reconnaissance, exploitatie, mitigatie en security impact duidelijk werden uitgewerkt. Het doel hiervan was niet alleen om de aanval technisch te begrijpen, maar ook om deze op een gestructureerde en begrijpbare manier te documenteren.

Naast de aanvalstechnieken zelf heb ik ook gekeken naar detectie en monitoring. Hierbij onderzocht ik welke logs en events gegenereerd worden tijdens het uitvoeren van bepaalde AD CS-aanvallen. In het begin verwachtte ik dat veel van deze tools relatief eenvoudig detecteerbaar zouden zijn. Tijdens het testen bleek echter dat tools zoals Certipy vaak zeer efficiënt werken en relatief weinig opvallende activiteiten genereren. Hierdoor werd het detectieluik moeilijker dan oorspronkelijk verwacht. Dit zorgde ervoor dat ik mijn aanpak meerdere keren moest aanpassen en verder moest onderzoeken welke indicatoren nog wel bruikbaar zijn voor detectie.

Een andere belangrijke realisatie tijdens het project was hoe uitgebreid AD CS eigenlijk is. In het begin leek het onderwerp relatief afgebakend, maar naarmate ik dieper onderzoek deed, werd duidelijk hoeveel verschillende aanvalspaden, configuraties en uitzonderingen er bestaan. Hierdoor was het soms moeilijk om duidelijke grenzen te bepalen binnen het project. Ik heb daarom geprobeerd om de focus vooral te leggen op de meest relevante en realistisch misbruikbare aanvalstechnieken. Het project is momenteel grotendeels afgewerkt, maar er zijn nog enkele zaken die verder verfijnd kunnen worden tijdens de laatste week van de stage. Vooral het verbeteren van bepaalde documentatie, het verder analyseren van enkele detectiescenario's en het structureren van de finale resultaten zijn nog aandachtspunten. Toch ben ik tevreden met de vooruitgang die reeds gemaakt is en het niveau van detail dat ondertussen bereikt werd.

De documentatie en testen die tijdens deze stage werden opgesteld kunnen in de toekomst gebruikt worden als referentie voor zowel offensieve security testing als awareness rond AD CS hardening en detectie. Omdat AD CS in veel organisaties aanwezig is maar vaak onvoldoende beveiligd wordt, kan deze informatie bijdragen aan een beter begrip van de risico's rond certificaatgebaseerde authenticatie. Als advies voor de toekomst zou ik aanraden om binnen organisaties meer aandacht te besteden aan het hardenen van AD CS-omgevingen en het regelmatig auditen van certificate templates en CA-configuraties. Daarnaast denk ik dat verdere investering in monitoring en logging rond certificate services belangrijk blijft, aangezien misbruik van certificaten vaak minder zichtbaar is dan klassieke aanvalstechnieken.

3. Persoonlijke reflectie

Deze stage heeft voor mij persoonlijk een grote meerwaarde gehad. Ik kreeg de kans om mij gedurende meerdere weken volledig te verdiepen in een onderwerp dat mij sterk interesseert binnen cybersecurity. Vooral het feit dat ik zelfstandig onderzoek kon uitvoeren en veel vrijheid kreeg binnen het project maakte deze stage zeer leerrijk.

Op technisch vlak heb ik vooral veel bijgeleerd over Active Directory, Kerberos-authenticatie, certificate services en privilege escalation technieken. Voor de start van de stage had ik al een basiskennis van Active Directory attacks, maar AD CS was grotendeels nieuw voor mij. Door de verschillende attack paths zelf op te zetten en te testen, heb ik een veel beter inzicht gekregen in hoe certificaatgebaseerde authenticatie werkt en waarom bepaalde misconfiguraties zo gevaarlijk kunnen zijn.

Naast de technische kennis heb ik ook verschillende andere competenties ontwikkeld. Eén van de belangrijkste was zelfstandig probleemoplossend denken. Tijdens het project liep ik regelmatig vast op problemen waarvoor geen directe oplossing beschikbaar was. Sommige technieken werkten anders door patching of specifieke configuraties binnen Windows-omgevingen. Hierdoor moest ik vaak zelf verder onderzoeken, testen uitvoeren en documentatie vergelijken om tot een oplossing te komen. Dit heeft mij geleerd om gestructureerder en geduldiger om te gaan met technische problemen.

Ook op vlak van documentatie en organisatie ben ik gegroeid. Omdat het project veel research, commands, testen en notities bevatte, werd het belangrijk om alles goed te structureren. Ik heb geprobeerd om mijn documentatie consequent en overzichtelijk te houden zodat informatie later gemakkelijk teruggevonden kon worden. In vergelijking met eerdere projecten merk ik dat ik hier veel consistentier in geworden ben. Daarnaast heb ik ook ervaren hoe verschillend een professionele werkomgeving is tegenover een schoolomgeving. Tijdens de stage werk je niet enkel aan een opdracht, maar maak je deel uit van een professionele omgeving waar zelfstandigheid, communicatie en verantwoordelijkheid belangrijk zijn. Regelmatige feedbackmomenten en technische discussies hielpen mij om duidelijker te communiceren over mijn bevindingen en keuzes.

Een uitdaging tijdens de stage was vooral het afbakenen van het project. Omdat AD CS een zeer uitgebreid onderwerp is, was het soms moeilijk om te bepalen hoeveel diepgang nodig was binnen bepaalde onderdelen. Ik merkte dat ik soms te lang bleef doorgaan op specifieke details of edge cases. Door beter prioriteiten te leren stellen kon ik hier uiteindelijk beter mee omgaan.

Algemeen kijk ik zeer positief terug op deze stageperiode. Ik heb niet alleen veel technische kennis opgedaan, maar ben ook persoonlijk gegroeid op vlak van zelfstandigheid, probleemoplossend denken en professionele communicatie. De stage heeft mijn interesse in cybersecurity verder versterkt en gaf mij een realistischer beeld van hoe onderzoek en security testing binnen een professionele omgeving verlopen.