Hidde van Brouwershaven    
Luc van den Acker    
Stan Akkermans

Fontys  FHICT Cyber S4

PenTest Rapport Cubics IT

**Document eigenschappen**

|  |  |
| --- | --- |
| Titel | Pentest Rapport Cubics IT |
| Versie | V3.0 |
| Auteurs | Hidde van Brouwershaven   Luc van den Acker   Stan Akkermans |
| Pen-testers | Hidde van Brouwershaven   Luc van den Acker   Stan Akkermans |
| Opdrachtgever | Cubics IT |
| Classificatie | Vertrouwelijk |

Versie beheer

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Auteur(s)** | **Wijzigingen** |
| 1 | 09/11/2022 | Stan Akkermans | Eerste aanmaak, globale opzet gemaakt |
| 2 | 22/11/2022 | Luc van den Acker, Stan Akkermans, Hidde van Brouwershaven | Invulling van hoofdstukken 2 en 3 |
| 3 | 29/11/2022 | Luc van den Acker  Stan Akkermans | Afronding rapport, invulling hoofdstuk 1 en illustratielijst |

Inhoud

[Illustratielijst 3](#_Toc237834468)

[1. Samenvatting 4](#_Toc642209944)

[1.1 Scope 5](#_Toc518153718)

[1.2 Doel van het project 5](#_Toc1905481800)

[1.3Aanname 5](#_Toc689027938)

[1.4 Tijdlijn 5](#_Toc1323750929)

[1.5 Samenvatting vondsten 5](#_Toc2038740895)

[1.6 Samenvatting aanbeveling 6](#_Toc685105851)

[2. Onderzoeksmethode 6](#_Toc1891218379)

[2.1 Planning 7](#_Toc183381879)

[2.2Exploitatie 8](#_Toc1286987258)

[2.3Rapportering 8](#_Toc1536563238)

[3. Gedetailleerde bevindingen 9](#_Toc1474468846)

[3.1Systeem informatie 10](#_Toc1098006865)

[3.2Forward node 178.248.157.78 10](#_Toc1374818101)

# Illustratielijst

Lijst van tabellen

* Tabel 1 Pentest tijdlijn
* Tabel 2 Risicobeoordeling
* Tabel 3 Risicotabel
* Tabel 4 Open poorten doelwit

Lijst van afbeeldingen

* Afbeelding 1 Het cyberkill chain model
* Afbeelding 2 Resultaten versiescan

# 1. Samenvatting

Dit document beschrijft de bevindingen van de penetratie test op een forward node van Cubics. Het doel van de penetratie test was om eventuele kwetsbaarheden te vinden en deze te rapporteren.

## 1.1 Scope

Het project bevat een op afstand penetratie test van het IP-adres 178.248.157.78. Hierbij is de pentest uitgevoerd vanuit een "black box" perspectief, waar de enige verstrekte informatie het IP-adres van het doelwit is.

## 1.2 Doel van het project

De penetratie test is uitgevoerd om zwakheden in de security oplossing C-fence van Cubics IT te vinden. De hoofdvraag was om te kijken of er iets te vinden was over de verbinding tussen een forward node van een klant en de SIEM van Cubics. Omdat het IP-adres behoort tot een live klant omgeving is er geen exploitatie uitgevoerd op de eventuele bevonden zwakheden.

## 1.3 Aanname

Tijdens het opstellen van dit rapport hebben we de aanname dat het IP-adres publiekelijk is, de NDA is ondertekend en dat C-fence een security oplossing is die op de machine van het IP-adres draait.

## 1.4 Tijdlijn

De tijdlijn van het pentesten is als volgt:

|  |  |  |
| --- | --- | --- |
| Penetratie Test | Start datum/tijd | Eind datum/tijd |
| Shodan | 16/11/2022 10:22 | 16/11/2022 10:22 |
| Ping scan | 16/11/2022 10:24 | 16/11/2022 10:24 |
| Null scan | 16/11/2022 10:26 | 16/11/2022 10:26 |
| Stealth scan | 16/11/2022 10:28 | 16/11/2022 10:28 |
| Operating scan | 16/11/2022 10:44 | 16/11/2022 10:44 |
| Versie scan | 16/11/2022 11:57 | 16/11/2022 11:57 |
| All port scan | 16/11/2022 12:38 | 16/11/2022 12:42 |

Tabel 1: Pentest tijdlijn

## 1.5 Samenvatting vondsten

De security oplossing C-fence van Cubics IT lijkt een veilige service. Wij hebben wat informatie van het geteste IP-adres gewonnen zoals de service die er draait, het Operating System en de versie en om wat voor apparaat het gaat. De enige poort die open staat op de host is poort 161, deze wordt gebruikt voor het versturen van SNMP querries. Deze querries bevatten informatie van het netwerk en worden naar Cubics gestuurd. Een mogelijk risico hierbij zou een MitM aanval zijn waarbij een aanvaller tussen de verbinding gaat zitten en het verkeer kan aantasten, dit is echter een laag risico omdat de aanvaller hiervoor zou moeten weten naar welk IP-adres deze pakketjes gestuurd worden. Een ander risico zijn DoS en DDoS aanvallen waarbij een aanvaller grote aantallen pakketjes aan netwerkverkeer naar de poort stuurt en de service vast laat lopen. Beide risico hebben wij niet kunnen testen waardoor we geen accurate waarde kunnen geven. Een DDoS aanval zou moeilijker moeten zijn dan een DoS aanval aangezien een DDoS meerdere complexe stappen heeft dan een standaard DoS aanval en heeft een grotere impact dan een DoS aanval.

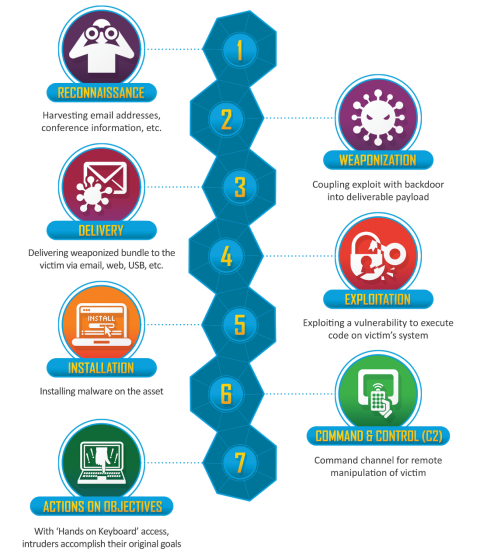
|  |  |
| --- | --- |
| Waarde | Aantal risico's |
| Laag | 2 |
| Gemiddeld | 1 |
| Hoog | 0 |
| Zeer hoog | 0 |

Tabel 2: Risicobeoordeling

## 1.6 Samenvatting aanbeveling

Onze aanbeveling is om de huidige service te blijven gebruiken. Ondanks onze bevindingen lijken de risico's onwaarschijnlijk met weinig impact.

# 2. Onderzoeksmethode

Tijdens de pentest is gewerkt volgens het “cyber kill chain” model. In figuur 1 wordt weergegeven hoe dit model eruit ziet. Hieronder is per stap te lezen wat het verrichte werk is. Niet iedere stap is volledig uitgevoerd. Zo is bijvoorbeeld de stap “exploitation” niet uitgevoerd, omdat schade aanrichten aan C-fence niet het doel van het project is.

Figuur 1

Afbeelding 1: De cyberkill chain

Reconnaissance.

De eerste stap is natuurlijk het verzamelen van informatie over het doelwit. Hiervoor is de website van Cubics afgespeurd voor nuttige informatie, maar ook social media platforms als LinkedIn zijn bestudeerd om informatie over de medewerkers te achterhalen. De belangrijkste bron van informatie over C-fence is Cubics zelf geweest. Cubics heeft informatie aangeboden over de werking van C-fence, en een IP-adres waarop een onderdeel gehost wordt.

Weaponization.

Nadat de benodigde informatie verzameld is, volgt het gebruiken van deze informatie. Om vanaf deze informatie tot een potentiële hack te komen, is gekeken waar mogelijk kwetsbaarheden liggen. Vervolgens is een plan opgezet om deze kwetsbaarheden bloot te leggen, en zijn de tools klaargezet die hiervoor nodig zijn.

Delivery, exploitation, installation en command&control.

Tijdens deze fase worden de “wapens” uit de vorige fase afgeleverd bij het doelwit, en de kwetsbaarheden vervolgens uitgebuit. Aangezien deze wapens vrij veel schade aan kunnen richten aan de oplossing van Cubics, worden deze stappen niet uitgevoerd. Wel is beschreven wat deze wapens zijn, en hoe ze onschadelijk gemaakt kunnen worden. Waarom deze keuzes gemaakt zijn, is later in dit verslag terug te vinden.

## 

## 2.1 Planning

Tijdens het plannen is informatie verzameld over het doelwit. De volgende onderwerpen stonden hierin centraal:

* De werking van C-fence.
* De technische infrastructuur van Cubics.
* IP-adressen waarop C-fence draait.
* Algemene informatie over Cubics als bedrijf.

Vervolgens probeerde we deze informatie te gebruiken om kwetsbaarheden te vinden in C-fence. Deze kwetsbaarheden hebben we niet geëxploiteerd omdat C-fence een live omgeving is waarvan de klanten van Cubics afhankelijk zijn om de veiligheid van hun digitale infrastructuur te waarborgen. Het is niet verantwoord om stappen te zetten die potentieel de functionaliteit van C-fence op het spel zetten.

## 2.2 Exploitatie

Door de gevonden informatie in Planning konden we beginnen met kwetsbaarheden vinden en waar mogelijk deze exploiteren. Hieronder vindt U een overzicht van de gevonden kwetsbaarheden.

Uit testcase 01 blijkt dat poort 161 op IP-adres 178.248.157.78 open staat, en gebruik maakt van SNMP. Vervolgens is gekeken of er een bekende CVE(Common Vulnerabilty and Exposures) is voor SNMP. [CVE-2002-0013](https://www.cvedetails.com/cve/CVE-2002-0013/?q=CVE-2002-0013) gaat over een kwetsbaarheid waarbij Denial of Service toegepast kan worden om privileges te krijgen over de host. De bijbehorende CVSS(Common Vulnerability Scoring System) score van deze vulnerability is 10.0. Een score van 10.0 is de hoogst mogelijke score, wat natuurlijk betekent dat van een groot risico te spreken is. Aangezien een DoS-aanval voor serieuze problemen kan zorgen, wordt deze kwetsbaarheid niet uitgebuit.

Testcase 05 gaat over het uitvoeren van een netwerkscan waarbij geprobeerd wordt om de OS van de host te achterhalen. Hieruit blijkt dat de OS van de host zeer waarschijnlijk NX-OS 6 gebruikt, een operating system van Cisco. Aangezien SNMP vooral gebruikt wordt door switches, routers en modems, sluit deze informatie goed aan op de resultaten van TC01. [CVE-2015-0718](https://www.cvedetails.com/cve-details.php?t=1&cve_id=cve-2015-0718) gaat wederom over een DoS-aanval, maar deze keer gericht op de NX-OS versies 4.0 tot 6.1, waar de OS van de geteste host dus ook onder valt.

## 2.3 Rapportering

Na de eerste twee stappen kunnen we de resultaten gaan analyseren. Onze risk rating wordt berekend met de formule:

Risico = dreiging \* kwetsbaarheid \* impact

In de onderstaande tabel wordt de risk rating nogmaal weergegeven. Hierin is visueel weergegeven hoe risico’s ingeschat worden. Hierbij staat groen voor een kleine dreiging met een lage impact, en rood voor een grote dreiging met een grote impact.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **RISICOTABEL** |  |  |  |  |  |
| **1. Bedreigingen** | **2. impact beschrijving** | **3. Impact niveau (1-5)** | **4. Kans (1-3)** | **5. Risiconiveau** | **6. Conclusie** |
| DDoS | Downtime van het systeem kan leiden tot financiële schade, reputatieschade, schade voor een klant en kosten voor incident handling | 5 | 1 | 5 | **Configureer de juiste firewall rules, creeër een verdedigings strategie, train een team en bespreek rollen, houdt software up-to-date, Vergroot de bandbreedte zodat de server voorbereid is om verkeerspieken op te vangen** |
| DoS | Downtime van het systeem kan leiden tot financiële schade, reputatieschade, schade voor een klant en kosten voor incident handling | 5 | 2 | 10 | **Update naar SNMPv3 indien dit nog niet is gedaan, configureer de juiste firewall rules.** |
| MitM | Reputatieschade door gebrek aan integriteit van verkeer | 3 | 1 | 3 | **Gebruik versleuteld verkeer door encryptie te gebruiken, maak gebruik van IPS om een MitM aanval te detecteren/blokkeren** |

Tabel 3: Risicotabel met de bevonden risico's

# 3. Gedetailleerde bevindingen

## 3.1 Systeem informatie

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **IP Adres** | **Systeem Type** | **OS Informatie** | **Open Ports**   |  |  |  | | --- | --- | --- | | **Port#** | **Protocol** | **Service name** | | | |
| 178.248.157.78 | Switch | Cisco Nexus  NX-OS 6.X | 161 | TCP | SNMPv3 |

Tabel 4: Open poorten doelwit

## 3.2 Forward node 178.248.157.78

**De service (SNMPv3 Server) is actief:**

**Risico Niveau**

Laag

**Kwetsbaarheid**

Laag

**Analyse:**

SNMP is een protocol dat gebruikt wordt voor het verzamelen en wijzigen van gegevens van een aantal apparaten in een netwerk. SNMP wordt voornamelijk gebruikt door switches, routers, workstations en modems. Dit verkeer zou onderschept kunnen worden met een MitM aanval of de service zou kunnen worden gestopt door een Denial of Service (dos) aanval.

Text

Description automatically generatedAfbeelding 2: Resulaten van de versie scan laten zien welke versie de SNMP server gebruikt.

**Impact:**

Laag

**Risicoclassificatie**

Laag

**Aanbeveling**

Op het moment van de pentest hebben we nog geen kwetsbaarheden geconstateerd onze aanbeveling is dan ook om de service te houden.