**Projectplan**

***Pentest Cubics IT***

*Cubics IT*

***Tilburg***

Hidde van Brouwershaven   
Luc van den Acker   
Raoul Goorden   
Stan Akkermans

#### Versie

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Versie** | **Datum** | **Auteur(s)** | **Wijzigingen** | **Status** |
| 1 | 05-10-2022 | Luc van den Acker | Nieuw projectplan ingevuld | Klaar |
|  |  |  |  |  |
|  |  |  |  |  |

Inhoudsopgave

[1. Projectopdracht 4](#_Toc118888297)

[1.1 Context 4](#_Toc118888298)

[1.2 Doel van het project 4](#_Toc118888299)

[1.3 De opdracht 4](#_Toc118888300)

[1.4 Scope 4](#_Toc118888301)

[o Randvoorwaarden 4](#_Toc118888302)

[o Eindproducten 5](#_Toc118888303)

[1.5 Hoofdvraag 5](#_Toc118888304)

[1.6 Deelvragen 5](#_Toc118888305)

[1.6.1 Wat is C-fence? 5](#_Toc118888306)

[1.6.2 Hoe handelt C-fence bij cyber aanvallen? 5](#_Toc118888307)

[1.6.3 Wat is een forward-node? 5](#_Toc118888308)

[1.6.4 Wat voor tools zijn er om netwerken te scannen? 5](#_Toc118888309)

[1.6.5 Hoe reageert C-fence op netwerk scans? 6](#_Toc118888310)

[1.6.6 Hoe kunnen buitenstaanders verbinding maken met C-fence? 6](#_Toc118888311)

[1.6.7 Wat kan er fout gaan vanaf de forward node van een klant? 6](#_Toc118888312)

[2. Aanpak en Planning 7](#_Toc118888313)

[2.1 Aanpak 7](#_Toc118888314)

[**2.1.1** **Test aanpak** 7](#_Toc118888315)

[2.2 Onderzoeksmethoden 7](#_Toc118888316)

[2.3 Tijdplan 7](#_Toc118888317)

[3. Projectorganisatie 8](#_Toc118888318)

[3.1 Teamleden 8](#_Toc118888319)

[3.2 Communicatie 8](#_Toc118888320)

# Projectopdracht

## Context

Cubics is een IT-consultancy bedrijf met vestigingen in Tilburg en Eindhoven. Cubics biedt verschillende IT-services aan. Een van die services is *C-fence*. C-fence is een open-source platform voor network security monitoring (NSM) en Enterprise security monitoring (ESM). NSM is het bewaken van een netwerk. Het systeem is proactief wanneer het gebruikt wordt om kwetsbaarheden te identificeren. C-fence is een oplossing bedoeld voor iedereen. Zowel grote als kleine bedrijven.

## Doel van het project

Om de veiligheid en kwaliteit van C-fence in kaart te brengen, gaan we een pentest uitvoeren, waarbij verschillende onderdelen van het systeem getest gaan worden.

## De opdracht

Met behulp van een aantal (door cubics aangeboden) IP-adressen gaan we proberen om een netwerk waar C-fence op draait in kaart te brengen. Dit zal een forward node op een live omgeving van cubics zelf uit Tilburg of Eindhoven zijn.

Ook gaan we proberen C-fence te benaderen vanuit een klantomgeving om een insider threat te simuleren. Hiervoor zullen we een forward node op een smart switch installeren. Tussen deze forward node en C-fence zal een verbinding zitten die we gaan testen.

## Scope

|  |  |
| --- | --- |
| **Tot het project behoort:** | **Tot het project behoort niet:** |
| Onderzoek naar de benodigde middelen/technieken | Exploitatie van kwetsbaarheden |
| Pentest m.b.v. verschillende IP-adressen van Cubics | Applicaties pentesten |
| Het testen van C-fence vanuit een klantomgeving. | Social engineering |
| Verslag/rapport van de resultaten |  |

## Randvoorwaarden

Om tot een succesvol project te komen hebben we de volgende dingen nodig vanuit Cubics:

* IP-adressen waar C-fence op gehost wordt.
* IP-adressen van een forward node.
* Contactgegevens
* Begeleiding tijdens het project van de contactpersoon.
* Hulp bij het installeren van de forward node.
* Verbinding tussen C-fence en onze forward node.

Verder hebben we het volgende vanuit Fontys nodig:

* Begeleiding door de semestercoach.
* Een smartswitch om een forward node te hosten.
* Een teams omgeving.
* Office-software.
* Een virtual machine omgeving (Kali Linux).

Mochten één of meerdere van de boven genoemde zaken niet aangeleverd zijn dan dienen we met de semestercoach te bespreken welke stappen te ondernemen om toch tot een succesvol project te komen.

## Eindproducten

Aan het einde van het project rapporteren we alle bevindingen in een verslag, op basis van dit verslag zullen wij een advies aan de stakeholder geven. Het verslag en advies bespreken we vervolgens met Cubics. Ook leveren we een presentatie waarin wij de bevindingen uit dit verslag bespreken. Deze presentatie zal aan de semestercoach worden gegeven, vooraf zal met de stakeholder worden afgesproken wat er wel en niet besproken zal worden in de presentatie.

## Hoofdvraag

Wat voor kwetsbaarheden bevat de integrale oplossing van het C-fence platform?

## Deelvragen

### Wat is C-fence?

C-fence is een SIEM voor netwerken dat op basis van security onion is gemaakt. C-Fence levert forward nodes die een overzicht geven in het netwerk en alerts doorsturen naar een SOC.

Om te herkennen voor wat de nodes alerts moeten sturen heeft C-Fence een uitgebreide database aan aanvallen waardoor C-Fence kan reageren als iemand een aanval doet naar een van de klanten van Cubics.

### Hoe handelt C-fence bij cyber aanvallen?

Als er een aanval is op een netwerk waar C-Fence een forward node in heeft kijkt C-Fence of ze herkennen wat er binnen komt en als het overeen komt met een aanval uit hun database krijgt Cubics een alert binnen waar ze gelijk op kunnen reageren. Daarnaast heeft C-Fence heeft ook een zero trust manier van werken waardoor er minder in het netwerk kan komen.

### Wat is een forward-node?

### Wat voor tools zijn er om netwerken te scannen?

Nmap

Wanneer we het over netwerk scans hebben, is nmap een van de bekendste gratis tools beschikbaar. Nmap biedt een groot aanbod aan van verschillende type netwerk scans, variërend van lichte, stealthy scans, tot zware en luidruchtige scans. Hieronder staan een aantal verschillende type scans die toegepast gaan worden in de pentest voor Cubics IT, inclusief waarom deze variant zinvol is voor de scope van het project.

Stealth scans

Een stealth scan is bedoeld om zo onopvallend mogelijk te zijn voor de netwerkbeheerders. Een stealth scan stuurt een SYN(synchorization) pakket. Een Syn pakket wordt gebruikt om een verbinding op te zetten met de server. Vervolgens zou er vanaf de server een ACK(Acknowledgment) pakket verstuurd moeten worden, waarop de client ook een ACK- pakket verstuurt. Als dit proces klaar is, staat er een verbinding tussen de client en de server. Om deze verbinding af te breken wordt een RST-pakket naar de server gestuurd. Dit RST-pakket zorgt ervoor dat stealth scans mogelijk zijn. Bij een stealth scan wordt namelijk het RST-pakket verstuurd vanaf de client voordat een ACK-pakket naar de server gaat, waardoor er nooit een verbinding opgezet wordt. Stealth scans worden dus niet gedetecteerd door standaard servers, maar door Intrusion Detection Systems zouden ze wel gedetecteerd moeten worden.

Door stealth scans uit te voeren wordt getest hoe goed de NIDS/HIDS van Cubics functioneren, en hoe er gereageerd wordt door de security officers van Cubics. De verwachtig is dat een stealth scan direct opgemerkt wordt Door C-fence. Hoe er binnen Cubics gereageerd wordt, is lastiger te voorspellen.

NULL scans

Met een NULL scan wordt letterlijk een lege TCP header naar de server verstuurd. Dit houdt in dat er geen SYN, ACK of RST pakket verstuurd wordt. Omdat er geen concrete data beschikbaar is voor de server, wordt er niet echt op gereageerd.

Ook NULL-scans kunnen gedetecteerd worden door NIDS/HIDS systemen, maar omdat er regelmatig incorrecte pakketjes verstuurd worden, is de kans relatief groot dat er niet gereageerd wordt op zo’n scan.

Xmas scan

Voor een xmas scan worden de PSH, URG en FIN flags van de TCP header gemanipuleerd. Wanneer zo’n header in wireshark bekeken wordt, is te zien dat afwisselende flags geactiveerd zijn. Dit symboliseert het oplichten van een kerstboom, vandaar de naam. Een xmas scan scant voor open poorten op een netwerk. Dit doet de scan door specifieke pakketjes naar de poorten te sturen. Als het poortje dan open staat, zal er geen reactie gestuurd worden, maar wanneer de poort gesloten is, wordt er een RST-pakket teruggestuurd. Geen reactie betekent dus een open poort.

*Version Detection scans*

Met dit type scans kan gezocht worden naar wat voor Operating System(OS) gebruikt wordt op de server. Ook kan er gezocht worden naar de versie en nog een hoop andere nuttige informatie.

Op basis van deze scans is mogelijk te achterhalen op wat voor OS C-fence draait. Bovendien kunnen we eventueel achterhalen welke versie gebruikt wordt. Met deze informatie kunnen hackers natuurlijk al een hoop, dus hoort het niet zo eenvoudig te achterhalen te zijn. Of Cubics hiertegen bestand is, zal uit de testen blijken.

### Hoe reageert C-fence op netwerk scans?

### Hoe kunnen buitenstaanders verbinding maken met C-fence?

### Wat kan er fout gaan vanaf de forward node van een klant?

# Aanpak en Planning

## Aanpak

Tijdens de duur van het project werken we volgens de Scrum-Methode. Hierbij werken we in sprints van drie weken. Aan het eind van iedere sprint wordt geëvalueerd hoe de sprint verlopen is, en wordt een nieuwe planning gemaakt voor de volgende sprint. Ook begint iedere werkdag met een stand-up. Tijdens de stand-up bespreken we de voortgang van het project, wat er die dag gedaan moet worden, en bespreken we eventuele problemen.

### **Test aanpak**

Voordat de testen beginnen, zal er onderzoek gedaan worden naar methodes en tools waarmee netwerken in kaart gebracht kunnen worden. Op basis van dit onderzoek worden verschillende methodes uitgekozen, en uitgevoerd. De eerste netwerk scans die vervolgens uitgevoerd gaan worden, zijn het type scans die het minste aandacht trekken. Zo wordt opgebouwd naar steeds zwaardere en luidruchtigere scans waarmee meer en meer aandacht getrokken wordt. Op deze manier wordt niet alleen getest op kwetsbaarheden, maar ook hoe goed de IDS/IPS systemen van Cubics functioneren. De resultaten worden verwerkt in een verslag, en op basis hiervan wordt een advies gegeven.

## Onderzoeksmethoden

*<< Beschrijf (per onderzoeksvraag en voor het hele project) welke methoden (zie ictresearchmethods.nl of cmdmethods.nl) je gaat gebruiken om antwoord te krijgen op de belangrijkste vragen binnen je project (= hoe je de belangrijkste keuzes gaat onderbouwen). Noem niet alleen de methode, maar licht ook kort toe hoe je die dan gaat gebruiken (bv. wie je gaat interviewen en met welk doel?). Uiteraard kan je aanpak kan nog aangepast worden gedurende je stage.>>*

*Tip: bedenk ook welk “model” (bv Cyber Kill Chain) je gaat gebruiken.*

## Tijdplan

|  |  |  |
| --- | --- | --- |
| **Sprint** | **Start** | **Taken** |
| 0 | 3/10/2022 | Eerste bezoek cubics + opstellen projectplan |
|  | | 2/11/2022 | Pentesten + Pentest rapport |
|  | 23/11/2022 | Presentatie |

# Projectorganisatie

## Teamleden

|  |  |  |  |
| --- | --- | --- | --- |
| *Organisatie* | *Naam* | *Functie* | *Contactgegevens* |
| Cubics IT | Jean‑Paul Sablerolle | Contactpersoon | jp.sablerolle@cubics.nl |
| Fontys | Rudy Bouland | Semsetercoach | [r.bouland@fontys.nl](mailto:r.bouland@fontys.nl) |
| Fontys | Luc van den Acker | Projectleider | [l.vandenacker@student.fontys.nl](mailto:l.vandenacker@student.fontys.nl) |
| Fontys | Hidde van Brouwershaven | Contactpersoon | [377781@student.fontys.nl](mailto:377781@student.fontys.nl) |
| Fontys | Raoul Goorden | Scrum master | [r.goorden@student.fontys.nl](mailto:r.goorden@student.fontys.nl) |
| Fontys | Stan Akkermans | Notulist | [454067@student.fontys.nl](mailto:454067@student.fontys.nl) |

## Communicatie

Er zijn een aantal afspraken gemaakt over de communicatie binnen de groep. Deze afspraken zijn bindend. Als deze afspraken niet nageleefd worden, zal er overleg plaatsvinden met de docentbegeleider en, indien nodig, met de stakeholder. De afspraken zijn als volgt:

* Op de ingeroosterde dagen dient iedereen uiterlijk om 9:30 aanwezig te zijn. Indien dit niet mogelijk blijkt voor een teamlid, dient dit voor 9:30 gecommuniceerd te zijn met de rest van het team.
* Wanneer taken niet afgerond zijn op het moment dat de vooraf vastgestelde deadline verstreken is, zal overleg plaatsvinden met de docentbegeleider over de nodige vervolgstappen.