ACEN

STAGE

Cybersecurity: Identiteit onder vuur

Beschrijving van de opdracht

Bijna elke moderne cyberaanval begint of eindigt met een gecompromitteerde identiteit. Tijdens deze stage zie je beide kanten van dat verhaal: eerst val je zelf een realistische identiteitsomgeving van een onderneming aan, daarna zorg je ervoor dat diezelfde aanvallen niet langer werken.

Tijdens deze stage neem je de rol op van Junior Security Consultant en focus je op het beveiligen van digitale identiteiten binnen een bedrijfsomgeving. Active Directory (AD) en Microsoft Entra ID, de ruggengraat van identiteit in de meeste organisaties, staan centraal in deze opdracht.

Je werkt in een bestaand, realistisch identiteitslab dat bestaat uit een on-premises Active Directory-omgeving en, afhankelijk van de duur van je stage, een gesynchroniseerde Microsoft Entra ID-tenant. Vervolgens onderzoek je hoe identiteitsgebaseerde aanvallen worden uitgevoerd, spoor je zwakke plekken in de omgeving op en onderzoek je in een gecontroleerde labomgeving hoe aanvallers deze kwetsbaarheden misbruiken.

Op basis van je bevindingen beoordeel je de bijbehorende risico's, implementeer je beveiligingsmaatregelen met Silverfort en evalueer je de doeltreffendheid van de verbeteringen. Doorheen het project leer je denken vanuit het perspectief van zowel een aanvaller als een verdediger, en ontwikkel je het vermogen om de kloof tussen beide te begrijpen en te overbruggen.

Je krijgt een roadmap met de doelstellingen, mijlpalen en evaluatiemomenten, maar je bent zelf verantwoordelijk voor de aanpak, de keuze van de tools, het onderzoek en de diepgang van je analyse. Een basiskennis van netwerken en authenticatieconcepten zoals Kerberos en NTLM helpt je om snel aan de slag te gaan. Eventuele kennishiaten worden tijdens de eerste weken van de stage weggewerkt.

De labomgeving is al opgezet en gedocumenteerd, zodat je je vanaf dag één kunt richten op aanvalsonderzoek, technieken voor privilege-escalatie, scenario's van identiteitsmisbruik en de bijbehorende verdedigingsmaatregelen. Onderweg werk je met tools die in het vakgebied veel gebruikt worden, zoals BloodHound, Impacket, Rubeus, Mimikatz en PingCastle, en verken je scenario's zoals Kerberoasting, AS-REP roasting, DCSync en ACL-misbruik. Daarnaast ontwikkel je je eigen scripts en tools om aanvallen en beveiligingscontroles te automatiseren.

Tijdens de stage presenteer je regelmatig je voortgang, onderzoeksresultaten en aanbevelingen. Deze presentaties vormen een belangrijk onderdeel van de evaluatie en zorgen ervoor dat het project afgestemd blijft op de leerdoelen. Aan het einde van de stage lever je een uitgebreid rapport op met een overzicht van de vastgestelde risico's, de uitgevoerde tests, de geïmplementeerde beveiligingsmaatregelen en strategische aanbevelingen voor een fictieve klant.

Doelstellingen

- De aangeleverde Active Directory-labomgeving analyseren en identiteitsgerelateerde beveiligingszwaktes opsporen.
- Veelvoorkomende Active Directory-aanvalstechnieken reproduceren en demonstreren met gangbare tools uit de sector en je eigen scripts.
- Beveiligingsverbeteringen implementeren en valideren via Active Directory-hardening en Silverfort-maatregelen.
- De doeltreffendheid van verdedigingsmaatregelen meten door het succes van aanvallen vóór en na mitigatie te vergelijken.
- Afhankelijk van de duur van de stage de analyse uitbreiden naar hybride identiteitsscenario's in Microsoft Entra ID.
- Op basis van de bevindingen concrete technische en bedrijfsgerichte beveiligingsaanbevelingen formuleren.

Technologieën & concepten

- **Entra ID**
- **Active Directory**
- **Applicatieontwikkeling**
- **Red Teaming**
- **Silverfort**
- **Blue Teaming**
- **Netwerken**
- **Vulnerability Assessment**

Aanpak & tijdlijn

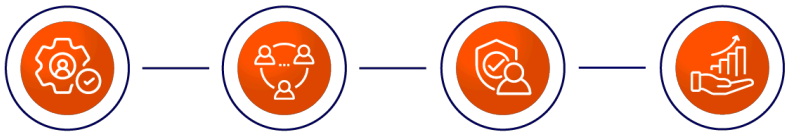
Je werkt in korte iteraties met regelmatige check-ins en feedback van je begeleider, zodat je altijd weet waar je staat en snel kunt bijsturen. De stage verloopt grofweg in de volgende fases:

1. **Onboarding (week 1–2):** maak kennis met het lab, de roadmap en Silverfort, en werk eventuele kennishiaten weg.
2. **Aanvalsonderzoek:** breng het aanvalsoppervlak van het lab in kaart en reproduceer identiteitsgebaseerde aanvallen.
3. **Hardening en Silverfort:** implementeer Active Directory-hardeningmaatregelen en Silverfort-maatregelen.
4. **Meten en rapporteren:** herhaal de aanvallen, vergelijk de resultaten vóór en na mitigatie, en werk je rapport en aanbevelingen af.

Wat je eraan overhoudt

- Praktijkervaring met realistische aanvals- en verdedigingstechnieken rond identiteit in een veilige labomgeving.
- Praktische ervaring met Silverfort, een modern platform voor identiteitsbeveiliging.
- Persoonlijke coaching door ervaren security consultants van ACEN gedurende de hele stage.
- Presentatie- en rapportagevaardigheden die elke security consultant nodig heeft.
- Een eindrapport en demo's die je aan je portfolio kunt toevoegen.
- Een kijkje achter de schermen bij ACEN, een Europees adviesbureau in cybersecurity dat organisaties helpt hun cyberrisico te begrijpen, te beheersen en te verkleinen.

Profiel



De ideale stagiair is in de eerste plaats gemotiveerd om zijn of haar vaardigheden te verbeteren en een nieuw technologisch domein te leren kennen.

Een student cybersecurity, systeem- en netwerkbeheer of een verwante richting, die nieuwsgierig is, geen genoegen neemt met "het werkt gewoon" als antwoord en graag dingen uitlegt. Praktijkervaring met Active Directory is een pluspunt. Voorafgaande ervaring met Silverfort is niet vereist; je maakt er tijdens de stage kennis mee. Vertrouwdheid met Windows Server, PowerShell en minstens één scripttaal is handig. Goede schriftelijke en mondelinge communicatie is essentieel.

Voldoe je niet aan alle criteria? Solliciteer toch. Nieuwsgierigheid en motivatie zijn voor ons belangrijker dan een perfecte match.

Contactgegevens

Contactpersoon	Cindy Van den Hoecke	**cindy.vandenhoecke@acen.eu**
Stagebegeleider	Kelvin Bogaerts	**Kelvin.Bogaerts@acen.eu**