AYI NEDJIMI Consultants

Livre Blanc Détaillé : Guide Pratique Cybersecurite

Catégorie : Livres Blancs Lecture : 6 min Publié le : 07/12/2025 Auteur : Ayi NEDJIMI

Guide de pentest avancé pour les environnements Cloud. Explorez les vecteurs d Livre Blanc Détaillé : Pentest Cloud AWS, Azure & GCP. Expert en.

Livre Blanc

Pentest Cloud : Sécuriser vos Environnements AWS, Azure & GCP (Édition 2025)

Le Cloud offre une agilité majeur, mais introduit aussi de nouveaux références de sécurité. Une simple erreur de configuration peut exposer des téraoctets de données. Ce guide explore les approches de pentest spécifiques aux trois principaux fournisseurs : AWS, Azure et GCP. Guide de pentest avancé pour les environnements Cloud. Explorez les vecteurs d Livre Blanc Détaillé : Pentest Cloud AWS, Azure & GCP. Expert en. Ce guide technique sur livre blanc pentest cloud aws s'appuie sur des retours d'expérience terrain et des méthodologies éprouvées en environnement de production. Nous abordons notamment : pentest cloud : sécuriser vos environnements aws, azure & gcp (édition 2025), chapitre 1 : le modèle de responsabilité partagée et la configuration et chapitre 2 : pentest sur aws (amazon web services). Les professionnels y trouveront des recommandations actionnables, des commandes prêtes à l'emploi et des stratégies de mise en œuvre adaptées aux environnements d'entreprise.

Notre avis d'expert
Un livre blanc en cybersécurité n'a de valeur que s'il est actionnable. Les méthodologies théoriques sans exemples d'implémentation concrète restent lettre morte. Notre approche privilégie systématiquement les guides step-by-step validés en environnement de production.

Chapitre 1 : Le Modèle de Responsabilité Partagée et la Configuration

La règle d'or du Cloud est le **modèle de responsabilité partagée**. Le fournisseur (ex: AWS) est responsable de la sécurité *du* Cloud (hardware, infrastructure physique, hyperviseurs). Vous, le client, êtes responsable de la sécurité *dans* le Cloud (gestion des identités et des accès, configuration des services, sécurité des données, configuration réseau).

Cela signifie que la principale menace dans le Cloud n'est pas tant une vulnérabilité logicielle qu'une **erreur de configuration humaine**. Un pentest Cloud se concentre donc massivement sur l'identification de ces erreurs, une pratique souvent appelée CSPM (Cloud Security Posture Management), mais avec une approche offensive pour valider l'exploitabilité des failles.

Votre stratégie de cybersécurité repose-t-elle sur un référentiel méthodologique éprouvé ?

Chapitre 2 : Pentest sur AWS (Amazon Web Services)

La gestion des identités (IAM) : le cœur du réacteur

IAM (Identity and Access Management) est le service central d'AWS. Une mauvaise configuration ici est la porte d'entrée la plus courante. Un attaquant cherchera à : Pour approfondir, consultez Livre Blanc Détaillé :.

- **Obtenir des crédentiels :** Via une vulnérabilité de type Server-Side Request Forgery (SSRF) sur une application hébergée sur une instance EC2 pour atteindre le service de métadonnées (`169.254.169.254`) et voler le token du rôle IAM attaché. D'autres sources sont les clés d'accès (Access Key ID & Secret Access Key) laissées en clair dans du code sur GitHub, des variables d'environnement ou des fichiers de configuration.
- **Escalader les privilèges :** Une fois qu'il a des crédentiels, même peu privilégiés, il cherchera des permissions d'escalade. Il existe plus de 200 techniques documentées, les plus connues étant la possibilité de créer une nouvelle version d'une policy (`iam:CreatePolicyVersion`), de

passer un rôle à une nouvelle ressource (`iam:PassRole` sur un rôle privilégié), ou de mettre à jour la fonction d'un Lambda (`lambda:UpdateFunctionCode`). Des outils comme **Pacu** ou les recherches de **Rhino Security Labs** ont cartographié ces chemins.

Autres vecteurs d'attaque courants sur AWS

- **Buckets S3 publics :** Le classique. Un simple oubli dans la configuration d'un bucket ou de sa politique peut exposer des données sensibles au monde entier. L'audit doit vérifier à la fois les ACLs et les Bucket Policies.
- **Snapshots EBS publics :** Une copie de disque dur d'une instance EC2 peut contenir des secrets, des clés privées, du code source. Si elle est rendue publique, tout est exposé.
- **Groupes de sécurité trop permissifs :** Exposer des ports d'administration (SSH, RDP) ou des bases de données (PostgreSQL, MySQL) à tout Internet (`0.0.0.0/0`) est une invitation à des attaques de brute-force ou à l'exploitation de vulnérabilités 0-day.
- **Services managés mal configurés :** Des bases de données RDS avec des mots de passe par défaut, des files d'attente SQS lisibles publiquement, ou des Lambdas avec des rôles sur-privilégiés.

Vos configurations Cloud sont-elles à l'épreuve des balles ?
Un audit de configuration automatisé est un bon début, mais il ne suffit pas. Notre approche de pentest combine outils (Prowler, ScoutSuite) et expertise manuelle pour découvrir les chaînes d'attaque complexes que les scanners ignorent.

Planifier un pentest Cloud

Cas concret
Le framework MITRE ATT&CK, devenu le référentiel standard de l'industrie, a transformé la manière dont les organisations modélisent les menaces. Son adoption généralisée depuis 2020 a permis de structurer les échanges entre équipes offensives et défensives autour d'un langage commun et mesurable.

Chapitre 3 : Pentest sur Azure

Azure Active Directory (Microsoft Entra ID) : l'épine dorsale

L'écosystème Azure est profondément lié à Azure AD. Les attaques ciblent souvent :

- **Les principaux de service (Service Principals) :** L'équivalent des rôles IAM. Si un attaquant compromet un principal de service avec des droits "Contributor" ou "Owner" sur une souscription, il a gagné. Il peut exfiltrer des disques de VM, accéder à des Key Vaults, etc.
- **Le consentement aux applications OAuth (Illicit Consent Grant - T1528) :** Une attaque de phishing peut amener un utilisateur à consentir à une application malveillante qui demande des permissions étendues sur son compte (ex: `Mail.ReadWrite.All` , `Files.ReadWrite.All`). L'application de l'attaquant reçoit alors un token et peut agir au nom de l'utilisateur, même si ce dernier change son mot de passe.
- **Mots de passe faibles et absence de MFA :** Azure AD est une cible de choix pour les attaques de "password spraying".

Stockage et services PaaS

Les comptes de stockage Azure sont une cible majeure. Un conteneur de Blob Storage avec un accès anonyme public est l'équivalent d'un bucket S3 ouvert. De plus, les signatures d'accès partagé (SAS tokens) avec une durée de vie trop longue et des permissions trop larges (niveau compte plutôt que conteneur) sont un risque majeur si elles fuient. Pour approfondir, consultez Top 10 des Attaques.

Des services comme les App Services ou les Azure Functions peuvent être involontairement exposés sur Internet sans authentification adéquate, ou avec des secrets de connexion dans leurs paramètres d'application.

Chapitre 4 : Pentest sur GCP (Google Cloud Platform)

IAM et comptes de service

GCP a un modèle IAM similaire à AWS. Les comptes de service (Service Accounts) sont clés. Une attaque classique consiste à compromettre une instance GCE (Google Compute Engine) pour obtenir le token du compte de service qui lui est attaché via l'API de métadonnées. L'attaquant cherchera ensuite des permissions d'escalade, comme la capacité de se faire passer pour un autre compte de service (`iam.serviceAccounts.actAs`), qui est une permission extrêmement dangereuse.

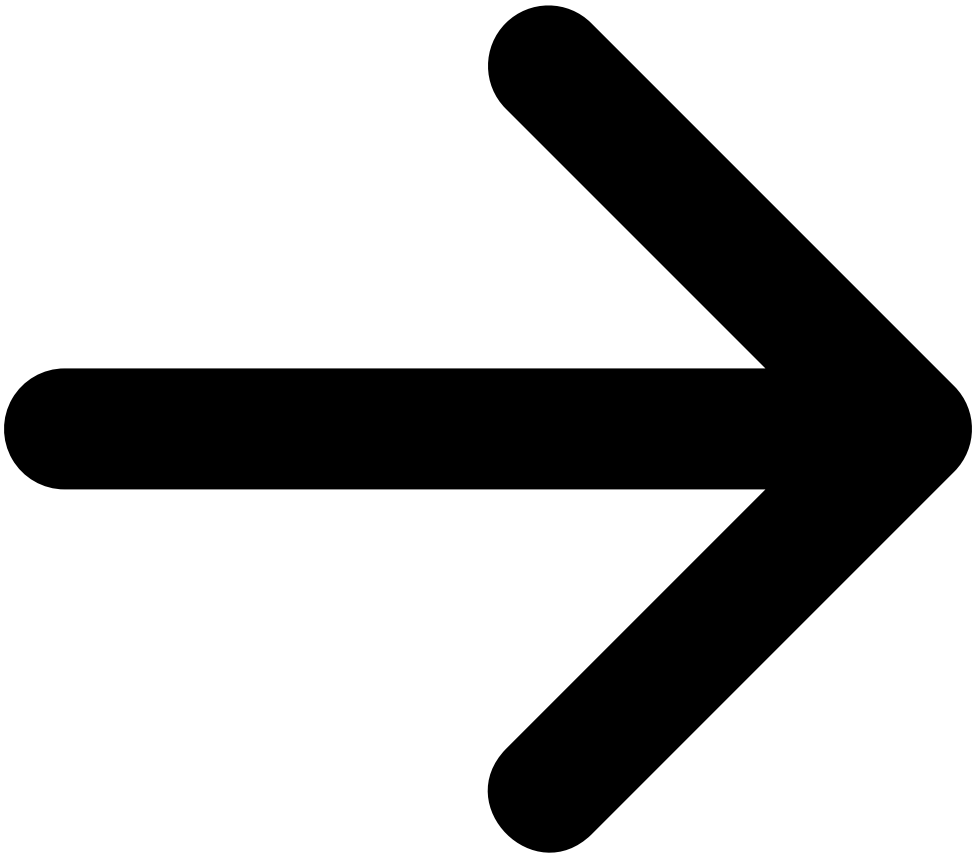
Exposition par défaut

Historiquement, certains services GCP avaient des configurations par défaut dangereuses. Par exemple, le réseau VPC par défaut autorisait tout le trafic interne. Bien que Google ait amélioré cela, les anciens environnements peuvent encore être vulnérables. Pour approfondir, consultez Evasion d'EDR/XDR : techniques.

De l'infrastructure aux applications

Maintenant que votre infrastructure Cloud est mieux comprise, voyons comment sécuriser les applications qui y tournent, avec Kubernetes.

Lire le livre blanc suivant : Sécurité Kubernetes



Ressources open source associées :

- cloud-security-fr — Dataset sécurité cloud AWS/Azure/GCP (HuggingFace)
- pentest-checklist-fr — Dataset méthodologie pentest (HuggingFace)

Questions frequentes

Comment ce sujet impacte-t-il la securite des organisations ?

Ce sujet a un impact significatif sur la securite des organisations car il touche aux fondamentaux de la protection des systemes d'information. Les entreprises doivent evaluer leur exposition, mettre en place des mesures preventives adaptees et former leurs equipes pour faire face aux risques associes a cette problematique. Pour approfondir, consultez OWASP Top 10 pour les LLM : Guide Remédiation 2026.

Quelles sont les bonnes pratiques recommandees par les experts ?

Les experts recommandent une approche basee sur les risques, incluant l'evaluation reguliere de la posture de securite, la mise en place de controles techniques et organisationnels, la formation continue des equipes et l'adoption des referentiels de securite reconnus comme ceux du NIST, de l'ANSSI et de l'OWASP.

Pourquoi est-il important de se former sur ce sujet en 2026 ?

En 2026, la maitrise de ce sujet est devenue incontournable face a l'evolution constante des menaces et des exigences reglementaires. Les professionnels de la cybersecurite doivent maintenir leurs competences a jour pour proteger efficacement les actifs numeriques de leur organisation et repondre aux obligations de conformite.

Conclusion

Cet article a couvert les aspects essentiels de Chapitre 1 : Le Modèle de Responsabilité Partagée et la Configuration, Chapitre 2 : Pentest sur AWS (Amazon Web Services), Chapitre 3 : Pentest sur Azure. La mise en pratique de ces recommandations permet de renforcer significativement la posture de securite de votre organisation.

Sources et références : ANSSI · CERT-FR

Outils et Ressources Pentest Cloud

Decouvrez nos outils open source et modeles d'IA developpes pour les professionnels de la cybersecurite :

Outil / Ressource	Description	Lien
AzureArcAgentChecker	Verificateur d''agents Azure Arc pour l''audit d''infrastructure hybride	Voir sur GitHub
TcpPortFuzzer	Fuzzer de ports TCP pour la decouverte de services cloud exposes	Voir sur GitHub
Bug Bounty Pentest Explorer	Explorateur interactif de techniques de pentest cloud	Voir sur HuggingFace
WFPFilterInspector	Inspecteur de filtres WFP pour l''analyse reseau avancee	Voir sur GitHub
Awesome Cybersecurity Tools	Collection d''outils pour le pentest et l''audit de securite	Voir sur GitHub

Tous ces outils sont disponibles en open source sur notre profil GitHub et nos modeles d'IA sur notre espace HuggingFace. N'hesitez pas a contribuer et a signaler les issues.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr