THOMAS MORE

Stage Orange Cyberdefense Red Team Environment

Bryan Poleunis
Student Bachelor in de Elektronica-ICT – Cloud & Cyber Security

2024 - 2025

Inhoudsopgave

1. Inleiding

In dit realisatiedocument wordt de realisatie van een red team operatie infrastructuur uitgebreid beschreven. Red team operaties spelen een cruciale rol in de hedendaagse cybersecurity door potentiële kwetsbaarheden in IT-omgevingen te identificeren. Dit gebeurt door middel van het simuleren van realistische cyberaanvallen.

Dit document omvat niet alleen een analyse van de gebruikte tools en technologieën, maar ook een gedetailleerde beschrijving van de implementatie van de infrastructuur. Bovendien worden de overwegingen achter de gemaakte keuzes toegelicht, alsook de uiteindelijke conclusies en geleerde lessen. Het voornaamste doel is om een efficiënte, betrouwbare en schaalbare oplossing te bieden voor het effectief uitvoeren van red team operaties, waardoor organisaties beter beschermd kunnen worden tegen daadwerkelijke dreigingen.

Mijn stageproject, **Red Team Infrastructure**, betreft het ontwerpen en realiseren van een **geautomatiseerde, modulaire en reproduceerbare red team-omgeving**. Deze omgeving wordt volledig uitgerold in de **Hetzner Cloud** met behulp van **Infrastructure as Code (IaC)** via **OpenTofu**, een open-source alternatief voor Terraform. Het project biedt het Red Team van Orange Cyberdefense de mogelijkheid om per klant snel en veilig een volledig gescheiden testomgeving op te zetten. Dit verhoogt de efficiëntie en minimaliseert het risico op het hergebruiken van gevoelige gegevens of configuraties tussen klanten.

Het doel van dit project is het ontwikkelen van een schaalbaar platform dat:

- Veilig en geïsoleerd is per klant.
- Volledig automatisch uitgerold kan worden.
- Eenvoudig te beheren en op te ruimen is na gebruik.

2. Stagebedrijf

Mijn stage vond plaats bij **Orange Cyberdefense Belgium**, een onderdeel van de internationale Orange-groep die zich richt op cybersecurityoplossingen. Orange Cyberdefense levert onder andere diensten zoals pentesting, red teaming, threat hunting, SOC-monitoring en security consulting.
Gedurende mijn stage werkte ik binnen het **Red Team**, een gespecialiseerd team dat zich bezighoudt met het simuleren van realistische aanvallen om de weerbaarheid van klanten te testen. Het team voert onder andere **red team engagements**, **phishingcampagnes** en **social engineering**-scenario's uit, steeds met de focus op realistische dreigingen en het omzeilen van traditionele beveiligingslagen.

3. Analyse

In dit hoofdstuk analyseren we de verschillende componenten en keuzes voor het opzetten van het Red Team cloudplatform. We onderzoeken beschikbare tools, hun mogelijkheden en beperkingen, en onderbouwen zo onze uiteindelijke keuzes voor het platformontwerp.

3.1. Phishing

Phishing is een belangrijk onderdeel van red team-operaties. We onderzochten verschillende tools voor phishingcampagnes:

Geselecteerde tools:

- **GoPhish** + **Evilginx**: combinatie voor tracking, credential harvesting en realistische phishingflows.
- **Alternatieven:** Social Engineering Toolkit, King Phisher, Phishious, phishing-frenzy, Metasploit Pro, Zphisher, HiddenEye, Modlishka, PwnAuth, o365-attack-toolkit.
-

Beoordelingscriteria:

- E-mail delivery & spoofing support
- Tracking en credential harvesting
- Customizability & uitbreidbaarheid (o.a. spearpishing)
- Integratie met andere tools

3.2. C2 server

Voor het beheren van implantaten en command execution onderzochten we meerdere C2-frameworks.
Geselecteerde tool:

- **Mythic C2**: Beste score op gebruiksgemak, stealth, flexibiliteit en integraties.

Onderzochte tools:

- ninjaC2
- phosC2
- covenant
- cobaltstrike
- Caldera
- metasploit
- prismatica
- infection monkey
- Mythic
- Merlin (also standalone)
- Sliver (enkel windows)

Kriteria:

- Ease of use (gui-cli)
- Kost
- Stealth/evasion techniques
- Flexiblility
- Tool integration

WRM op volgende pagina

	ninjaC2	phosC2	Covenant	caldera	Metasploit	Prismatica	Infection monkey	Mythic C2	Merlin	sliver
Ease of use	3	3	3	2	3	3	2	5	4	5
Kost	5	5	5	5	5	5	5	5	3	2
Stealth/evasion techniques	3	3	3	3	3	3	2	5	2	3
flexibility	3	3	3	3	3	3	2	5	3	1

3.3. Attack Server

De aanvalsmachine moest veel tools bevatten, makkelijk te gebruiken zijn en goed integreerbaar in cloudomgevingen.
Geselecteerde tool:

- **Exegol**

Onderzochte tools:

- Kali
- Blackarch
- Exegol
- Parrot

Hieronder zie je de WRM analyze

	Kali	Exegol	Blackarch	ParrotOS
Aantal tools	4	3	5	4
Gebruiksgemak	4	5	3	4
Cloud compatability	3	5	2	2
Extra tools	4	4	4	4
logging	3	5	2	3

3.4. Cloud

Geselecteerde Provider:

- Hetzner

Onderzochte Providers:

- AWS
- Azure
- Hetzner
- Google cloud

Kriteria:

- prijs
- Availability
- Respons time
- Plaats
- Automatisering

	AWS	Azure	Hetzner	Google Cloud
prijs	4	4	2	4
Availability	5	5	4	5
Respons time	3	3	4	3
Plaats	5	5	5	5
Automatisering	5	5	3	5

3.5. Cloud deployment

We vergeleken verschillende **cloud provisioning tools en kozen er voor een combinatie van deze te gebruiken:**

- **Opentofu**
- **Ansible**
- **Cloud-Init**

Onderzochte Tools:

- Terraform
- opentofu
- Cheff
- Ansible
- Jenkins
- Salt
- Cloud-init

Kriteria:

- Ease of use
- Kost
- Samenwerking met andere tools
- Documentatie

	Terraform	OpenTofu	Cheff	Jenkins	Salt	Cloud Init	Ansible
Ease of use	4	4	2	3	2	4	4
Kost	5	0	4	0	0	0	0
Samenwerking met andere tools	4	4	4	3	4	4	4
Documentatie	4	4	3	4	2	3	4

3.6. Proxy

We vergeleken verschillende reverse proxy-oplossingen voor beheer en automatisatie.
Geselecteerde tool:

- **Nginx**: eenvoudig te gebruiken en goed te integreren met scripts.

Onderzochte tools:

- Nginxproxy manager
- Caddy
- Traefik proxy
- Haproxy
- Nginx x

- Ease of use
- Payed/opensource
- automatable?
- Setup

	Nginx Proxy Manager	Caddy	Traefik	haproxy	Nginx	Apache
Ease of use	4	5	3	2	3	3
Payed/opensource	0	2	2	3	3	0
automatable?	1	4	4	3	3	3
Setup	4	4	3	4	2	3

3.7. VPN

Voor veilige toegang van buitenaf was een VPN-oplossing vereist.
Geselecteerde tool:

- **OpenVPN**: eenvoudig zelf te hosten, brede ondersteuning, goed integreerbaar.

Onderzochte tools:

- Openvpn
- Wireguard
- Tailscale

Kriteria:

- Ease of use
- Payed/opensource
- Selfhosted
- Password/mfa

Ease of use	OpenVPN	Wireguard	Tailscale
Ease of use	3	3	4
Price	2	0	3
Selfhosted	5	5	1
Password/mfa	3	4	3

3.8. Logging

Voor logverzameling en visualisatie onderzochten we verschillende logging stacks.
Geselecteerde tool:

- **Grafana** in combinatie met **Alloy-agent**

Onderzochte tools:

- Grafana
- Elk Stack
- Splunk

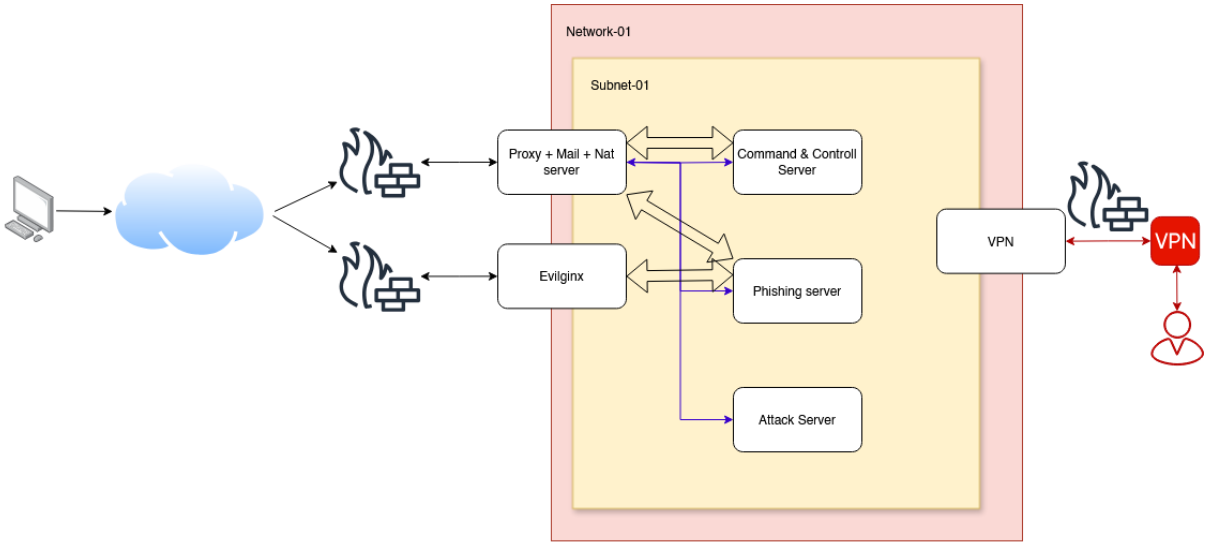
	Grafana	Splunk	ELK Stack
Ease of use	5	4	3
Payed/opensource	5	1	3
automatable?	4	4	5
Setup	5	5	5

4. Realisatie

In dit hoofdstuk beschrijf ik hoe de red team infrastructuur stap voor stap werd opgebouwd op basis van de gekozen technologieën uit de analysefase. De nadruk ligt op de concrete uitwerking van het platform: hoe de omgeving werd geautomatiseerd met tools zoals OpenTofu en Ansible, welke componenten zijn ingezet (zoals de VPN, phishingtools, C2-server en attack server), en hoe logging en monitoring zijn geïntegreerd. Elk onderdeel wordt toegelicht met de bijbehorende configuratie en motivatie, zodat duidelijk is hoe de uiteindelijke infrastructuur tot stand kwam.

4.1 Schematische weergave

Onderstaande afbeelding toont een overzicht van de opbouw van de red team infrastructuur, inclusief de verschillende componenten die met elkaar samenwerken via geautomatiseerde processen. De uitrol en het beheer van de infrastructuur gebeurt volledig geautomatiseerd met behulp van OpenTofu en Ansible.



Legende
Internet Access
Communications

	Network	range
Network-01	10.66.X.0	/24
Subnet-01	10.69.X.0	/24

Ip-Table		
Proxy + mail	10.66.X.2	/24
Command & Controll server	10.66.X.3	/24
Phishing Server	10.66.X.4	/24
Attack Server	10.66.X.5	/24
VPN	10.66.X.6	/24
Evilginx	10.66.X.7	/24

4.2 Setup

4.2.1 Python Wrapper

Er is een Python wrapper ontwikkeld om de interactie met verschillende tools en API's te vereenvoudigen. Deze wrapper automatiseert taken zoals het ophalen van statusinformatie, het monitoren van actieve omgevingen, en het opstarten van processen. Dankzij de wrapper is er een centrale interface waarmee beheerders snel overzicht en controle hebben.

4.2.2 OpenTofu

OpenTofu wordt gebruikt voor het opzetten en beheren van de cloudinfrastructuur. Het stelt ons in staat om infrastructuur als code te definiëren, waardoor we snel en herhaaldelijk omgevingen kunnen creëren en aanpassen. Dit zorgt voor een consistente en geautomatiseerde manier van het beheren van de infrastructuur. We gebruiken OpenTofu omdat het een open-source alternatief is voor Terraform, en het ons de flexibiliteit biedt om de infrastructuur naar onze specifieke behoeften aan te passen.

4.2.3 Cloud init

Cloud init wordt gebruikt voor de initiële configuratie van virtuele machines in de cloud. Het zorgt ervoor dat de instances bij het opstarten automatisch worden geconfigureerd met de juiste instellingen, zoals het installeren van software, het configureren van netwerkinterfaces, en het toevoegen van gebruikers. Door Cloud init te gebruiken, kunnen we snel en consistent omgevingen opzetten zonder handmatige tussenkomst, wat de efficiëntie en betrouwbaarheid van de implementatie verhoogt.

4.2.4 Ansible

Ansible wordt gebruikt voor de automatisering van systeemconfiguratie en applicatie-implementatie. Het stelt ons in staat om taken op meerdere servers tegelijkertijd uit te voeren, waardoor handmatige configuratie overbodig wordt. We gebruiken Ansible om consistente configuraties te garanderen, updates uit te rollen, en de algehele systeemstatus te beheren. Dit zorgt voor een efficiëntere en betrouwbaardere infrastructuur.

4.3 Technische Componenten

4.3.1 VPN - OpenVPN

Voor veilige communicatie tussen de verschillende componenten van de infrastructuur is OpenVPN geïmplementeerd. OpenVPN biedt flexibele configuratiemogelijkheden en ondersteunt een brede waaier aan platformen, inclusief legacy-ondersteuning. Dit maakt het een betrouwbare keuze in complexe netwerkomgevingen.

4.3.2 Command & Control - Mythic C2

Na een grondige analyse van meerdere C2-frameworks is Mythic C2 gekozen. Mythic combineert flexibiliteit, uitbreidbaarheid en stealth-capaciteiten met een gebruiksvriendelijke interface. Dankzij de modulaire opbouw kunnen verschillende payloads en communicatiekanalen worden beheerd via één gecentraliseerd systeem.

4.3.3 Phishing Framework - Gophish + Evilginx

Voor de uitvoering van phishing-simulaties is gekozen voor een combinatie van Gophish en Evilginx. Gophish verzorgt de e-mailcampagnes en tracking, terwijl Evilginx wordt gebruikt voor het omzeilen van MFA via reverse proxy techniek. Deze combinatie biedt zowel schaalbaarheid als diepgang in simulaties.

4.3.4 Attack Server - Exegol

Exegol is geselecteerd als dedicated attack server dankzij zijn uitgebreide toolset en loggingcapaciteiten. Het platform is geoptimaliseerd voor offensieve operaties en integreert gemakkelijk met andere onderdelen van de infrastructuur. De standaardconfiguratie biedt een volledig werkende omgeving bij de eerste opstart.

4.3.5 Logging en Monitoring - Grafana, Loki, Alloy

Voor centrale logging is gekozen voor de combinatie van Grafana (visualisatie), Loki (log aggregatie) en Alloy (data collectie en forwarding). Deze tools geven real-time inzicht in systeem- en applicatielogs. Dit verhoogt de detectiemogelijkheden en maakt auditing achteraf eenvoudiger.

4.4 Besluit

In dit realisatiedocument is de opzet en realisatie van een red team operatie infrastructuur beschreven, waarbij na grondige analyse bewuste keuzes zijn gemaakt voor Python scripting voor automatisering, OpenTofu voor infrastructuurbeheer, Ansible voor configuratiebeheer, OpenVPN voor veilige communicatie, Mythic C2 voor command en control, Gophish en Evilginx voor phishing-simulaties, Exegol als dedicated attack server, en Grafana, Loki en Alloy voor logging en monitoring. Deze gekozen oplossingen vormen samen een robuust platform dat realistische cyberaanvallen simuleert, kwetsbaarheden identificeert, efficiëntie verhoogt, inzicht biedt door uitgebreide logging en monitoring, en uiteindelijk de cybersecurity van de organisatie verbetert, waardoor de gerealiseerde infrastructuur voldoet aan de gestelde eisen en een waardevolle bijdrage levert aan het verbeteren van de beveiligingsmaatregelen.

5. Literatuurlijst

https://opentofu.org/
https://developer.hashicorp.com/terraform
https://docs.ansible.com/
https://mythic-c2.netlify.app/
https://gophish.io/
https://github.com/kgretzky/evilginx2
https://github.com/SEKOIA-IO/Exegol
https://grafana.com/
https://grafana.com/oss/loki/
https://grafana.com/oss/alloy/
https://openvpn.net/
https://Kali.org
https://Exegol.readthedocs.io
https://Blackarch.org
https://Parrotsec.org
https://developer.hashicorp.com/terraform
https://opentofu.org/
https://www.chef.io/
https://www.redhat.com/en/ansible-collaborative
https://saltproject.io/
https://cloudinit.readthedocs.io/en/latest/
https://traefik.io/traefik/
https://www.haproxy.org/
https://nginx.org/
https://nginxproxymanager.com/
https://httpd.apache.org/
https://caddyserver.com/
https://openvpn.net/
https://tailscale.com/
https://www.wireguard.com/