CYSLAB

CGI Business Consulting

Ligolo-ng

EBIOS RM face à Ligolo-ng : anatomie d'un outil de tunneling moderne, décryptée par son concepteur

Nicolas Chatelain

Présentation

Nicolas Chatelain

- Directeur à **CGI Business Consulting**
- **CGI Business Consulting :** 35+ années d'experience dans tous les secteurs ; 4 Laboratoires de sécurité qualifies ; 1500 professionnels de la sécurité
- **CysLab :** Laboratoire qualifié **PASSI** pour la réalisation de tests d'intrusion, audit de code, configuration, architecture & organisationnel
- **Développeur d'outils offensifs** Chashell, Ligolo-ng, Ligolo-IWA

Gestion des risques d'entreprise | **Laboratoire qualifié** | **Managed Security Services** | **Gestion de l'identité numérique** | **Continuité d'activité d'entreprise** | **Gouvernance de la sécurité**

CYSLAB
CGI Business Consulting

Objectif de la session

Comprendre où Ligolo-ng aide — et où il faut le cadrer.

1. Ligolo-ng ?

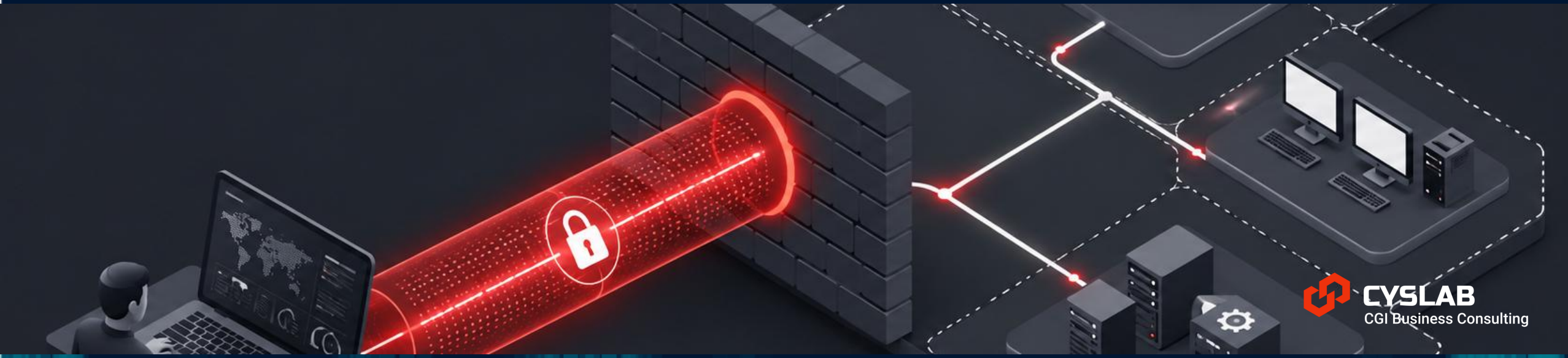
Relier un outil de pivot à l'analyse de scénarios de menace : faisabilité, impacts, mesures.

2. Comment ça marche ?

Architecture proxy/agent, interface TUN, routage L3 et listeners.

3. Moyens de protection

Démonstration contrôlée, règles de sécurité, traces attendues et limites.



CYSLAB
CGI Business Consulting

Qu’est-ce que Ligolo-ng ?

Ligolo-ng est un outil de **post-exploitation** utilisé par les professionnels de la cybersécurité pour effectuer du mouvement latéral (attaquer d’autres ordinateurs d’un même réseau) depuis un poste préalablement compromis.

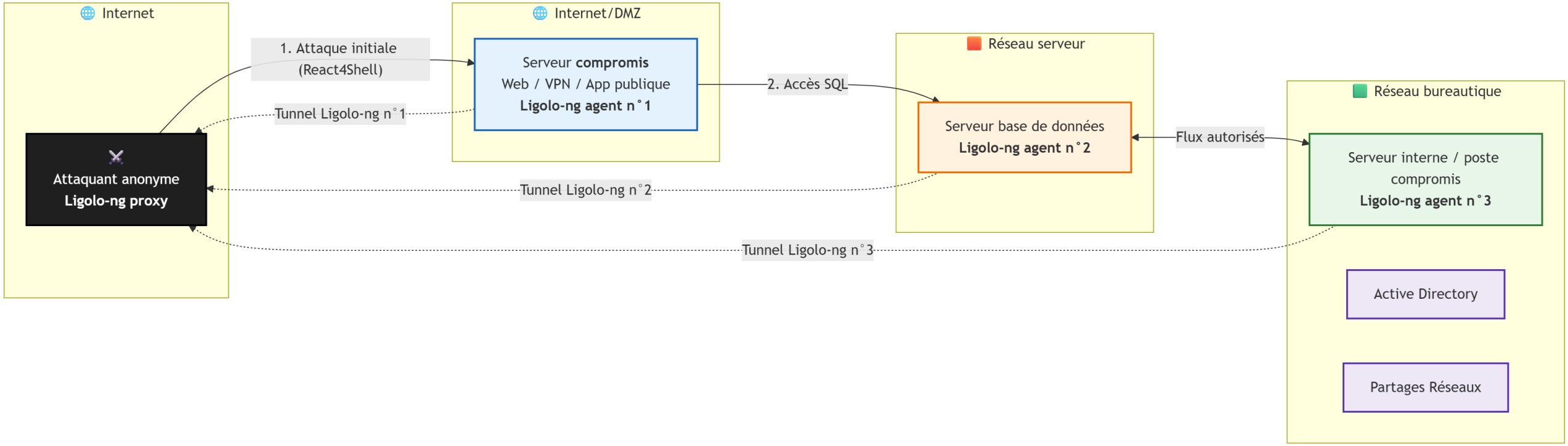
Ses points forts :

- **Il s'installe partout :** Grâce à sa conception moderne, il fonctionne sur presque tous les appareils : ordinateurs (Windows, Linux, Mac), smartphones Android et même certaines télévisions connectées.
- **Zéro prise de tête :** Contrairement aux anciennes méthodes complexes, il crée une sorte de "câble réseau virtuel" direct entre vous et la cible. Plus besoin de configurer des redirections de ports ou des réglages interminables.
- **Ultra-flexible :** Il permet de faire circuler les données dans tous les sens (de chez vous vers la cible, ou de la cible vers chez vous), ce qui est idéal pour contourner les barrières de sécurité et les pare-feux.
- **Open-Source et gratuit : https://github.com/nicocha30/ligolo-ng**

Le « mythe » des protections contre le tunneling

- **Utilisateur non privilégié :** Ligolo-ng fonctionne sans aucune permission administrateur.
- **Proxy filtrant :** Ligolo-ng supporte les communications à travers proxy HTTP (Websocket).
- **EDR :** Ligolo-ng est détectable, mais facilement modifiable afin de le rendre invisible aux EDR.
- **AppLocker :** Ligolo-IWA est un agent alternatif Ligolo-ng fonctionnant directement depuis votre navigateur web, sans installation ou exécution de binaire.
- **Pas d'accès direct à Internet :** Ligolo-ng a démontré sa capacité à traverser des réseaux isolés (DNS tunneling – DEFCON Paris 2025)

Ligolo-ng en 60 secondes



L'attaquant provenant d'Internet et ayant préalablement compromis un serveur utilise Ligolo-ng pour « sauter » de réseau en réseau.

CYSLAB
CGI Business Consulting

Ce que Ligolo-ng change par rapport aux pivots classiques

Critère	Anciennes solutions (SOCKS)	Ligolo-ng
Mode	Proxy applicatif	Routage IP via TUN
Expérience outils	Configuration par outil	Usage quasi natif des outils réseau
Protocoles	Souvent centré TCP	TCP, UDP et ICMP selon capacités/environnement
Complexité	Simple mais parfois fragile	Routage à maîtriser, plus propre en lab

Ligolo-ng, contrairement aux anciennes solutions, permet de cibler des réseaux entiers plutôt que des applications bien spécifiques.

Comparatif avant/après

Ligolo-ng a révolutionné le tunneling réseau en combinant vitesse maximale et simplicité absolue.

```
┌──(kali㉿kali)-[~/Documents/THM/borderland]
└─$ proxychains -q nmap -sV -Pn 172.16.1.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-02 15:53 WIB
Stats: 0:14:39 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 72.70% done; ETC: 16:13 (0:05:26 remaining)
Stats: 0:14:40 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 72.80% done; ETC: 16:13 (0:05:24 remaining)
Nmap scan report for 172.16.1.128
Host is up (1.2s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 2.3.4
179/tcp  open  bgp?
2601/tcp open  quagga  Quagga routing software 1.2.4 (Derivative of GNU Zebra)
2605/tcp open  quagga  Quagga routing software 1.2.4 (Derivative of GNU Zebra)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nm
.
Nmap done: 1 IP address (1 host up) scanned in 1394.11 seconds
```

```
┌──(kali㉿kali)-[~/Documents/THM/borderland]
└─$ nmap -sV -Pn 172.16.1.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-02 16:25 WIB
Nmap scan report for 172.16.1.128
Host is up (0.40s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE    VERSION
21/tcp   open  ftp        vsftpd 2.3.4
179/tcp  open  tcpwrapped
2601/tcp open  quagga     Quagga routing software 1.2.4 (Derivative
2605/tcp open  quagga     Quagga routing software 1.2.4 (Derivative
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at
.
Nmap done: 1 IP address (1 host up) scanned in 62.66 seconds
```

(Avant) Scan d'une machine : 23 minutes

Avec Ligolo-ng : 62 secondes.

Ligolo-ng modélisé dans la démarche EBIOS

Sources de risques et objectifs visés

Attaquant provenant d'Internet ou d'un réseau adjacent ayant compromis un service et souhaitant se latéraliser sur des réseaux internes.

Chemin d'attaque

Machine initialement compromise (phishing, vulnérabilité)
Saut de machine en machine

Mesures de sécurité

Alimenter les mesures : filtrage egress, segmentation, détection tunnel, bastion, durcissement.

CYSLAB
CGI Business Consulting

Exemple de trois chemins d'attaques

Objectif : matérialiser les points où le pivot devient possible.

Chemin A — poste bureautique

- Hameçonnage / compte compromis
- Poste utilisateur
- Flux sortant autorisé
- Pivot vers VLAN applicatif
- Accès DB / fichiers métier

Chemin B — serveur exposé

- Service web vulnérable
- Serveur DMZ
- Compte de service réutilisé
- Rebond vers admin interne
- Impact SI critique

Chemin C — prestataire

- VPN tiers
- Poste support
- RDP / SMB ouverts
- Rebond latéral
- Exfiltration ou chiffrement

Vulnérabilités permettant l'exécution des actions élémentaires

Ces exemples ne sont pas des prérequis à Ligolo-ng : ce sont les conditions qui rendent un pivot crédible dans un scénario.

Segmentation permissive

Flux inter-zones trop larges, règles "any/any", absence de filtrage egress par destination et port.

Identités réutilisées

Mots de passe partagés, comptes locaux identiques, comptes de service sur-privilégiés ou non rotatifs.

Services latéraux exposés

RDP, SMB, WinRM, SSH, bases de données ou interfaces admin accessibles depuis des zones non prévues.

Postes peu durcis

Absence d'EDR, exécution binaire non contrôlée, droits admin locaux, journaux insuffisants.

Sorties Internet peu contrôlées

TLS sortant non catégorisé, proxy non authentifiant, DNS direct, absence d'allow-list par usage.

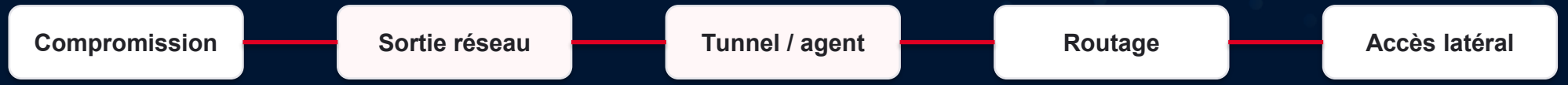
Supervision incomplète

Peu de corrélation entre nouveaux processus, connexions sortantes et scans internes.

Exemples à intégrer dans les scénarios : CVE sur service exposé, mauvais cloisonnement AD, secrets en clair dans scripts, règle firewall historique, compte prestataire dormant.

Mesures anti-pivoting

Une défense efficace combine prévention, détection et capacité de confinement. L'objectif n'est pas seulement de bloquer l'outil, mais de casser le chemin.



Prévenir

Filtrage egress strict, proxy authentifié, allow-list destinations, blocage DNS direct, durcissement postes et serveurs.

Cloisonner

Micro-segmentation, ACL par besoin métier, bastions d'administration, interdiction des flux latéraux par défaut.

Détecter

Alertes sur logiciel inconnu, connexions TLS persistantes, scans internes.

Réagir

Quarantaine EDR/NAC, révocation comptes, coupure flux, collecte forensic, playbook "pivot suspecté".

Utilisation de Ligolo-ng dans la cadre d’un audit

Objectif : montrer un pivot “VPN-like” sans fournir un mode opératoire hors cadre.

1 → 2 → 3 → 4

Préparer

Périmètre, autorisations, VM/lab, plan d’adressage.

Connecter

Agent vers proxy via flux sortant explicitement autorisé.

Configurer

Créer l’interface TUN, associer la session et les routes lab.

Observer

Tester connectivité, logs, détections et points de blocage.

À éviter dans le déroulement de l’audit : binaires non maîtrisés, cibles réelles, données clientes, scans agressifs.

Retour d’expérience : pivot par le prestataire

Cas d’école pour relier un incident prestataire à un scénario stratégique EBIOS : exposition d’un point d’administration, rebond applicatif, puis atteinte de l’Active Directory.

Chemin d’attaque plausible

VPN prestataire autorisé mais insuffisamment borné : accès direct à un jump server interne.

Depuis le jump server, découverte de flux autorisés vers un serveur applicatif exposant des comptes ou secrets techniques.

Le serveur applicatif sert de tremplin vers l’AD : comptes de service trop privilégiés, délégations ou administration distante permissive.

Vulnérabilités / faiblesses observées

VPN tiers trop large ; jump server partagé, sessions peu journalisées.

Secrets applicatifs ou comptes de service sur-privilégiés ; flux ouverts.

Mesures pour casser le pivot

Bastion prestataire dédié : PAM/JIT, MFA fort, vérification de posture.

Cloisonnement nominatif + EDR/NDR ; tiering AD, gMSA, droits locaux réduits.

Le risque n’est pas seulement l’accès VPN du prestataire, mais la chaîne d’autorisations qui transforme cet accès en compromission du domaine.

Messages clés pour les RSSI / auditeurs

Ligolo-ng rend visible un problème souvent abstrait : la segmentation ne vaut que si les flux et les contrôles tiennent face au pivot.

- Très utile en lab pour démontrer des chemins d’attaque réalistes.
- À manier avec règles d’engagement, journalisation et arrêt d’urgence.

Merci !

Avez-vous des questions ?

CYSLAB
CGI Business Consulting