Ingénierie Sociale & Hacking Éthique — Manuel Complet

Un cours structuré pour comprendre en profondeur l'ingénierie sociale, l'OSINT et le hacking éthique.

PARTIE 1 — FONDATIONS

Chapitre 1. Qu'est-ce que l'ingénierie sociale ?

L'ingénierie sociale désigne l'ensemble des techniques utilisées pour manipuler des individus afin qu'ils divulguent des informations confidentielles, accordent un accès, ou effectuent une action qu'ils n'auraient pas faite en connaissance de cause. Contrairement au piratage technique, qui exploite des failles logicielles, l'ingénierie sociale exploite des failles humaines : confiance, habitude, politesse, peur, curiosité.

Kevin Mitnick, l'un des hackers les plus célèbres au monde, résumait cela ainsi : le maillon le plus faible d'un système de sécurité n'est presque jamais la machine, mais la personne qui l'utilise. On peut investir des millions dans des pare-feux et du chiffrement ; un simple coup de téléphone bien mené peut suffire à contourner tout cela.

Pourquoi ça fonctionne

Le cerveau humain fonctionne par raccourcis. Face à une situation qui ressemble à quelque chose de connu (un email qui ressemble à ceux de la banque, une voix qui semble autoritaire au téléphone), on ne remet pas systématiquement en question chaque détail — on réagit selon un schéma appris. Les attaquants exploitent précisément ces raccourcis cognitifs, appelés heuristiques.

Trois idées structurent tout ce manuel :

1. **L'information précède la manipulation.** Plus l'attaquant en sait sur la cible, plus le prétexte est crédible. D'où l'importance centrale de l'OSINT.
2. **La manipulation exploite des biais universels**, pas des faiblesses individuelles. N'importe qui peut être victime, y compris des experts en sécurité.

3. **La défense repose sur des processus, pas sur la vigilance individuelle.** Compter sur "les gens feront attention" est une stratégie vouée à l'échec ; il faut des garde-fous systémiques.

Chapitre 2. Histoire et évolution

Les origines (avant l'informatique)

Les techniques de manipulation sociale précèdent largement l'informatique. Les escroqueries à la confiance ("confidence tricks") du 19e siècle utilisaient déjà les mêmes ressorts : se faire passer pour une autorité, créer un climat de confiance rapide, exploiter la cupidité ou la peur.

L'ère du phreaking (1960s-1970s)

Les premiers "hackers téléphoniques" (phreakers) utilisaient l'ingénierie sociale pour obtenir des informations techniques des opérateurs télécoms — se faisant passer pour des employés afin d'obtenir des codes ou des informations sur le réseau.

Kevin Mitnick et la popularisation (1980s-1990s)

Mitnick a démontré à grande échelle que l'accès aux systèmes les plus protégés passait souvent par un simple appel téléphonique bien construit. Son livre *The Art of Deception* (2002) reste une référence, documentant des dizaines de scénarios réels.

L'ère numérique (2000s-aujourd'hui)

Avec la démocratisation d'internet, les réseaux sociaux et le volume massif de données personnelles disponibles publiquement, l'ingénierie sociale s'est industrialisée : phishing de masse, spear phishing ciblé grâce aux réseaux sociaux, deepfakes vocaux pour le vishing. Les attaques par ransomware modernes commencent presque systématiquement par un vecteur d'ingénierie sociale (email piégé, faux support technique).

PARTIE 2 — PSYCHOLOGIE DE LA MANIPULATION

Chapitre 3. Les principes de Cialdini

Robert Cialdini, psychologue, a identifié six (puis sept) principes d'influence dans son ouvrage *Influence et manipulation*. Ces principes sont devenus la base théorique de

l'ingénierie sociale moderne.

1. Réciprocité

On se sent obligé de rendre un service reçu. Un attaquant peut "aider" une cible (résoudre un faux problème technique) avant de demander quelque chose en retour — la cible se sentira redevable.

2. Engagement et cohérence

Une fois qu'une personne s'est engagée publiquement ou même mentalement sur une position, elle cherche à rester cohérente avec ce choix. Un attaquant peut faire dire "oui" à une cible sur une petite chose anodine avant de demander quelque chose de plus important dans la continuité logique.

3. Preuve sociale

On imite le comportement des autres, surtout en situation d'incertitude. "Vos collègues ont déjà validé cette procédure" rassure et abaisse la vigilance.

4. Sympathie (Liking)

On accède plus facilement aux demandes de personnes qu'on apprécie, qui nous ressemblent, ou qui nous complimentent. Les attaquants créent délibérément des points communs (même ville, mêmes centres d'intérêt trouvés sur les réseaux sociaux).

5. Autorité

On obéit aux figures d'autorité, même symboliques (un uniforme, un titre, un ton assuré). Se faire passer pour un technicien IT, un cadre supérieur, ou un agent des forces de l'ordre exploite ce biais.

6. Rareté / urgence

On accorde plus de valeur à ce qui est rare ou limité dans le temps. "Vous devez agir dans les 10 prochaines minutes" court-circuite la réflexion critique.

7. Unité (ajouté plus tard par Cialdini)

Le sentiment d'appartenance à un groupe commun ("nous, employés de cette entreprise") renforce la confiance envers quelqu'un perçu comme faisant partie du même groupe.

Chapitre 4. Biais cognitifs exploités

Au-delà des principes de Cialdini, plusieurs biais cognitifs spécifiques sont exploités :

- **Biais de confirmation** : on cherche des informations qui confirment ce qu'on croit déjà. Si un email "confirme" une attente (facture attendue, colis en cours), on le traite avec moins de suspicion.
- **Effet de halo** : une apparence professionnelle (logo, mise en page soignée) suffit à donner une impression de légitimité globale.
- **Aversion à la perte** : la peur de perdre quelque chose (compte bloqué, amende) motive plus que la perspective d'un gain équivalent.
- **Surcharge cognitive** : dans un contexte de stress ou de fatigue (fin de journée, période de forte activité), la vigilance diminue mécaniquement.
- **Biais d'autorité perçue numérique** : un nom de domaine ressemblant, une adresse email "presque" correcte, suffisent souvent car on ne vérifie pas caractère par caractère.

Chapitre 5. Profils de cibles et prétextes

Les attaquants adaptent leur approche selon le profil de la cible :

- **Nouveaux employés** : ne connaissent pas encore les procédures internes, hésitent à remettre en question une demande par peur de mal faire.
- **Personnel support/accueil** : habitué à aider, formé à la serviabilité, donc plus vulnérable aux demandes qui exploitent cette disposition.
- **Cadres dirigeants** : cibles de choix pour le spear phishing (fraude au président), car leurs décisions ont un impact financier direct.
- **Personnel technique (IT)** : paradoxalement vulnérable au faux support technique inversé — un attaquant se faisant passer pour un collègue en urgence.

PARTIE 3 — OSINT : LA RECONNAISSANCE

Chapitre 6. Principes de l'OSINT

L'Open Source Intelligence (OSINT) désigne la collecte et l'analyse d'informations provenant de sources publiques et légalement accessibles : réseaux sociaux, sites web, registres publics, forums, données de fuite indexées, métadonnées de fichiers.

Dans le cadre de l'ingénierie sociale (ou d'un audit autorisé), l'OSINT sert à :

1. **Cartographier l'organisation** — organigramme, filiales, prestataires, outils utilisés.
2. **Identifier les individus** — noms, fonctions, habitudes, présence en ligne.
3. **Construire un prétexte crédible** — plus les détails sont précis (nom du logiciel de ticketing interne, nom d'un vrai projet en cours), plus l'attaque paraît légitime.
4. **Repérer les failles d'exposition** — documents mal configurés, informations sensibles publiées par erreur.

Chapitre 7. Sources et catégories de collecte

Sources organisationnelles

- Site web officiel (pages "équipe", "carrières")
- Offres d'emploi (révèlent la stack technique, les outils internes, parfois l'organisation des équipes)
- Communiqués de presse, rapports annuels (pour les sociétés cotées)
- Registres publics (Infogreffe en France, Companies House au UK) : dirigeants, dates de création, adresses.

Sources individuelles

- Réseaux sociaux professionnels (LinkedIn) : parcours, poste actuel, relations
- Réseaux sociaux personnels : centres d'intérêt, habitudes, localisation
- Forums et communautés (GitHub, Stack Overflow, Reddit) : pseudonymes réutilisés, compétences techniques

Sources techniques

- Métadonnées de documents publiés (auteur, logiciel utilisé, chemins de fichiers internes)
- Enregistrements DNS et certificats (sous-domaines, infrastructure)
- Recherche de fuites de données (emails compromis, mots de passe réutilisés)

Chapitre 8. Méthodologie de collecte structurée

Une reconnaissance OSINT efficace suit un processus, pas une collecte aléatoire :

1. **Définir le périmètre** — qu'est-ce qui est autorisé à être recherché (dans un cadre d'audit) ?
2. **Collecte large** — identifier tous les points d'entrée possibles (domaines, réseaux sociaux, employés).
3. **Croisement des données** — relier les informations entre elles (un même pseudonyme utilisé sur plusieurs plateformes, une même photo de profil).
4. **Vérification** — éliminer les faux positifs, confirmer les informations par recoupement.
5. **Priorisation** — identifier les cibles ou informations les plus exploitables pour l'objectif fixé.
6. **Documentation** — consigner les sources et la méthode, essentiel pour un rapport d'audit professionnel.

Chapitre 9. Outils courants (aperçu conceptuel)

Sans entrer dans le détail opérationnel, voici les grandes familles d'outils utilisés en reconnaissance OSINT :

- **Recherche de pseudonymes** : outils qui vérifient la présence d'un nom d'utilisateur sur de nombreuses plateformes simultanément.
- **Vérification d'email** : outils qui déterminent si une adresse email est associée à des comptes existants sur divers services.
- **Reconnaissance de domaine** : outils qui collectent sous-domaines, historique DNS, certificats SSL associés à une organisation.
- **Recherche de fuites** : bases de données consultables recensant les identifiants compromis lors de fuites connues.
- **Analyse d'image géographique** : techniques d'estimation de localisation à partir d'éléments visuels (végétation, architecture, panneaux).
- **Visualisation de liens** : outils de cartographie qui relient entités, personnes et organisations sous forme de graphe.

PARTIE 4 — VECTEURS D'ATTAQUE EN DÉTAIL

Chapitre 10. Phishing et spear phishing

Le phishing consiste à envoyer des communications frauduleuses imitant une source légitime, dans le but d'obtenir des informations ou de faire cliquer sur un lien malveillant.

Caractéristiques du phishing de masse :

- Envoi à grande échelle, faible taux de personnalisation
- Imite des marques connues (banques, services de livraison)
- Compte sur le volume : même un taux de réussite de 1% est rentable à grande échelle

Le spear phishing est ciblé et personnalisé grâce à l'OSINT : nom du destinataire, nom du service, référence à un projet réel en cours, style d'écriture imitant un collègue connu. Le taux de réussite est nettement plus élevé car les signaux d'alerte habituels (fautes, formulation générique) sont absents.

La fraude au président (Business Email Compromise) est une forme évoluée de spear phishing où l'attaquant usurpe l'identité d'un dirigeant pour ordonner un virement urgent et confidentiel à un employé du service financier.

Chapitre 11. Vishing (phishing vocal)

Le vishing utilise le téléphone. Il exploite particulièrement bien le principe d'autorité et d'urgence, car la voix humaine en temps réel laisse peu de temps à la cible pour réfléchir ou vérifier.

Scénarios classiques :

- Faux support technique signalant un problème urgent
- Faux service financier demandant une vérification d'identité
- Faux appel interne (RH, direction) demandant une information confidentielle

L'essor des outils de synthèse vocale rend aujourd'hui possible l'imitation de la voix d'une personne réelle (deepfake vocal), amplifiant considérablement la crédibilité de ce vecteur.

Chapitre 12. Prétexting

Le pretexting consiste à construire un scénario complet et crédible justifiant la demande

d'information. Contrairement au phishing qui repose sur un message écrit unique, le pretexting est souvent interactif et peut se dérouler sur plusieurs échanges.

Exemple de structure d'un prétexte réussi :

1. Établir une identité crédible (nom, fonction, référence vérifiable)
2. Justifier le contact (raison plausible, urgence modérée)
3. Construire la confiance progressivement (petites demandes avant la demande principale)
4. Formuler la demande réelle de façon naturelle, dans la continuité de l'échange

Chapitre 13. Baiting, tailgating, quid pro quo

- **Baiting** : appâter la cible avec quelque chose de désirable (clé USB "trouvée" contenant un logiciel malveillant, offre trop belle pour être vraie).
- **Tailgating / piggybacking** : suivre physiquement une personne autorisée pour pénétrer dans une zone sécurisée, en exploitant la politesse (tenir la porte).
- **Quid pro quo** : proposer un service en échange d'une action ou d'une information ("je répare votre problème informatique, donnez-moi votre mot de passe pour vérifier").

Chapitre 14. Étapes d'une attaque complète

Une attaque d'ingénierie sociale structurée suit généralement quatre phases :

1. **Reconnaissance** (chapitre 6-9) — collecte d'informations sur la cible.
2. **Développement de la relation** — premier contact, établissement de la confiance, souvent anodin en apparence.
3. **Exploitation** — la demande réelle est formulée, appuyée sur les leviers psychologiques identifiés.
4. **Exécution / sortie** — l'attaquant obtient ce qu'il cherche et se retire sans éveiller de soupçons, parfois en laissant une porte ouverte pour une future exploitation.

PARTIE 5 — CADRE ÉTHIQUE ET LÉGAL

Chapitre 15. Le hacking éthique : définition et cadre

Le hacking éthique consiste à utiliser les mêmes techniques que des attaquants malveillants, mais dans un cadre légal, autorisé et encadré, dans le but d'identifier des vulnérabilités avant qu'elles ne soient exploitées.

Trois conditions définissent un test légitime :

1. **Autorisation écrite explicite** du propriétaire du système ou de l'organisation testée
2. **Périmètre défini** — quelles cibles, quelles techniques, quelles limites
3. **Objectif défensif** — le but est d'améliorer la sécurité, avec un rapport et des recommandations, pas de nuire

Chapitre 16. Méthodologie d'un audit d'ingénierie sociale

1. **Cadrage (Statement of Work)** — contrat définissant précisément le périmètre, les techniques autorisées et exclues, les personnes de contact d'urgence.
2. **Reconnaissance OSINT** — collecte d'informations dans les limites autorisées.
3. **Conception des scénarios** — prétextes réalistes mais proportionnés, validés avec le client si nécessaire.
4. **Exécution contrôlée** — traçabilité complète, arrêt immédiat si un risque réel apparaît (ex : la cible semble en détresse).
5. **Rapport** — description factuelle, taux de réussite, vulnérabilités identifiées, recommandations concrètes et priorisées.
6. **Restitution et formation** — présentation aux équipes concernées dans un esprit constructif, jamais dans le but d'humilier des individus nommément.

Chapitre 17. Cadre légal (France et international)

En France :

- Article 226-4-1 du Code pénal : usurpation d'identité numérique, punie d'un an d'emprisonnement et 15 000€ d'amende.
- Article 323-1 du Code pénal (loi Godfrain) : accès ou maintien frauduleux dans un système de traitement automatisé de données.
- Le RGPD encadre strictement la collecte et le traitement de données personnelles, y

compris dans un cadre d'audit — la reconnaissance OSINT doit rester proportionnée et documentée.

Principe général : sans mandat écrit explicite couvrant précisément les actions entreprises, toute tentative d'ingénierie sociale sur des tiers constitue une infraction pénale, quelle que soit l'intention déclarée.

PARTIE 6 — DÉFENSE ET SENSIBILISATION

Chapitre 18. Construire une défense organisationnelle

La défense contre l'ingénierie sociale ne peut pas reposer uniquement sur la vigilance individuelle — elle doit être intégrée dans les processus :

- **Vérification par canal indépendant** : toute demande sensible (virement, changement d'accès, information confidentielle) doit être confirmée via un canal différent de celui utilisé pour la demande (rappeler sur un numéro connu, pas celui fourni dans l'email).
- **Principe du moindre privilège** : chaque personne n'a accès qu'à ce qui est strictement nécessaire à sa fonction, limitant l'impact d'une compromission individuelle.
- **Procédures d'urgence standardisées** : un protocole clair et non négociable retire le pouvoir de persuasion du levier "urgence".
- **Culture du signalement sans blâme** : les employés doivent pouvoir signaler une tentative suspecte (ou une erreur commise) sans crainte de sanction, pour que l'information remonte rapidement.

Chapitre 19. Formation et sensibilisation des utilisateurs

- **Simulations régulières** (campagnes de phishing internes) avec retour pédagogique immédiat, jamais punitif.
- **Exemples concrets et récents** plutôt que des principes abstraits — les cas réels marquent davantage.
- **Formation continue**, pas un événement unique : les techniques évoluent, la sensibilisation doit suivre.
- **Réduction de l'empreinte OSINT organisationnelle** : limiter les informations

exposées publiquement (organigrammes détaillés, formats d'adresses email prévisibles, métadonnées de documents publiés).

Chapitre 20. Indicateurs d'alerte à enseigner

Les signaux suivants doivent devenir des réflexes de vérification, sans paranoïa excessive :

- Urgence inhabituelle associée à une demande sensible
- Demande de contournement d'une procédure normale
- Contact inhabituel (canal, horaire, ton) même s'il semble provenir d'une source connue
- Demande d'information qui ne devrait normalement pas être nécessaire pour la tâche annoncée
- Petites incohérences (adresse email légèrement différente, ton inhabituel d'un contact connu)

CONCLUSION GÉNÉRALE

L'ingénierie sociale reste, année après année, le vecteur d'attaque le plus efficace et le plus utilisé dans les incidents de sécurité majeurs — bien plus que les failles purement techniques. Elle exploite des mécanismes psychologiques universels, documentés depuis des décennies, et amplifiés aujourd'hui par la quantité d'informations personnelles disponibles publiquement.

Une posture de sécurité solide combine trois piliers : une **reconnaissance de sa propre exposition** (ce que l'OSINT révèle sur une organisation), des **processus de vérification systémiques** qui ne dépendent pas uniquement de la vigilance individuelle, et une **formation continue et non punitive** des personnes qui restent, in fine, la cible privilégiée de toute attaque.

La compréhension de ces mécanismes n'a de valeur que dans un cadre éthique et légal clair : elle sert à protéger, former et anticiper — jamais à nuire.

Fin du manuel. Bonne lecture à la plage. -e

Ingénierie Sociale & OSINT — Module de Maîtrise Pratique

Complément au manuel principal : exercices, méthodologie OSINT avancée, études de cas réels.

PARTIE 1 — ÉTUDES DE CAS RÉELS

Cas 1 — Kevin Mitnick et la reconnaissance téléphonique (années 1990)

Mitnick obtenait fréquemment des accès à des systèmes protégés sans jamais toucher un clavier lors de la phase initiale. Sa méthode typique : appeler un standard, se présenter comme un employé d'un autre service en difficulté technique, demander une information apparemment anodine (un nom, un numéro de poste). Chaque appel enrichissait le suivant. Après plusieurs appels, il disposait d'assez de vocabulaire interne (noms de projets, de logiciels, d'organigramme) pour se faire passer pour un employé légitime auprès du service informatique et obtenir un mot de passe.

Leçon clé : aucune information isolée n'est dangereuse ; c'est l'accumulation et le recoupement qui construisent une attaque crédible. C'est le principe fondateur de toute reconnaissance OSINT moderne.

Cas 2 — La fraude au président (Business Email Compromise), entreprise française, 2015-2016

Plusieurs grandes entreprises françaises ont été victimes de fraudes où un attaquant, après avoir étudié l'organigramme et le style de communication du dirigeant via des sources publiques (interviews, réseaux sociaux, communiqués), envoyait un email usurpant son identité à un responsable financier, demandant un virement urgent et confidentiel vers un compte à l'étranger, en insistant sur la discrétion ("ne pas en parler avant la clôture de l'opération").

Mécanismes exploités : autorité (le dirigeant), urgence, confidentialité (empêche la vérification par les canaux normaux).

Leçon clé : la vérification par canal indépendant (rappeler le dirigeant sur son numéro connu) est la seule défense fiable contre ce type d'attaque — aucune formation ne peut

totalement neutraliser la pression hiérarchique combinée à l'urgence.

Cas 3 — Twitter, juillet 2020 : ingénierie sociale contre des employés

Des attaquants ont ciblé des employés de Twitter en se faisant passer pour le service IT interne (vishing), leur demandant de se connecter à un faux portail imitant l'outil VPN de l'entreprise. Plusieurs employés, dont certains disposant d'accès administrateurs aux outils internes, ont saisi leurs identifiants sur ce faux portail. Les attaquants ont ensuite utilisé ces accès pour prendre le contrôle de comptes Twitter de personnalités publiques.

Mécanismes exploités : autorité (faux support IT), contexte de télétravail généralisé (moins de vérification en personne), imitation fidèle des outils internes réels (renseignée par reconnaissance préalable).

Leçon clé : même des employés d'une entreprise technologique majeure, formée à la sécurité, restent vulnérables si le prétexte est suffisamment bien informé et que la procédure de vérification n'est pas totalement indépendante du canal d'attaque.

Cas 4 — RSA Security, 2011 : spear phishing ciblé

Un employé de RSA a reçu un email intitulé "2011 Recruitment Plan" contenant une pièce jointe Excel piégée. L'email semblait provenir d'une source plausible dans un contexte RH plausible pour l'entreprise. L'ouverture du fichier a exploité une faille technique, mais le point d'entrée était entièrement social : un prétexte crédible et contextuellement pertinent, déposé dans les spams mais récupéré et ouvert par curiosité.

Leçon clé : la frontière entre ingénierie sociale et exploitation technique est souvent ténue — le facteur humain reste le point d'entrée initial même dans des attaques à forte composante technique.

PARTIE 2 — MÉTHODOLOGIE OSINT AVANCÉE

Chapitre A — Cadre méthodologique structuré (cycle du renseignement)

L'OSINT professionnel suit le cycle classique du renseignement, adapté :

1. **Direction** — définir précisément la question à laquelle répondre (ex : “quelle est la surface d’exposition de l’organisation X ?”).
2. **Collecte** — rassembler les données brutes depuis les sources multiples.
3. **Traitement** — nettoyer, dédupliquer, structurer les données collectées.
4. **Analyse** — croiser les données pour en tirer des informations exploitables (pas seulement des données brutes).
5. **Diffusion** — restituer les résultats de façon claire et actionnable (rapport, graphe, timeline).

C’est exactement le principe qu’un outil comme DOSSIER opérationnalise : automatiser les étapes 2-3 (collecte + traitement via Sherlock, Holehe, Maigret, theHarvester, crt.sh, dnstwist) pour concentrer l’effort humain sur l’analyse (étape 4), visualisée via le graphe force-directed.

Chapitre B — Techniques de corrélation d’identité

La corrélation est le cœur analytique de l’OSINT : relier des identifiants disparates à une même personne ou organisation.

- **Réutilisation de pseudonyme** : un même nom d’utilisateur sur plusieurs plateformes (GitHub, Reddit, forums) est un signal fort de corrélation, à confirmer par d’autres éléments (photo, style d’écriture, horaires d’activité).
- **Réutilisation d’email** : un email utilisé pour créer un compte sur une plateforme peut être recherché sur d’autres (théorie derrière Holehe) — révèle des services associés à une même identité.
- **Empreinte stylométrique** : le style d’écriture (longueur de phrases, expressions récurrentes, fautes typiques) peut relier des comptes anonymes entre eux, bien que cette technique demande prudence et corroboration.
- **Métadonnées d’image** : données EXIF (quand présentes), mais aussi indices visuels (arrière-plan, reflets, ombres) permettant une géolocalisation approximative — le principe derrière les outils type GeoCLIP que tu explores.
- **Analyse temporelle** : les horaires de publication répétés sur différentes plateformes peuvent révéler un fuseau horaire, donc une zone géographique probable.

Chapitre C — Reconnaissance d’infrastructure (domaines

et organisations)

- **Énumération de sous-domaines** : révèle souvent des environnements de test, de staging, ou des services oubliés, moins bien sécurisés que le domaine principal.
- **Historique de certificats SSL** (via crt.sh) : les certificats sont publics dès leur émission (Certificate Transparency Logs) et révèlent souvent des sous-domaines qui n'apparaissent nulle part ailleurs.
- **Typosquatting défensif** (via dnstwist) : identifier les domaines visuellement proches d'un domaine légitime, souvent enregistrés à des fins de phishing — utile en défense pour surveiller les usurpations potentielles.
- **theHarvester** et outils similaires : agrègent emails, sous-domaines et noms associés à une organisation depuis des moteurs de recherche et sources publiques, offrant une vue d'ensemble rapide de la surface d'exposition.

Chapitre D — Construction et lecture d'un graphe d'investigation

Un graphe force-directed (comme celui de DOSSIER) représente entités et relations : chaque nœud est une identité (email, pseudo, domaine), chaque lien une relation confirmée (même compte, même mot de passe compromis, même adresse IP).

Bonnes pratiques d'analyse de graphe :

- **Les nœuds à forte connectivité** (hubs) révèlent souvent l'identité pivot d'une investigation — l'élément qui relie plusieurs branches.
- **Les nœuds isolés** peuvent indiquer soit une fausse piste, soit une identité compartimentée intentionnellement (opsec de la cible elle-même).
- **La pondération des liens** (confiance haute/moyenne/faible selon la source) évite de traiter une simple coïncidence comme une preuve.
- **La visualisation temporelle** (quand disponible) aide à repérer les changements de comportement (abandon d'un pseudonyme, création d'une nouvelle identité après une fuite).

Chapitre E — Éthique et limites de l'OSINT

Même si les données sont publiques, leur collecte et leur croisement systématique soulèvent des questions éthiques et légales :

- **Proportionnalité** : collecter uniquement ce qui est nécessaire à l'objectif déclaré.
- **RGPD** : le traitement de données personnelles, même publiques, est encadré ; une investigation OSINT professionnelle doit avoir une base légale claire (contrat, mandat).
- **Ne jamais publier de dossiers de corrélation sur des tiers sans cadre légal** — la limite entre OSINT défensif/professionnel et harcèlement ("doxxing") tient uniquement à l'intention, au cadre et à l'usage qui en est fait.

PARTIE 3 — EXERCICES ET AUTO-ÉVALUATION

Quiz 1 — Fondations et psychologie

1. Quels sont les 7 principes d'influence de Cialdini ? Donne un exemple d'exploitation pour chacun.
2. Explique la différence entre biais de confirmation et effet de halo, avec un exemple d'ingénierie sociale pour chacun.
3. Pourquoi les nouveaux employés sont-ils statistiquement plus vulnérables aux attaques d'ingénierie sociale ?
4. Dans le cas RSA (2011), quel principe psychologique explique que l'employé ait ouvert la pièce jointe malgré le filtre spam ?

Quiz 2 — Vecteurs d'attaque

5. Différencie phishing, spear phishing et fraude au président — en quoi le niveau de personnalisation change le taux de réussite ?
6. Pourquoi le vishing exploite-t-il particulièrement bien le principe d'urgence, plus que l'email ?
7. Donne un exemple concret de pretexting en 4 étapes, comme structuré dans le manuel principal.
8. Qu'est-ce qui différencie le tailgating du baiting en termes de vecteur (physique vs numérique) ?

Quiz 3 — OSINT et méthodologie

9. **Décris les 5 étapes du cycle du renseignement appliqué à l'OSINT.**
10. **Pourquoi la réutilisation de pseudonyme est-elle un signal de corrélation "fort" mais non suffisant à lui seul ?**
11. **Qu'est-ce que les Certificate Transparency Logs révèlent, et pourquoi sont-ils utiles en reconnaissance de domaine ?**
12. **Dans un graphe d'investigation, comment interpréter un nœud à très forte connectivité ?**

Quiz 4 — Cadre légal et défense

13. **Cite les deux articles du Code pénal français les plus pertinents pour l'ingénierie sociale illégale.**
14. **Pourquoi la "vérification par canal indépendant" est-elle considérée comme la défense la plus fiable contre la fraude au président ?**
15. **Explique pourquoi une culture de "signalement sans blâme" améliore la sécurité globale d'une organisation.**
16. **Quelle est la limite légale/éthique entre OSINT professionnel et doxxing ?**

Exercice pratique 1 — Analyse de scénario

Lis ce scénario et identifie : (a) le vecteur d'attaque, (b) les principes psychologiques exploités, (c) ce que la victime aurait dû vérifier.

> *"Bonjour, je suis Julien du support informatique. On a détecté une activité suspecte sur votre compte ce matin, on doit vérifier votre identité rapidement avant que le compte soit suspendu automatiquement dans 15 minutes. Pouvez-vous me confirmer votre identifiant et me donner le code que vous venez de recevoir par SMS ?"*

Exercice pratique 2 — Construction d'un prétexte (cadre défensif uniquement)

Sans écrire de script opérationnel, décris à haut niveau : si tu devais auditer (avec mandat) la résistance au phishing d'une PME, quelles 3 informations OSINT chercherais-tu en priorité pour construire un scénario crédible, et pourquoi ces 3-là plutôt que d'autres ?

Exercice pratique 3 — Construction d'un graphe

À partir de 3 identifiants fictifs (un email, un pseudonyme, un numéro de téléphone), dessine à la main quelles relations tu chercherais à établir entre eux et avec quel niveau de confiance tu les pondérerais.

Corrigés disponibles sur demande — dis-moi si tu veux que je vérifie tes réponses. -e

---

OSINT Avancé — Approfondissement pour DOSSIER

Ce chapitre va plus loin sur la méthodologie OSINT, en lien direct avec un outil de type DOSSIER (recon automatisée + graphe).

---

1. Architecture d'une investigation automatisée

Un outil comme DOSSIER industrialise le cycle du renseignement (Direction → Collecte → Traitement → Analyse → Diffusion) en automatisant les étapes coûteuses en temps humain. Il est utile de penser la conception de l'outil selon ces couches :

Couche collecte — chaque module (Sherlock, Holehe, Maigret, theHarvester, crt.sh, dnstwist) répond à une question précise :

- Sherlock/Maigret : "ce pseudonyme existe-t-il sur quelles plateformes ?"
- Holehe : "cet email est-il associé à quels services ?"
- theHarvester : "quels emails/sous-domaines sont publiquement liés à ce domaine ?"
- crt.sh : "quels certificats/sous-domaines ont été émis pour ce domaine, y compris ceux jamais indexés ailleurs ?"
- dnstwist : "quels domaines visuellement proches existent (typosquatting, phishing potentiel) ?"

Couche normalisation — chaque module retourne un format différent ; la valeur ajoutée d'un outil comme DOSSIER est de normaliser ces résultats en entités communes (type : email/pseudo/domaine/IP, source, niveau de confiance, timestamp).

Couche corrélation — c'est la partie la plus difficile et la plus utile : relier automatiquement les entités entre elles (même email trouvé par deux modules différents, même pseudonyme réutilisé). Une architecture solide construit un graphe interne où chaque arête porte un poids de confiance basé sur la source.

Couche visualisation — le graphe force-directed rend lisible ce qui serait imbuvable en tableau brut, mais son utilité dépend entièrement de la qualité de la couche corrélation en amont.

2. Pondération de la confiance — un point souvent négligé

Tous les résultats OSINT ne se valent pas. Une architecture mature distingue au moins trois niveaux :

- **Confiance haute** : donnée confirmée par recoupement de plusieurs sources indépendantes (ex : même pseudo + même photo de profil + horaires d'activité cohérents).
- **Confiance moyenne** : donnée issue d'une seule source fiable mais non recoupée (ex : Holehe confirme un compte sur un service, sans autre corroboration).
- **Confiance faible** : correspondance possible mais avec un risque élevé de faux positif (ex : pseudonyme générique du type "john123", email formaté de façon standard).

Un graphe qui affiche tout au même niveau visuel induit en erreur l'analyste — un des axes d'amélioration les plus utiles pour un outil comme DOSSIER est de coder visuellement cette confiance (épaisseur de trait, couleur, opacité).

3. Réduction du bruit et faux positifs

Les outils de recon automatisée génèrent naturellement beaucoup de bruit :

- **Pseudonymes communs** : "shadow", "ghost", "admin" existent sur des centaines de plateformes sans aucun lien réel entre les comptes — un filtrage par popularité du pseudonyme (fréquence dans des bases publiques) aide à pondérer automatiquement la confiance.
- **Domaines parkés/génériques** : dnstwist retourne souvent des domaines enregistrés à des fins commerciales sans rapport avec du phishing — croiser avec l'âge du domaine et son historique DNS aide à trier.
- **Emails désactivés/anciens** : Holehe peut confirmer un compte créé il y a des années et jamais utilisé depuis — la fraîcheur de la donnée est un axe de pondération

important.

4. Extension méthodologique — au-delà des modules actuels

Pistes de modules complémentaires cohérentes avec l'orientation actuelle de l'outil :

- **Analyse de métadonnées de documents** : extraction EXIF/métadonnées Office des fichiers publiquement accessibles liés à une cible (auteur, logiciel, chemins internes).
- **Recherche de fuites structurée** : intégration de vérification de compromission (identifiants exposés dans des fuites connues), avec horodatage pour évaluer la fraîcheur du risque.
- **Analyse de réseau social passive** : cartographie des interactions publiques (mentions, réponses) pour repérer des relations non déclarées explicitement.
- **Module de géolocalisation d'image** : cohérent avec ton projet GeoCLIP + EasyOCR séparé — pourrait à terme s'intégrer comme un nœud supplémentaire du graphe (image → localisation estimée → recoupement avec d'autres indices géographiques).

5. Limites et angles morts à connaître

- **OSINT ne capture pas la donnée privée par design** — un individu avec une bonne hygiène numérique (pseudonymes cloisonnés, emails dédiés par service) sera naturellement peu corrélable, ce qui n'est pas un échec de l'outil mais une limite structurelle de la méthode.
- **Faux sentiment d'exhaustivité** — un graphe vide ou pauvre en connexions peut donner l'impression erronée qu'aucune information n'existe, alors que les sources interrogées sont simplement limitées en couverture.
- **Dérive vers la sur-interprétation** — plus un graphe est riche visuellement, plus il est tentant d'y voir des patterns qui relèvent en réalité du hasard (coïncidences statistiques sur des pseudonymes ou emails génériques). La rigueur analytique doit primer sur l'esthétique du graphe.

Exercice d'application

Imagine que DOSSIER retourne les résultats suivants pour une recherche sur un

pseudonyme donné :

- Sherlock : compte trouvé sur 12 plateformes, dont 3 avec la même photo de profil
- Holehe : email associé trouvé sur 2 services financiers
- crt.sh : aucun certificat associé à un nom de domaine personnel

Question : comment pondérerais-tu la confiance de chaque résultat, et dans quel ordre prioriserais-tu l'analyse manuelle si tu n'avais que 20 minutes ?

(Pas de corrigé unique ici — c'est un exercice de jugement analytique, dis-moi ton raisonnement si tu veux qu'on en discute.) -e

---

Corrigés commentés — Quiz Ingénierie Sociale & OSINT

Ne lis pas ça avant d'avoir essayé de répondre toi-même — sinon ça perd tout son intérêt pédagogique.

Quiz 1 — Fondations et psychologie

1. Les 7 principes de Cialdini + exemple d'exploitation

- *Réciprocité* : un faux technicien "résout" un petit problème avant de demander un mot de passe "pour vérifier".
- *Engagement/cohérence* : faire dire "oui" à une question anodine ("vous utilisez bien Office 365 ?") avant la vraie demande.
- *Preuve sociale* : "vos collègues du service X ont déjà validé cette procédure ce matin".
- *Sympathie* : l'attaquant mentionne un centre d'intérêt commun trouvé sur LinkedIn pour créer un rapport rapide.
- *Autorité* : usurpation d'un titre (DSI, agent des forces de l'ordre) ou ton assuré au téléphone.
- *Rareté/urgence* : "votre accès sera coupé dans 10 minutes si vous ne confirmez pas".

- *Unité* : “en tant que collègue du même service, je comprends votre charge de travail” — crée un faux sentiment d’appartenance.

2. Biais de confirmation vs effet de halo

Le biais de confirmation fait qu’on traite avec moins de suspicion un message qui correspond à une attente déjà présente (ex : un faux email de livraison alors qu’on attend justement un colis). L’effet de halo, lui, transfère une impression positive globale à partir d’un seul élément crédible (un logo officiel bien reproduit donne l’impression que tout le message est légitime, sans vérifier le reste).

3. Pourquoi les nouveaux employés sont plus vulnérables

Ils ne connaissent pas encore les procédures internes réelles, n’ont pas de repères pour détecter une anomalie (“est-ce normal qu’on me demande ça ?”), et craignent de mal faire ou de sembler incompétents en posant des questions ou en refusant une demande d’apparence légitime.

4. Cas RSA — principe exploité

Principalement la *curiosité* combinée à la *pertinence contextuelle* : le sujet “recrutement” est plausible dans n’importe quelle entreprise, suffisamment neutre pour ne pas éveiller la méfiance, mais suffisamment intéressant pour inciter à l’ouverture malgré le passage en spam.

Quiz 2 — Vecteurs d’attaque

5. Phishing / spear phishing / fraude au président

Le phishing de masse n’est pas personnalisé, compte sur le volume (taux de réussite faible mais rentable à grande échelle). Le spear phishing cible un individu précis avec des détails OSINT réels, ce qui supprime les signaux d’alerte habituels et augmente fortement le taux de réussite. La fraude au président pousse cette logique au maximum : usurpation d’une autorité hiérarchique réelle, combinée à l’urgence et la confidentialité, avec un enjeu financier direct — c’est la forme la plus ciblée et la plus rentable pour l’attaquant.

6. Pourquoi le vishing exploite mieux l’urgence

À l’écrit, la cible peut relire, faire une pause, consulter un collègue. Au téléphone, la réponse est attendue en temps réel, la voix humaine crée une pression sociale immédiate (silence gênant, difficulté à raccrocher), ce qui laisse beaucoup moins de place à la réflexion critique.

7. Exemple de pretexting en 4 étapes

1. Identité : “Bonjour, je suis Sophie du service RH, nouvelle sur le dossier mobilité.”
2. Justification : “Je finalise les dossiers de télétravail avant la clôture de fin de mois.”
3. Confiance progressive : “Vous êtes bien sur le projet X ? Parfait, ça correspond à ce que j’ai.”
4. Demande réelle : “Pour finaliser, j’ai juste besoin de votre identifiant employé et de la date de votre dernier accès VPN.”

8. Tailgating vs baiting

Le tailgating est purement physique (suivre quelqu’un dans un lieu sécurisé). Le baiting peut être physique (clé USB piégée laissée dans un parking) ou numérique (fausse offre de téléchargement), la caractéristique commune étant d’exploiter la curiosité ou la cupidité plutôt que l’urgence ou l’autorité.

Quiz 3 — OSINT et méthodologie

9. Cycle du renseignement

Direction (définir la question) → Collecte (rassembler les données brutes) → Traitement (nettoyer/structurer) → Analyse (croiser pour en tirer du sens) → Diffusion (restituer de façon actionnable). C’est un cycle, pas une ligne droite : l’analyse révèle souvent de nouvelles questions qui relancent une collecte ciblée.

10. Pourquoi la réutilisation de pseudo est un signal fort mais insuffisant

Un même pseudonyme sur deux plateformes peut être une coïncidence (pseudo générique/commun) ou appartenir à deux personnes différentes ayant eu la même idée. Il faut le corroborer par d’autres éléments (photo similaire, style d’écriture, horaires d’activité cohérents, centres d’intérêt recoupés) avant de le traiter comme une preuve de corrélation fiable.

11. Certificate Transparency Logs

Ce sont des registres publics où chaque certificat SSL émis est enregistré dès sa création, de façon irrévocable. Ils révèlent souvent des sous-domaines qui n’ont jamais été indexés par un moteur de recherche classique (environnements de test, de staging), car le certificat doit être émis même pour un usage interne ou temporaire.

12. Nœud à forte connectivité dans un graphe

Il indique généralement une identité pivot — l'élément (email, pseudonyme, numéro) qui relie plusieurs branches d'investigation entre elles. C'est souvent le point d'entrée le plus utile pour continuer l'investigation, mais aussi celui qui mérite le plus de vérification pour éviter les faux positifs (un email générique utilisé par erreur sur plusieurs comptes différents, par exemple).

Quiz 4 — Cadre légal et défense

13. Articles du Code pénal français

Article 226-4-1 (usurpation d'identité numérique) et article 323-1, issu de la loi Godfrain (accès ou maintien frauduleux dans un système de traitement automatisé de données).

14. Pourquoi la vérification par canal indépendant est la plus fiable

Parce qu'elle brise la chaîne de confiance construite par l'attaquant : si celui-ci contrôle l'email et le téléphone utilisés dans l'attaque, toute vérification effectuée via ces mêmes canaux reste piégée. Rappeler sur un numéro connu et vérifié indépendamment de la communication reçue est la seule méthode qui échappe systématiquement au contrôle de l'attaquant.

15. Culture du signalement sans blâme

Si un employé craint une sanction pour avoir cliqué sur un lien suspect ou pour avoir failli se faire piéger, il ne le signalera pas — et l'organisation perd une information précieuse pour réagir vite (bloquer l'accès compromis, alerter les autres services). Une culture non punitive maximise la remontée d'information, condition indispensable à une réaction rapide.

16. Limite entre OSINT professionnel et doxxing

La limite tient à trois éléments : le cadre légal (mandat, contrat, base légale RGPD), l'intention (protection/audit vs nuisance), et l'usage final des données (rapport confidentiel à un client vs publication publique visant à exposer ou harceler un individu). Les mêmes techniques peuvent être légitimes ou illégales selon ces trois critères — pas selon la technique elle-même.

Exercice 1 — Analyse du scénario "Julien du support"

(a) Vecteur : vishing (usurpation du support informatique).

(b) Principes exploités : autorité (support IT), urgence (15 minutes), et exploitation

directe d'un code de vérification à usage unique — c'est une tentative de contournement de l'authentification à deux facteurs, une des attaques les plus dangereuses actuellement car elle vise à intercepter le second facteur en temps réel.

(c) Ce que la victime aurait dû faire : ne jamais communiquer un code reçu par SMS à qui que ce soit, y compris un interlocuteur se présentant comme un collègue légitime — aucun service IT légitime ne demande ce code. Raccrocher et rappeler le support sur un numéro interne connu pour vérifier l'incident.

Comment tu t'en sors ? Si certaines réponses ne correspondent pas à ce que tu avais écrit, dis-moi lesquelles et on regarde pourquoi.