

Projectplan

Bryan Poleunis

Thomas Deboel



Orange
Cyberdefense

THOMAS
MORE

Inhoud



- Wat doet Orange cyberdefense
- Doel project
- Plan
- Onderzoek
- Oplevering
- Stand van zaken



Orange
Cyberdefense

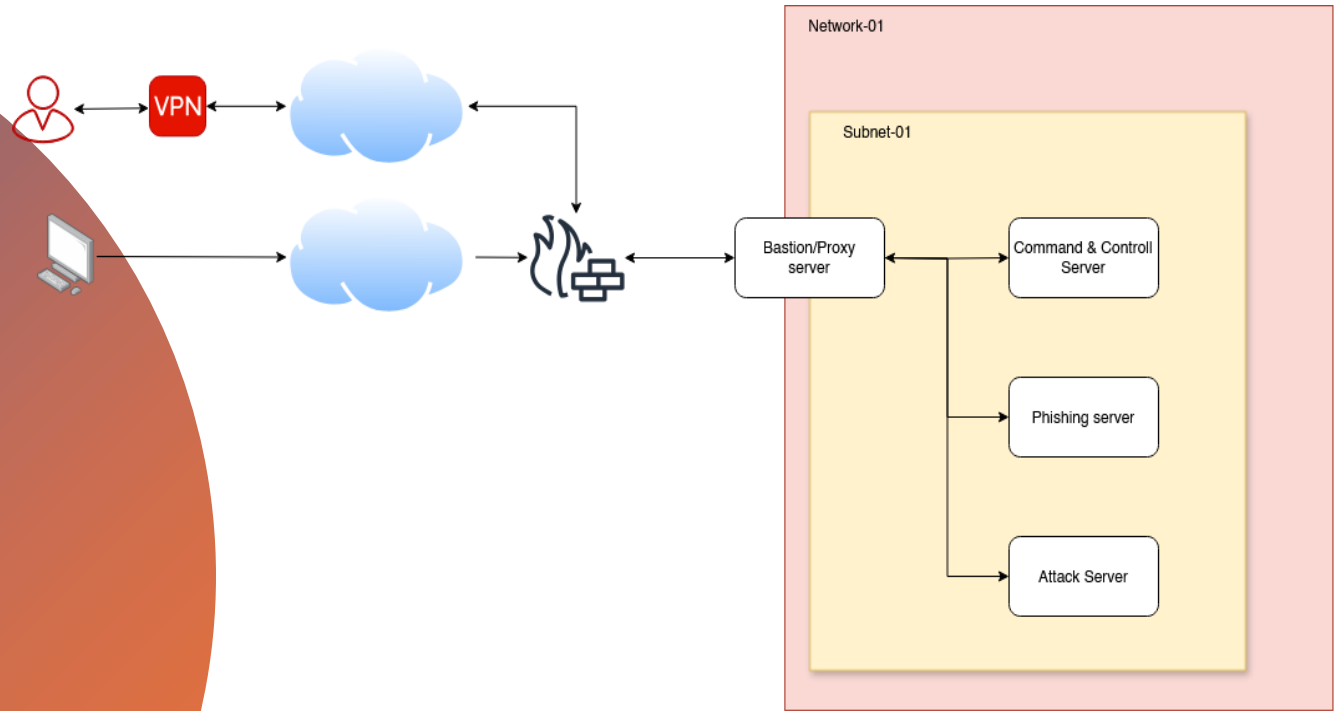


Orange Cyberdefense

- Wat is Orange Cyberdefense
 - Onderdeel van Orange Group
 - Gespecialiseerd in cybersecurity
- Dienst en oplossingen:
 - Beveiliging van netwerken
 - Incident respons
 - Risicoanalyse
 - Compliance check
 - Penetration testen

Doel project

- Red team environment
 - Veiligheid en isolatie
 - Herbruikbare infrastructuur
 - Bruikbaar in echte wereld
 - configureerbaar



	Network	range
Network-01	10.0.0.0	/16
Subnet-01	10.0.0.0	/16

Ip-Table		
Bastion/proxy	10.0.0.2	/16
Command & Control server	10.0.0.3	/16
Phishing Server	10.0.0.4	/16
Attack Server	10.0.0.5	/24



Plan



Orange
Cyberdefense

Onderzoek individuele componenten



Functionaliteit

Ease of use

Automatie mogelijkheden

openSource

VPN



Orange
Cyberdefense

Cloud



Wat moet er in de Cloud

Hoe moet de Cloud functioneren

Wat kan de Cloud

Hoeveel resources moet je hebben

- Storage?
- Ram?
- CPU?
- GPU?

Welke servers moet je hebben voor welke prijs



Automatizing Cloud



Iac: OpenTofu

Proxy : Nginx

VPN: Tailscale

C2: Mythic C2

Phishing: GoPhish en Evilginx

Attack Server: Exegol



OpenTofu³

tailscale



Orange
Cyberdefense

Oplevering



Github Repository

Handleiding

Documentatie offensive tools

Demo