

DOCUMENT DE RÉFÉRENCE CONFIDENTIEL : ALIGNEMENT BLUE TEAM / RED TEAM

L'Art de l'Intrusion : Méthodologie et Outils de Red Team

Manuel tactique de l'opérateur : De la reconnaissance passive à l'accès initial.



La Boucle Tactique

La maîtrise de l'orchestration garantit le succès. Une mission Red Team n'a de valeur que si l'organisation ciblée possède un niveau de maturité de sécurité suffisant.

Focus du Document : Ce manuel décortique les phases critiques menant à la brèche du périmètre.

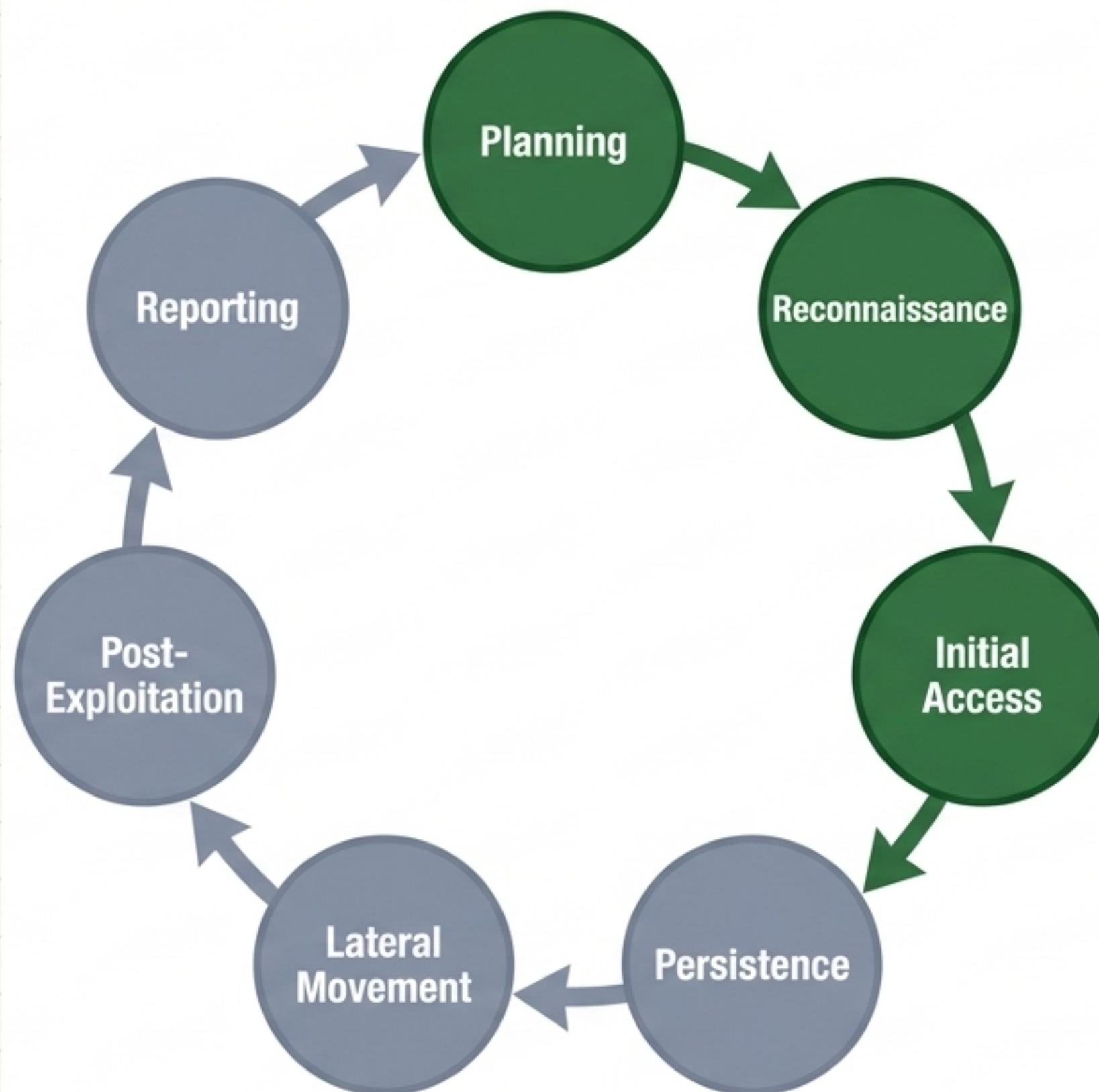


Figure 4-1 Red Team Methodology

Phase 1 : Planification et Prérequis

Définition du Périmètre (ROE)



Les **Règles d'Engagement (ROE)** documentent les **cibles exclues** et les **limites**. Elles doivent **simuler un acteur de menace spécifique**, ou être **opportunistes**, et être **signées par la direction**.

Le Cercle de Confiance (POC)



Limiter la planification à **une ou deux personnes de confiance (POC)** côté client. Plus le cercle s'élargit, plus le **risque de compromission prématurée de l'exercice** augmente.

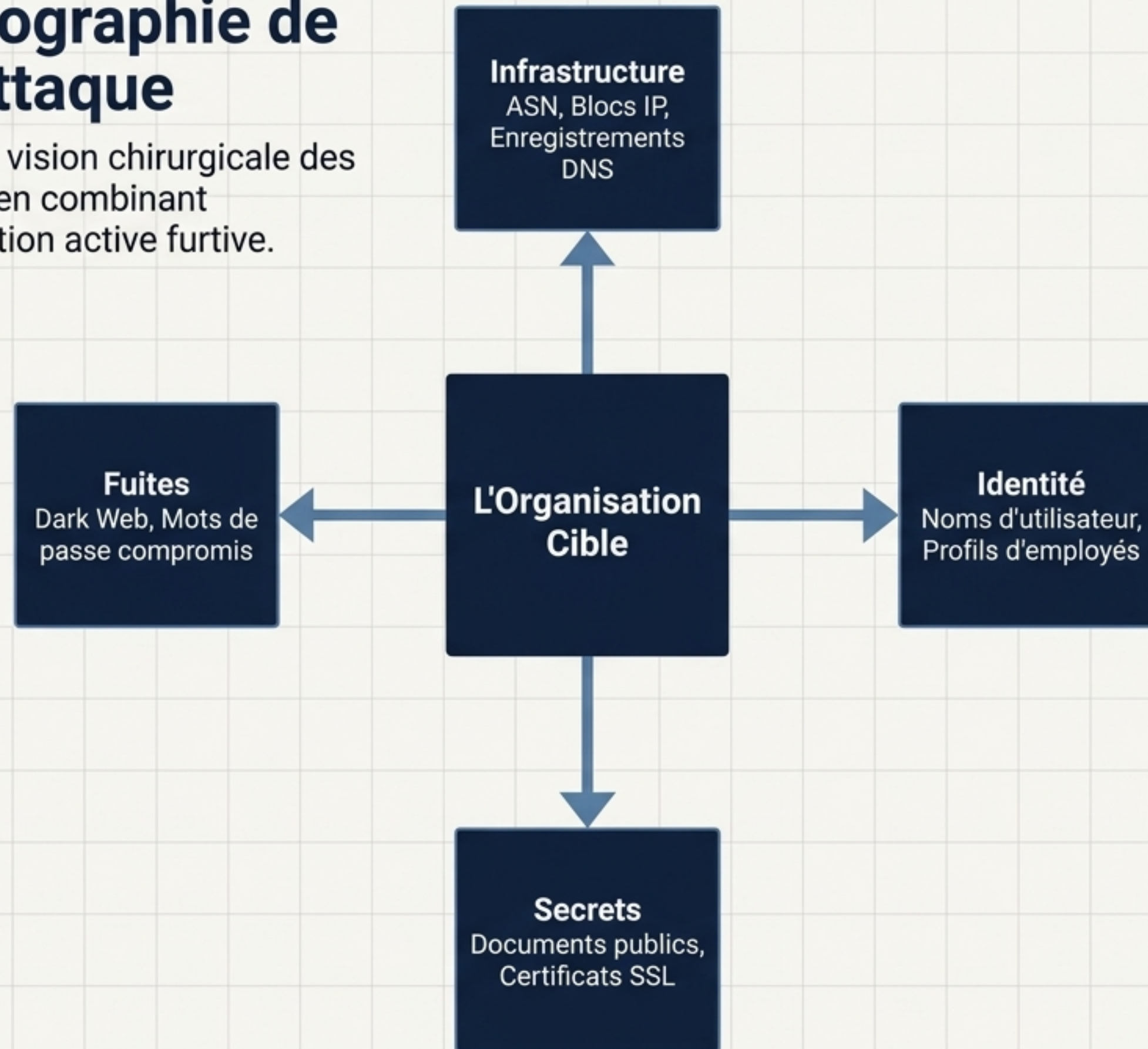
Communications Hors Bande



Mise en place obligatoire d'un **canal chiffré indépendant** (ex: Signal) **avant l'exécution** pour **alerter le POC** en cas de problème ou de déclenchement d'**alertes SOC**.

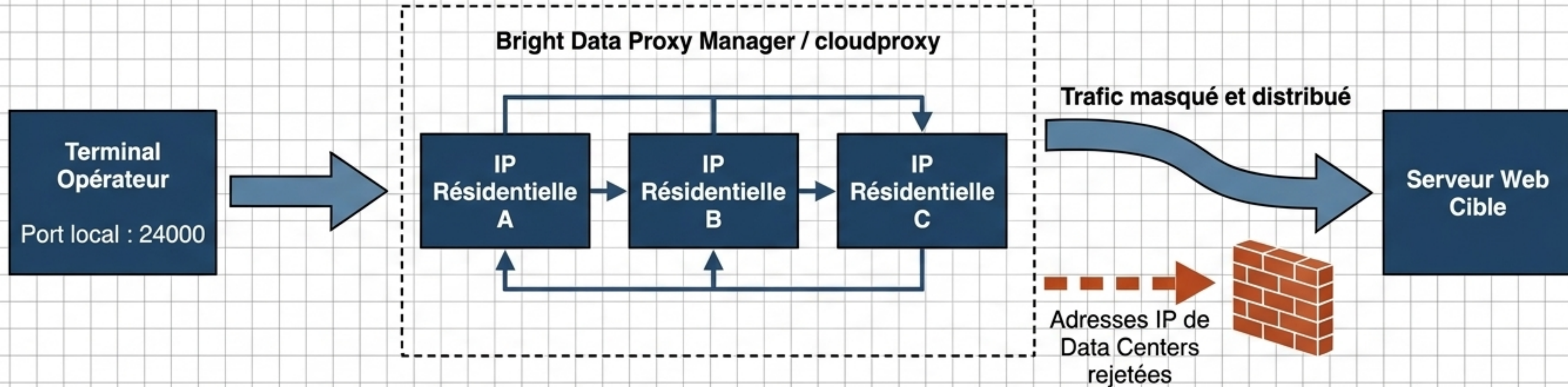
Phase 2 : Cartographie de la Surface d'Attaque

L'objectif est d'obtenir une vision chirurgicale des points d'entrée potentiels en combinant collecte passive et interaction active furtive.



Rester Invisible : L'Architecture Proxy

L'utilisation de serveurs mandataires résidentiels permet d'éviter la limitation de débit (throttling) et le blocage par les centres de données.



Configuration REQUISE :

- Protocole HTTPS
- Analyse SSL activée
- Certificat ca.crt installé localement

Cartographie de l'Infrastructure Externe

Énumération par Blocs IP (ASN)



L'exploitation des Numéros de Système Autonome (ASN) révèle les blocs d'adresses IP appartenant à l'entreprise, souvent oubliés ou négligés par les équipes de sécurité.

Énumération par Noms de Domaine

```
## Example command to query all the DNS records for the output of the  
discovered subdomains.
```

```
dnsx -l output.txt -recon -o output_dnsx.txt
```

```
dnsx v1.2.1  
projectdiscovery.io
```

```
[INF] Current dnsx version 1.2.1 (latest)  
mail.h4cker.org [A] [185.199.108.153]  
mail.h4cker.org [A] [185.199.109.153]  
mail.h4cker.org [A] [185.199.110.153]  
mail.h4cker.org [AAAA] [2606:50c0:8002::153]  
mail.h4cker.org [AAAA] [2606:50c0:8001::153]  
mail.h4cker.org [AAAA] [2606:50c0:8000::153]  
mail.h4cker.org [AAAA] [2606:50c0:8003::153]  
mail.h4cker.org [CNAME] [pentestplus.github.io]  
mail.h4cker.org [SOA] [ns-1622.awsdns-18.co.uk]  
mail.h4cker.org [SOA] [awsdns-hostmaster.amazon.com]
```

Outils : subfinder (découverte passive), dnsx (résolution active), httpx (analyse des en-têtes web).

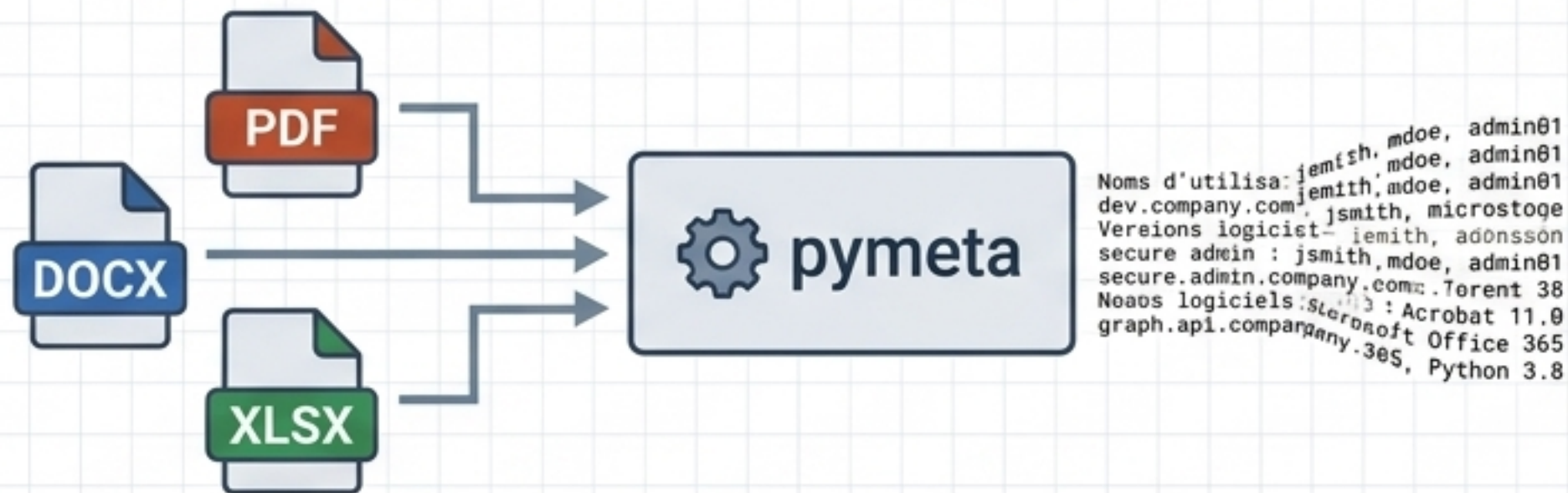
Exploitation de la Confiance et de la Transparence

Audit SSL (crt.sh)

ID	Logged At	Common Name	Issuer
188031	2021-07-21 15:22:57	...	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
188648	2021-07-21 18:23:59	...	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
188057	2021-07-21 15:23:59	intern.company.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
188668	2021-07-21 18:33:59	dev.company.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
188079	2021-07-21 15:23:10	secure.admin.company.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
188850	2021-07-21 18:33:37	...	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
188651	2021-07-21 18:34:53	graph.api.company.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
188636	2021-07-21 18:33:58	...	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA

Les journaux publics d'audit des autorités de certification dévoilent involontairement l'infrastructure interne cachée.

Extraction de Métadonnées (pymeta)



Noms d'utilisateurs : jsmith, mdoe, admin01

Versions logiciels : Adobe Acrobat 11.0,
Microsoft Office 365, Python 3.8

L'outil pymeta automatise l'extraction de schémas de noms et de configurations à partir de documents inoffensifs publiés en ligne par l'entreprise.

Cibler l'Humain : L'Usine à Identifiants

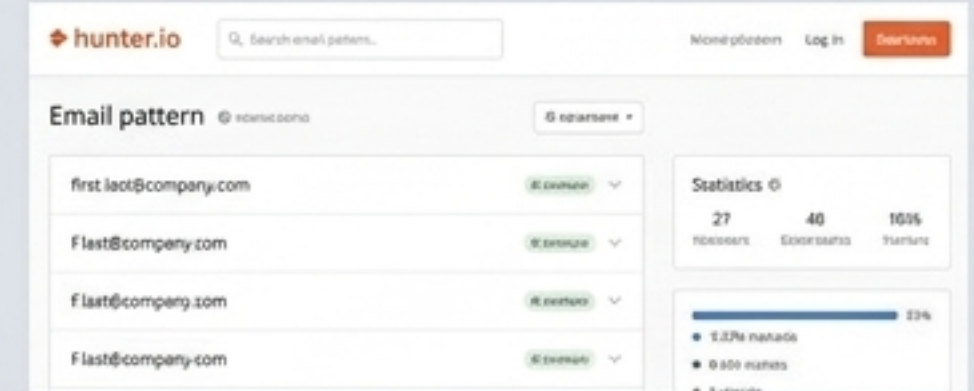
Collecte Brute (OSINT)

Hunter.io

LinkedIn

USStaff

Extraction de modèles d'adresses e-mail
et de listes brutes d'employés.



Génération et Filtrage (NameSpi)

Outil : **NameSpi**

Génération de noms statistiquement
probables et contournement des restrictions
de sécurité de LinkedIn via l'option -lir.

Validation et Enrichissement

Validation croisée

Le Trésor des Fuites (Dark Web)

Utilisation de **HavelBeenPwned** (14+ milliards de comptes) et **Flare.io** pour repérer les mots de passe et clés API pré-compromis des employés ciblés.

Matrice de Diagnostic : Topologie d'Identité M365

Résultats de l'outil o365-realminfo. L'impact direct sur la stratégie d'attaque de l'accès initial.

	Domaine Géré (Managed)	Domaine Fédéré (Federated)	Inconnu (Unknown)
Indicateur	NameSpaceType: Managed	NameSpaceType: Federated	Aucun enregistrement
Architecture	L'authentification est gérée à 100% dans le cloud Microsoft.	S'appuie sur l'infrastructure locale de la cible (Active Directory / ADFS).	L'organisation n'utilise potentiellement pas M365 pour la gestion des identités.
Stratégie Red Team	Cibler directement les portails web M365 et les API Azure avec les identifiants récoltés.	Cibler l'infrastructure sur site ; possibilité de contourner les politiques cloud si le serveur ADFS est vulnérable.	Pivoter vers la recherche d'autres fournisseurs SSO (Okta, Google Workspace, etc.).



Phase 3 : L'Accès Initial

Le renseignement est collecté. L'objectif passe désormais de l'invisibilité passive à la friction calculée : briser le périmètre externe via les identités, les appareils mobiles ou les vulnérabilités applicatives.

[PASSAGE À L'EXPLOITATION]

Le Pipeline de Password Spraying



RÈGLE D'OR DE L'OPÉRATEUR :

Rotation IP obligatoire via Proxy Résidentiel ET délai d'attente strict de 2 heures minimum entre chaque salve pour contourner le verrouillage Active Directory.

Contournement des Défenses : Postes de Travail (EDR & MDM)

Ciblage Endpoints MDM

- VMware AirWatch,
- Intune,
- MobileIron

> Outil : dauthi

Exploitation des angles morts de journalisation sur les plateformes de gestion mobile.

Évasion EDR via Side-loading

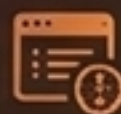
Processus Windows
Légitime

Charge Utile
(Payload) de
l'Opérateur

Process Hollowing /
Side-loading

L'Art du Silence (Génération avec ScareCrow & Mangle)

- Suppression des hooks de l'EDR (Unhooking)
- Utilisation d'appels système personnalisés (Custom Syscalls)
- Signature de la charge par de faux certificats
- Restriction d'exécution via IsDomainJoined



Camouflage final : Empaquetage de la charge utile via Advanced Installer pour simuler un déploiement logiciel d'entreprise légitime.

L'Arsenal de l'Opérateur : Synthèse des Outils

Infrastructure & Routage

cloudproxy : Génération d'API de proxys.

Bright Data : Réseau de proxys résidentiels.

subfinder : Découverte passive de sous-domaines.

dnsx : Résolution DNS active.

httpx : Analyse des en-têtes HTTP.

Identité & Renseignement

pymeta : Extraction de métadonnées documentaires.

Hunter.io : Identification des schémas d'e-mails.

NameSpi : Génération et filtrage de noms d'utilisateurs (OSINT).

Flare / HaveIBeenPwned : Analyse des fuites de données du Dark Web.

Diagnostic Pré-Attaque

o365-realminfo : Requêtes de domaine utilisateur (Managed vs Federated).

KnockKnock : Validation furtive via l'API externe Teams/OneDrive.

Armement & Contournement

TeamFiltration : Pulvérisation de mots de passe et exfiltration M365.

dauthi : Ciblage des plateformes MDM.

ScareCrow : Générateur de charge utile pour contournement EDR.

Mangle : Manipulation d'exécutables pour l'évasion.

Leçons Tactiques

```
root@target:~# accès initial  
établi  
root@target:~# début de  
l'escalade de privilèges...
```

1. La Furtivité prime sur la Vitesse

L'utilisation de proxies résidentiels rotatifs et le respect strict des fenêtres de délai (ex: 2 heures) font la différence entre une brèche réussie et une détection immédiate par le SOC.

2. L'Identité est le Nouveau Périmètre

La majorité des succès initiaux proviennent de la pulvérisation de mots de passe et de l'exploitation des configurations complexes (M365/ADFS), bien plus souvent que des failles zero-day.

3. La Rigueur de l'Opérateur

De la définition stricte des ROE à l'orchestration prudente de l'arsenal, c'est la méthodologie structurée qui garantit une réelle valeur diagnostique pour la Blue Team.