BTS SIO SISR – Épreuve E6
Guide Firewall + VPN + Honeypot + Port Knocking

Ce document présente la mise en place d'une infrastructure réseau sécurisée dans le cadre de l'épreuve E6 du BTS SIO option SISR. Le projet combine plusieurs mécanismes de sécurité : Firewall Linux, VPN Tailscale, Honeypot, IPTABLES et Port Knocking.

1. Architecture Réseau

Machine	Adresse IP	Rôle
Firewall	192.168.2.1	Routage et sécurité
Serveur Web	192.168.2.2	Serveur réel SSH/Web
Honeypot	192.168.2.4	Piège pour les attaquants

2. Installation SSH

```
apt update
apt install openssh-server -y
```

3. Configuration Réseau Firewall

```
auto lo
iface lo inet loopback

allow-hotplug ens33
iface ens33 inet dhcp

allow-hotplug ens37
iface ens37 inet static
 address 192.168.2.1
 netmask 255.255.255.0
```

4. Installation VPN Tailscale

```
apt install curl -y
curl -fsSL https://tailscale.com/install.sh | sh
tailscale up
tailscale ip -4
```

5. Subnet Routing

```
tailscale up --advertise-routes=192.168.2.0/24
```

6. Configuration Serveur Web

```
iface ens33 inet static
 address 192.168.2.2
 netmask 255.255.255.0
 gateway 192.168.2.1
```

7. Configuration Honeypot

```
iface ens33 inet static
 address 192.168.2.4
 netmask 255.255.255.0
 gateway 192.168.2.1
```

8. Installation Port Knocking

```
apt install knockd iptables-persistent -y
```

9. Configuration Knockd

```
[openSSH]
sequence = 7000,8000,9000
seq_timeout = 10
command = /sbin/iptables -t nat -I PREROUTING 1 -p tcp --dport 22 -j DNAT --to-destination 192.168.2.2
tcpflags = syn
```

10. IPTABLES

```
iptables -t nat -F PREROUTING
iptables -t nat -A PREROUTING -p tcp --dport 22 -j DNAT --to-destination 192.168.2.4
```

11. Test du Port Knocking

```
knock 192.168.2.1 7000 8000 9000
ssh user@192.168.2.1
```

Résultats Obtenus

Le projet permet :

• De masquer le véritable serveur SSH
• De détecter les attaques grâce au Honeypot
• De sécuriser les accès distants via Tailscale
• D’utiliser IPTABLES pour le filtrage et la redirection réseau
• D’améliorer la sécurité globale de l’infrastructure

Conclusion

Cette solution démontre la mise en œuvre de compétences en administration système et sécurité réseau dans un contexte professionnel. Le projet répond aux attentes techniques de l’épreuve E6 du BTS SIO SISR.