« Cyber Sécurité : Les outils selon ta couleur d'équipe »

Ce classement de solution regroupe les principales solutions utilisées en 2024. Certaines sont alternatives et d'autres complémentaires. Souvent, la combinaison de deux solutions dans un domaine permet de garantir une approche professionnelle mais surtout complète. Une solution de part ses fonctionnalités peut potentiellement figurer dans plusieurs sections. Dans la pratique, certaines solutions sont exploitables par les deux équipes. Le choix d'une solution dépend de la taille de l'entreprise, du budget, des compétences internes et des volumes à traiter.

RED TEAM

Reconnaissance et Collecte d'Informations

Pour collecter des informations sur vos cibles avant l'attaque.

OSINT (Open-Source Intelligence) :

- **Maltego** : Outil de cartographie pour visualiser les relations entre personnes, entreprises, domaines, et infrastructures, basé sur des données publiques et des recherches automatisées.
- **theHarvester** : Script de collecte d'informations OSINT permettant d'identifier des adresses e-mail, sous-domaines, et données associées à des cibles spécifiques.
- **Shodan** : Moteur de recherche spécialisé dans les appareils connectés (IoT, serveurs, caméras), permettant d'identifier les systèmes exposés à des vulnérabilités sur Internet.

Scanning et Cartographie Réseau :

- **Nmap** : Outil puissant de découverte réseau permettant d'identifier les hôtes actifs, de scanner les ports ouverts, et de détecter les services et versions des logiciels pour une cartographie détaillée des environnements cibles.
- **Amass** : Framework avancé pour la cartographie des sous-domaines, des adresses IP associées, et des relations DNS, essentiel pour révéler l'infrastructure externe d'une cible.
- **Masscan** : Scanner de ports ultra-rapide capable de balayer des réseaux à grande échelle en quelques minutes, idéal pour identifier rapidement les points d'entrée potentiels.

Scanning de Vulnérabilités

Pour identifier les failles avant exploitation.

- **Nessus :** Solution commerciale pour scanner les vulnérabilités et identifier les points faibles exploitables dans les réseaux et applications cibles.
- **OpenVAS :** Alternative open source idéale pour identifier rapidement des failles exploitables dans les environnements cibles.
- **Qualys :** Plateforme cloud pour cartographier les vulnérabilités à grande échelle, utilisée pour planifier les attaques sur des infrastructures complexes.

Exploitation de Failles

L'exploitation des vulnérabilités.

Exploitation :

- **Metasploit :** Framework polyvalent pour la découverte, l'exploitation de vulnérabilités, et la génération de payloads personnalisés.
- **Exploit Pack :** Framework léger pour exploiter des failles spécifiques, connues, ciblées à exploiter rapidement.
- **Core Impact** : Solution de tests d'intrusion offrant des fonctionnalités avancées pour simuler des attaques, exploiter des vulnérabilités, et valider la sécurité des réseaux, applications, Web, endpoints, etc.
- **Impacket** : Bibliothèque Python pour manipuler des protocoles réseau (e.g., SMB, LDAP).
- **Cobalt Strike :** Framework avancé permettant d'exploiter des vulnérabilités et de déployer des payloads personnalisés pour préparer la post-exploitation.

Exploitation Web et API :

- **Burp Suite Pro** : Outil avancé pour le test et l'exploitation des vulnérabilités web.
- **OWASP ZAP** : Alternative open source pour les tests de sécurité des applications web.

BLUE TEAM

Outils de Détection et de Surveillance

Ces outils aident à surveiller l'infrastructure pour détecter les activités suspectes.

SIEM (Security Information and Event Management) :
Collectent et analysent les journaux (logs) en temps réel pour identifier les anomalies.

- **Splunk** : Une solution complète pour l'analyse des données de sécurité.
- **IBM QRadar** : Intègre détection, analyse et réponse automatisée.
- **Elastic Stack (ELK)** : Open source, utilisé pour surveiller les logs et détecter les incidents.

EDR (Endpoint Detection and Response) :
Protègent les terminaux contre les menaces avancées et offrent des capacités de réponse rapide.

- **CrowdStrike Falcon** : Détection et réponse en temps réel.
- **Carbon Black** : Analyse comportementale des endpoints.
- **Microsoft Defender for Endpoint** : Solution intégrée pour les environnements Windows.
- **Tanium** : Plateforme de gestion et de sécurisation des terminaux, offrant une visibilité en temps réel, des capacités de détection des menaces et une réponse rapide.

NIDS/NIPS (Network Intrusion Detection/Prevention Systems) :
Détectent et préviennent les intrusions réseau.

- **Snort** : Open source pour l'analyse en profondeur des paquets.
- **Suricata** : Analyse réseau avec détection des menaces.
- **Darktrace :** Solution basée sur l'intelligence artificielle pour détecter et répondre aux menaces en analysant les anomalies comportementales dans les réseaux. Complémentaire à Splunk ou QRadar, qui se basent davantage sur la corrélation d'événements et les logs.

Outils de Gestion des Journaux et de la Corrélation

Ces outils permettent une meilleure analyse des événements de sécurité.

Gestion centralisée des logs :

- **Graylog** : Collecte et analyse les logs en temps réel.
- **Logstash** : Composant de la stack ELK pour traiter et analyser les logs.
- **Elastic Observability** : Plateforme open source pour centraliser et analyser logs, métriques et traces en temps réel.
- **Kibana** : Interface de visualisation pour Elastic Stack (ELK), permettant d'analyser et de corréler les logs en temps réel via des tableaux de bord interactifs et des visualisations avancées.

Monitoring et alertes :

- **Nagios** ou **Zabbix** : Outils de surveillance pour suivre les performances et détecter les anomalies.
- **Prometheus avec Grafana** : Surveillance avancée des métriques avec des visualisations détaillées.

Outils de Threat Intelligence (CTI)

Ils aident à comprendre les menaces émergentes et à réagir rapidement.

Renseignements sur les menaces :

- **Recorded Future** : Analyse des menaces en temps réel.
- **ThreatConnect** : Plateforme collaborative de threat intelligence.

- **Postman** : Pour tester et exploiter des failles dans les API.
- **SQLmap :** Automatisation des attaques par injection SQL pour tester la sécurité des bases de données.
- **Nikto :** Scanner open source de vulnérabilités pour serveurs web, détectant les configurations faibles et les modules obsolètes.
- **Wfuzz :** Outil de brute force pour trouver des fichiers cachés, paramètres ou ressources vulnérables sur les applications web.

Post-Exploitation et Persistance
Pour maintenir l'accès et escalader les privilèges après une compromission initiale.

Shells et Payloads :

- **Cobalt Strike** : Framework référence dans la post-exploitation. Conçu pour simuler des attaques complexes de type APT (Advanced Persistent Threat), en reproduisant les tactiques, techniques et procédures (TTP) des adversaires sophistiqués. Maintient d'accès, mouvements latéraux. Parfait après une exploitation via Exploit Pack.
- **Empire :** Plateforme de post-exploitation basée sur PowerShell et Python, spécialisée dans les environnements Windows. Utilisée pour automatiser les tâches de post-exploitation, maintenir l'accès, et effectuer des mouvements latéraux grâce à une bibliothèque modulaire de scripts.
- **Meterpreter (via Metasploit)** : Shell interactif puissant pour la post-exploitation.
- **Mimikatz** : Outil de post-exploitation spécialisé dans l'extraction des informations d'identification et la manipulation des mécanismes d'authentification Windows, comme Kerberos.

Élévation de privilèges :

- **WinPEAS / LinPEAS** : Scripts pour détecter les failles permettant l'escalade de privilèges sur Windows/Linux.
- **Impacket** : Scénario de complémentarité avec Cobalt Strike ou Empire pour extraire des identifiants (via secretsdump.py), ou exécuter des commandes à distance (via wmiexec.py).
- **PowerSploit** : Scripts PowerShell pour l'exploration et l'exploitation de systèmes Windows.
- **Atomic Red Team** : Ensemble de tests ciblés basés sur le cadre MITRE ATT&CK, utilisé pour simuler des tactiques post-exploitation et valider les défenses en place.

Automatisation et Orchestration
Pour gérer des campagnes d'attaques complexes.

- **Metta :** Plateforme d'automatisation RED TEAM, permettant de simuler des tactiques et techniques adverses dans des environnements contrôlés pour évaluer la résilience des systèmes.
- **Caldera :** Framework open source conçu pour simuler des attaques réalistes en utilisant les tactiques et techniques documentées dans le framework MITRE ATT&CK, afin de tester les défenses et détecter les vulnérabilités.
- **Pupy :** Plateforme modulaire et furtive de post-exploitation, écrite en Python, offrant des capacités avancées pour établir un contrôle persistant et exécuter des actions malveillantes sur des systèmes compromis.

Tests de Mots de Passe et Authentification
Pour forcer les systèmes mal protégés.

- **Hydra** : Attaques par force brute sur des services distants (SSH, FTP, HTTP, SMB, RDP, etc.), permettant de tester la robustesse des mots de passe.
- **Medusa** : Alternative rapide pour les attaques de mots de passe.
- **John the Ripper** : Outil polyvalent pour le craquage de mots de passe, compatible avec divers formats de hachage (MD5, SHA, bcrypt, etc.), utilisé pour évaluer la sécurité des mots de passe dans les environnements locaux.
- **Hashcat** : Craqueur de mots de passe ultra-performant exploitant la puissance des GPU, capable de traiter de grands volumes de hachages avec des algorithmes avancés pour des attaques rapides et efficaces. Idéal pour des algorithmes de hachage intensifs (bcrypt, SHA-512, Argon2, etc.).

- **Anomali** : Plateforme de threat intelligence qui collecte, analyse et corrèle des données de menaces pour détecter les indicateurs de compromission (IOC) et améliorer la réponse aux incidents. (Intégration Splunk ou QRadar)

Feeds de menaces :

- **Cyber Threat Alliance** : Organisation collaborative de partage d'informations sur les menaces, permettant à ses membres d'accéder à des renseignements approfondis pour mieux se défendre contre les cyberattaques.
- **AlienVault OTX** : Partage des indicateurs de compromission (IOC).
- **MISP (Malware Information Sharing Platform)** : Plateforme open source pour partager des informations sur les menaces.

Analyse des Paquets Réseau
Pour surveiller les flux réseau et identifier les comportements anormaux.

- **Wireshark** : Outil d'analyse réseau visuel permettant de capturer et d'analyser les paquets en temps réel pour détecter les anomalies, les failles de protocoles, ou les activités suspectes.
- **Zeek (anciennement Bro)** : Framework d'analyse des données réseau, offrant des capacités de scripting pour détecter automatiquement les comportements anormaux, les failles protocolaires, et les menaces persistantes.
- **Tcpdump** : Outil léger en ligne de commande pour capturer et filtrer les paquets réseau, idéal pour une analyse rapide ou en complément d'autres outils de sécurité..

Gestion des Vulnérabilités
Ces outils permettent d'identifier et de corriger les failles avant qu'elles ne soient exploitées.

- **Nessus** : Analyse de vulnérabilités pour réseaux, serveurs et applications.
- **OpenVAS** : Alternative open source pour le scanning des vulnérabilités.
- **Qualys** : Plateforme cloud pour la gestion des vulnérabilités.
- **InsightVM** : Si vous avez besoin d'une gestion des vulnérabilités **basée sur les risques** avec des capacités avancées de corrélation et une priorisation des correctifs grâce au scoring des menaces, c'est est une excellente option.
- **Tenable.io** : Si votre organisation a besoin de fonctionnalités étendues pour le cloud (intégration DevOps) ou une gestion continue à grande échelle, Tenable.io complète Nessus et offre une valeur ajoutée.
- **BeyondTrust Retina** : Solution de scanning des vulnérabilités et de conformité conçue pour les environnements fermés, idéale pour les secteurs hautement réglementés comme la défense, où la sécurité des infrastructures critiques est essentielle.

Analyse Forensique et Réponse aux Incidents
Pour investiguer les attaques et restaurer la sécurité.

- **Autopsy** : Analyse forensique des disques et récupération de données après une compromission.
- **Volatility** : Analyse des mémoires volatiles pour identifier les traces laissées par les malwares.
- **FTK (Forensic Toolkit)** : Suite d'investigation forensique pour examiner des systèmes compromis. Utile une fois les menaces neutralisées. Orienté vers les investigations détaillées, minutieuses voire judiciaire.
- **X-Ways Forensics** : Intervient après un incident pour analyser les supports compromis, retracer les événements, et collecter des preuves tout en offrant des fonctionnalités d'automatisation pour accélérer les enquêtes.
- **FireEye** : Solution intégrée pour la détection, la réponse aux incidents (IR) en temps réel et l'analyse forensique, avec un focus sur les menaces avancées APT. Conçu pour contenir et éradiquer les menaces. Threat Intelligence intégrée grâce à Mandiant. Fonctionnalités EDR/XDR, analyse, SOAR, CTI, IOC.
- **Alternatives crédibles :** selon infrastructure existante et budget : **CrowdStrike Falcon** ou **Cortex XDR de PALO ALTO**

Analyse de l'Infrastructure Interne
Pour cartographier les réseaux internes et identifier les failles.

- **BloodHound** : Analyse des relations et permissions dans les environnements Active Directory pour identifier les chemins d'escalade de privilèges.
- **Responder** : Capture et manipulation des requêtes réseau. Analyse réseau spécialisé dans l'exploitation des faiblesses des protocoles Windows (LLMNR, NBT-NS, NTLM) via des attaques MITM. Capture d'informations d'identification et manipulation des communications internes.
- **CrackMapExec** : Automatisation des attaques sur les environnements Windows (SMB, RDP, etc.).
- **Mimikatz** : Outil puissant pour examiner les mécanismes d'authentification Windows, récupérer des mots de passe en mémoire, et analyser les faiblesses des politiques de sécurité dans un environnement Active Directory.

Phishing et Ingénierie Sociale
Pour tester les failles humaines et les vulnérabilités des utilisateurs.

- **SET (Social-Engineer Toolkit)** : Framework pour réaliser des attaques d'ingénierie sociale (phishing, USB malveillants, etc.).
- **Gophish** : Plateforme pour gérer des campagnes de phishing.
- **Evilginx2** : Attaque de phishing avancée pour contourner l'authentification multi-facteurs (MFA).

Analyse des Paquets et des Protocoles
Pour comprendre les communications réseau et exploiter les vulnérabilités.

- **Wireshark** : Outil d'analyse réseau utilisé pour intercepter et analyser les paquets afin d'identifier des failles dans les protocoles, surveiller les communications, ou préparer des attaques ciblées comme le MITM.
- **Bettercap** : Outil polyvalent pour l'interception, l'analyse et la manipulation du trafic réseau via des attaques MITM. Idéal pour cibler des failles dans des environnements modernes (WiFi, Bluetooth, IoT).
- **Ettercap** : Framework d'attaque MITM pour exploiter les réseaux. (Environnements legacy)

Analyse des Fichiers Malveillants
Pour analyser ou créer des malwares adaptés aux tests.

- **Cuckoo Sandbox** : Outil d'analyse automatisée de malwares permettant d'exécuter des fichiers suspects dans un environnement isolé (sandbox) pour observer leur comportement sans risque pour le système hôte.
- **Any.Run** : Sandbox interactive en temps réel permettant d'examiner et de manipuler les fichiers malveillants pour une analyse approfondie, idéale pour comprendre les comportements dynamiques des menaces.
- **MSFVenom (Metasploit)** : Générateur polyvalent de payloads personnalisés, combinant création et encodage pour exploiter des vulnérabilités ou contourner les défenses des systèmes cibles.

Exploitation des Environnements Cloud
Pour tester les infrastructures cloud et conteneurs.

- **Pacu** : Exploitation des environnements AWS.
- **Kubesploit** : Outil pour exploiter des vulnérabilités Kubernetes.
- **ScoutSuite** : Analyse de sécurité des configurations cloud (AWS, GCP, Azure).

1. Automatisation et Orchestration (SOAR)
Pour automatiser la réponse aux incidents et orchestrer les outils de sécurité.

- **Cortex XSOAR** : Plateforme avancée d'orchestration et d'automatisation des processus de sécurité, intégrant des outils tiers pour centraliser les opérations, standardiser les réponses, et réduire les délais de traitement.
- **Splunk Phantom** : Solution SOAR puissante permettant d'automatiser les réponses aux incidents, orchestrer des actions sur plusieurs outils de sécurité, et créer des workflows personnalisés pour une gestion optimale des menaces.
- **TheHive** : Plateforme open source collaborative dédiée à la gestion des incidents, facilitant le triage, l'analyse, et la documentation des menaces grâce à une intégration avec des outils SIEM et CTI.
- **Swimlane** : Plateforme SOAR flexible offrant une personnalisation avancée des workflows pour automatiser la détection, la réponse aux incidents, et optimiser les processus de sécurité à l'échelle de l'entreprise.

Sandbox pour Analyser les Malwares
Pour examiner les fichiers suspects dans un environnement sécurisé.

- **Cuckoo Sandbox** : Open source pour l'analyse des malwares.
- **Any.Run** : Solution interactive de sandboxing.
- **Hybrid Analysis** : Plateforme en ligne pour analyser les fichiers suspects.
- **ReversingLabs** : Plateforme avancée d'analyse statique et de gestion des fichiers malveillants, permettant la détection des menaces à grande échelle et l'automatisation des workflows de sécurité. S'intègre facilement dans les pipelines DevOps. SIEM, SOAR.

1. Outils de Sécurité des Applications et des API
Pour protéger vos applications contre les vulnérabilités.

- **Burp Suite** : Suite d'outils complète pour analyser, tester, et sécuriser les applications web, permettant aux équipes de détecter les vulnérabilités telles que les injections SQL, les failles XSS, ou les mauvaises configurations, tout en automatisant les tests de sécurité.
- **OWASP ZAP** : Outil open source pour l'analyse des failles dans les applications. ZAP s'intègre dans les pipelines CI/CD.
- **Postman avec des tests de sécurité intégrés** : Pour sécuriser les API.
- **Fiddler** : Proxy débogueur pour analyser, inspecter et modifier les communications HTTP/HTTPS, utile pour détecter les vulnérabilités dans les interactions client-serveur.
- **SoapUI** : Outil de test avancé pour les API SOAP et REST, permettant de simuler des requêtes et d'automatiser des tests de sécurité pour détecter des vulnérabilités.

1. Cryptographie et Gestion des Clés
Pour protéger les données sensibles.

- **HashiCorp Vault** : Gestion des secrets et des clés.
- **Let's Encrypt** : Automatisation de la gestion des certificats SSL/TLS.
- **OpenSSL** : Utilitaire en ligne de commande pour la gestion des certificats et le chiffrement.