Build. Run. Secure.

Rapport de Test d’intrusion

ACME

Confidentiel

Date: 25 juillet 2025
Version 1.0

Index

Déclaration de Confidentialité

Ce document est la propriété exclusive de ACME et HATI. Il contient des informations confidentielles et propriétaires. Toute duplication, redistribution ou utilisation, en tout ou en partie, sous quelque forme que ce soit, nécessite le consentement de ACME et de HATI.

ACME peut partager ce document avec des auditeurs sous accords de confidentialité afin de démontrer la conformité aux exigences de tests d'intrusion.

Disclaimer

Un test d'intrusion représente une photographie à un instant donné. Les constats et recommandations reflètent les informations recueillies durant l'évaluation et ne prennent pas en compte les modifications ou changements survenus en dehors de cette période.

Les pentests limités dans le temps ne permettent pas une évaluation exhaustive. HATI a priorisé les tests afin d'identifier en premier lieu les vulnérabilités les plus critiques qu'un attaquant pourrait exploiter. HATI recommande de faire réaliser des évaluations similaires chaque année, par des services internes ou tiers.

Informations de Contact

Nom	Rôle	Contact
ACME		
John Doe	RSSI	Email: jdoe@acme.com
HATI		
Fabien GEORGE	Pentester	Email: contact.hati@proton.me

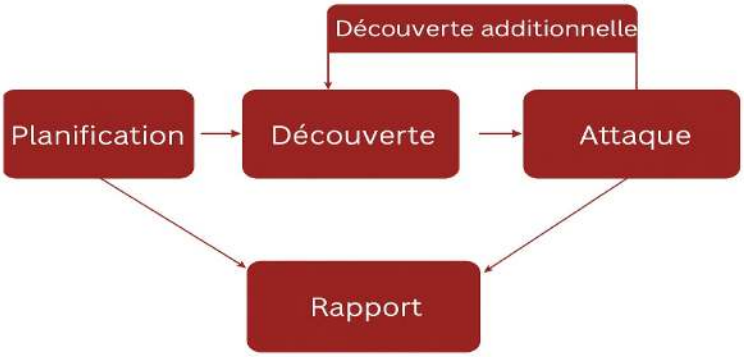
Présentation de l'Évaluation

Du 20 juillet 2025 au 25 juillet 2025, ACME a mandaté HATI pour évaluer la posture de sécurité de son système d'information. Cette mission comprenait un test d'intrusion sur le réseau interne.

L'évaluation s'appuie sur les méthodologies issues des bonnes pratiques internationales (NIST SP 800-115, OWASP Testing Guide v4) et des référentiels reconnus en France (ANSSI, ISO 27001), adaptées au contexte de la mission, ainsi que sur des méthodologies spécifiques à l'environnement client.

L'évaluation s'est déroulée en plusieurs phases :

- Planification : définition des objectifs du client et des règles d'engagement.
- Découverte : réalisation de scans et d'énumérations afin d'identifier les vulnérabilités potentielles, les failles de sécurité et les vecteurs d'attaque.
- Exploitation : validation des vulnérabilités identifiées par des tentatives d'exploitation, accompagnée de découvertes complémentaires suite à l'obtention d'accès.
- Restitution : rédaction d'un rapport détaillant les vulnérabilités exploitées, les tentatives échouées, ainsi qu'une analyse des points forts et faibles identifiés au sein de l'organisation.



Composantes de l'évaluation

Test d'intrusion interne

Le test d'intrusion interne consiste à simuler le rôle d'un attaquant ayant un accès initial au réseau interne. Le pentester effectue un scan du réseau afin d'identifier les vulnérabilités potentielles. Il réalise ensuite des attaques telles que : exploitation de vulnérabilités dans les partages réseau, capture et réutilisation d'identifiants, exploitation de faiblesses dans l'authentification Kerberos, élévation de privilèges via des vulnérabilités ou des configurations

erronées, exploitation de failles dans les politiques de groupe (GPO) ou dans les configurations Active Directory, et d'autres techniques. L'objectif est de savoir s'il est possible de progresser latéralement au sein du réseau, d'obtenir un accès aux postes et serveurs, de compromettre les comptes utilisateurs et administrateurs du domaine, ou d'exfiltrer des données sensibles.

Échelle de criticité des vulnérabilités

Le tableau ci-dessous définit les niveaux de criticité ainsi que les plages de scores CVSS v3 correspondantes, utilisées tout au long du rapport pour évaluer les vulnérabilités et leur impact.

Gravité	Score CVSS V3	Définition
Critique	9.0-10.0	Exploitation facile et généralement synonyme de compromission au niveau système. Il est recommandé d'établir un plan d'action et de corriger immédiatement.
Élevée	7.0-8.9	Exploitation plus complexe mais pouvant entraîner une élévation de privilèges, une perte de données ou une indisponibilité. Il est conseillé de planifier une correction rapide.
Moyenne	4.0-6.9	Vulnérabilités existantes mais difficiles à exploiter ou nécessitant des étapes supplémentaires (ex. ingénierie sociale). Correction à prévoir après les problèmes prioritaires.
Faible	0.1-3.9	Vulnérabilités non exploitables directement mais augmentant la surface d'attaque. Correction à planifier lors de la prochaine maintenance.
Informatif	N/A	Aucune vulnérabilité détectée. Informations complémentaires sur les contrôles efficaces ou observations faites pendant les tests.

Facteurs de risque

Le risque est évalué selon deux critères : la probabilité et l'impact.

Probabilité

La probabilité mesure la possibilité qu'une vulnérabilité soit exploitée. Cette évaluation tient compte de la difficulté de l'attaque, des outils disponibles, du niveau de compétence de l'attaquant, ainsi que du contexte environnemental du client.

Impact

L'impact mesure les conséquences potentielles de la vulnérabilité sur les opérations, incluant la confidentialité, l'intégrité et la disponibilité des systèmes et données, ainsi que les dommages réputationnels et pertes financières.

Périmètre

Évaluation	Détails
Test d'intrusion interne	10.x.x.x/8

Exclusions du périmètre

À la demande du client, HATI n'a pas réalisé les attaques suivantes pendant les tests :

- Attaques par déni de service (DoS)
- Phishing / Ingénierie sociale

Toutes les autres attaques non spécifiées ci-dessus ont été autorisées par ACME.

Autorisations du client

ACME a accordé à HATI les accès suivants :

- Accès au réseau interne via un VPN

Résumé exécutif

HATI a évalué la posture de sécurité interne de ACME au travers d'un test d'intrusion réalisé du 20 juillet 2025 au 25 juillet 2025. Les sections suivantes présentent un aperçu global des vulnérabilités identifiées, des tentatives d'exploitation réussies ou non, ainsi que des points forts et points faibles relevés.

Périmètre et contraintes temporelles

Le périmètre défini pour cette mission excluait les attaques de type déni de service (DoS) ainsi que les techniques d'ingénierie sociale sur l'ensemble des composantes testées.

Des contraintes de temps ont été appliquées : le test d'intrusion du réseau interne a été autorisé pour une durée de 5 jours ouvrés.

Synthèse des tests

L'évaluation a porté sur la posture de sécurité du réseau interne de ACME. Du point de vue interne, HATI a réalisé un scan de vulnérabilités sur l'ensemble des adresses IP fournies par ACME afin d'évaluer le niveau de risque global du parc. HATI a également mené des attaques courantes ciblant Active Directory, et évalué d'autres risques potentiels, comme les partages de fichiers ouverts, les identifiants par défaut sur serveurs et équipements, ainsi que les fuites d'informations sensibles.

L'équipe HATI a découvert que le protocole LLMNR était activé sur le réseau (Vulnérabilité SEC-001), ce qui a permis l'interception des hashs utilisateurs via un empoisonnement LLMNR. Ces hashs ont été extraits et craqués hors ligne par attaque par dictionnaire. En utilisant les mots de passe ainsi récupérés, l'équipe a pu accéder à plusieurs machines, indiquant des comptes utilisateurs trop permissifs.

Grâce à ces accès, il a été possible d'extraire les hashs des comptes locaux sur chaque machine compromise. L'équipe a constaté que ces hashs locaux étaient réutilisés sur plusieurs équipements (Vulnérabilité SEC-002), ce qui a permis d'accéder à d'autres machines via des attaques pass-the-hash.

Finalement, HATI a pu utiliser les comptes récupérés pour se déplacer latéralement dans le réseau, jusqu'à atteindre une machine disposant d'un identifiant administrateur de domaine. HATI a pu utiliser ces identifiants pour se connecter au contrôleur de domaine et compromettre l'ensemble du domaine.

Les autres vulnérabilités identifiées sont de niveaux élevés, moyens, faibles ou informationnels. Pour plus de détails, veuillez consulter la section « Résultats techniques ».

Notes et Recommandations

Les résultats de l'évaluation du réseau de ACME sont caractéristiques d'une organisation réalisant son premier test d'intrusion, ce qui est le cas ici. De nombreuses vulnérabilités identifiées concernent Active Directory et proviennent de configurations activées par défaut, telles que LLMNR et le Kerberoasting.

Au cours des tests, deux faiblesses majeures ont été constatées : une politique de mot de passe faible et une gestion des correctifs insuffisante. La faiblesse de la politique de mot de passe a conduit à la compromission initiale des comptes, ce qui représente généralement l'un des premiers points d'entrée qu'un attaquant cherche à exploiter sur un réseau. Cette faiblesse est confirmée par le fait que HATI a réussi à craquer plus de 10 mots de passe de comptes utilisateurs, incluant des comptes administrateurs de domaine, à l'aide d'attaques par dictionnaire simples.

Nous recommandons à ACME de réévaluer sa politique actuelle de mots de passe, et d'envisager l'application de mots de passe d'au moins 15 caractères pour les comptes utilisateurs standards et de 30 caractères minimum pour les comptes administrateurs de domaine. Il est également conseillé d'étudier la mise en place de mécanismes de blacklisting de mots de passe. Une liste des mots de passe craqués sera fournie à l'équipe afin d'aider à l'analyse. Enfin, la mise en place d'une solution de gestion des accès à privilèges (PAM) est également recommandée.

La gestion insuffisante des correctifs et la présence de systèmes d'exploitation obsolètes ont conduit à la compromission de plusieurs dizaines de machines au sein du réseau. Nous pensons que ce nombre aurait pu être bien plus élevé, cependant, les équipes HATI et ACME ont convenu qu'il n'était pas nécessaire de tenter l'exploitation de vulnérabilités d'exécution de code à distance (RCE), le contrôleur de domaine ayant déjà été compromis. Cette décision visait à limiter les risques de déni de service liés à des attaques non contrôlées.

Nous recommandons à l'équipe ACME de revoir attentivement les recommandations de correction listées dans la section « Résultats techniques » du rapport, ainsi que d'analyser les rapports de scan Nessus fournis pour obtenir une vue complète des éléments à corriger. Il est également conseillé d'améliorer les politiques et procédures de gestion des correctifs afin de réduire les risques d'attaques internes.

Concernant les aspects positifs, HATI a déclenché plusieurs alertes de sécurité au cours de la mission. L'équipe SOC de ACME a identifié notre activité de scan de vulnérabilités et a réagi à certaines attaques bruyantes menées sur une machine compromise. Bien que toutes les attaques n'aient pas été détectées, ces réactions sont un signe encourageant. Des recommandations complémentaires sur la détection et l'alerte ont été fournies, lorsque nécessaire, dans la section « Résultats techniques ».

Dans l'ensemble, le réseau de ACME a présenté un niveau de sécurité conforme à ce qui est attendu lors d'un premier test d'intrusion. Nous recommandons à l'équipe ACME d'examiner attentivement les recommandations de ce rapport, de corriger les vulnérabilités identifiées, et

de planifier un nouveau test d'intrusion annuel afin d'améliorer progressivement leur posture de sécurité interne.

Forces et faiblesses

Les points forts suivants ont été identifiés lors de l'évaluation :

1. Détection des scans effectués par des outils d'énumération courants (Nessus)
2. Détection de l'outil Mimikatz sur certaines machines
3. Les comptes de service n'étaient pas exécutés avec des privilèges d'administrateur de domaine
4. Le mot de passe du compte administrateur local était unique pour chaque machine

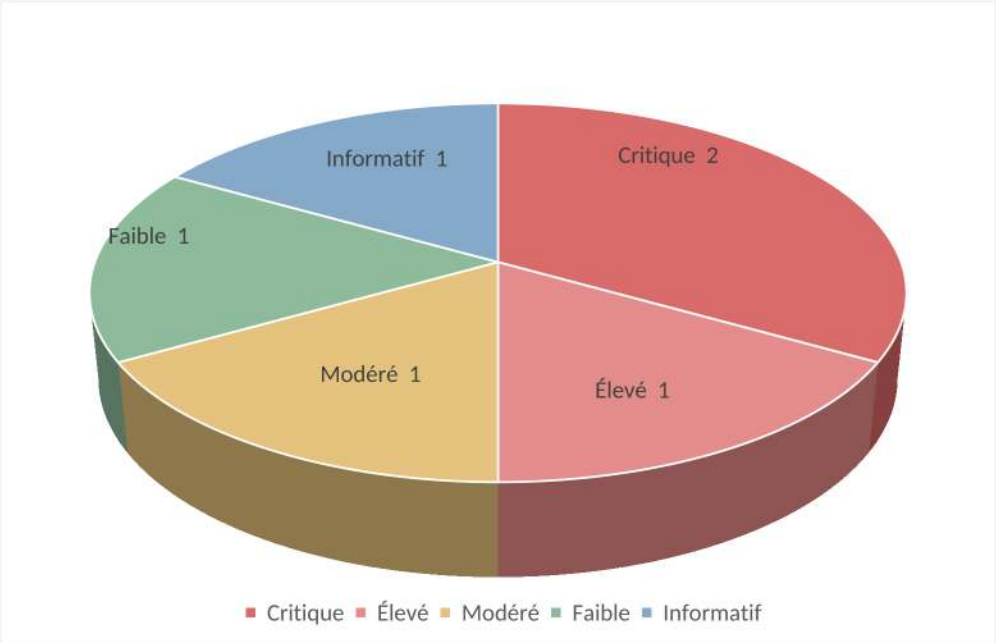
Les points faibles suivants ont été identifiés lors de l'évaluation :

1. Politique de mots de passe insuffisante
2. Systèmes d'exploitation obsolètes et gestion des correctifs défaillante
3. Fonctionnalité LLMNR activée sur le réseau
4. Signature SMB désactivée sur l'ensemble des postes non-serveurs
5. Réutilisation des mots de passe sur les comptes administrateurs locaux et privilèges excessifs
6. Identifiants par défaut découverts sur des équipements critiques
7. Partages réseau accessibles sans authentification
8. Utilisation de comptes utilisateurs standards comme comptes de service
9. Comptes de service protégés par des mots de passe faibles
10. Comptes administrateurs de domaine utilisant des mots de passe faibles

Synthèse des vulnérabilités

Les éléments ci-dessous présentent les vulnérabilités identifiées classées par niveau d'impact, ainsi que les recommandations associées.

Résultats – Test d'intrusion interne



Vulnérabilité / Chemin d'attaque	Gravité	Recommandation
Test d'intrusion interne		
SEC-001 : Configuration insuffisante de LLMNR	Critique	Désactiver la résolution de noms multicast via une GPO.
SEC-002 : Mauvaise configuration – Réutilisation des mots de passe administrateurs locaux	Critique	Utiliser des mots de passe uniques pour les comptes administrateurs locaux et limiter les privilèges via le principe du moindre privilège.
SEC-003 : Gestion insuffisante des comptes privilégiés – Kerberoasting	Élevé	Utiliser des comptes de service gérés par groupe (GMSA) pour les services privilégiés.
SEC-004 : Accès non authentifié aux partages SMB	Modéré	Désactiver le partage SMB ou imposer une authentification.
SEC-005 : Absence de bannière légale d'avertissement	Faible	Mettre en place une bannière légale d'avertissement sur toutes les interfaces d'accès (SSH, portails web internes, etc.).

Vulnérabilité / Chemin d'attaque	Gravité	Recommandation
SEC-006 : Cheminement vers la compromission du compte Domain Admin	Informatif	Analyser les actions menant à la compromission et mettre en œuvre les mesures correctives recommandées.

Résultats Techniques

Résultats – Test d'intrusion interne

SEC-001 : Configuration insuffisante de LLMNR (Critique)

Description	ACME autorise la résolution de noms multicast (LLMNR) sur les réseaux des utilisateurs finaux. HATI a intercepté 20 empreintes de mots de passe (hashes) de comptes utilisateurs en réalisant une attaque par empoisonnement du trafic LLMNR, et a réussi à en déchiffrer 2 à l'aide d'outils de cassage de mots de passe standards. Les comptes compromis ont ensuite été utilisés pour obtenir des accès supplémentaires, menant à la compromission du contrôleur de domaine.
Risque	Vraisemblance : Élevée – Cette attaque est très efficace dans des environnements où la résolution de noms multicast est autorisée. Impact : Très Élevé – L'empoisonnement LLMNR permet à un attaquant d'intercepter des empreintes de mots de passe afin de les déchiffrer hors-ligne ou de les relayer en temps réel, facilitant ainsi la progression latérale dans le système d'information.
Système concerné	Tous
Outils utilisés	Responder, Hashcat
Références	• Stern Security - Local Network Attacks: LLMNR and NBT-NS Poisoning • NIST SP800-53 r4 IA-3 – Identification et authentification des dispositifs • NIST SP800-53 r4 CM-6(1) – Paramètres de configuration

Preuve

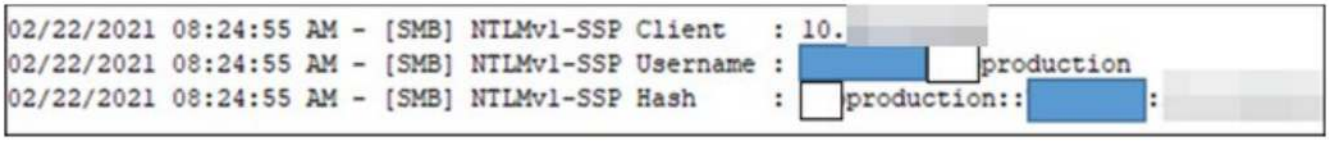


Figure 1 : Empreinte de mot de passe capturée pour le compte "production"

Figure 2 : Empreinte de mot de passe déchiffrée pour le compte "production"

Recommandations

- Désactiver la résolution de noms multicast (LLMNR) via une stratégie de groupe (GPO).
- Pour une atténuation complète et des recommandations de détection, consulter les directives MITRE correspondantes.
- Les empreintes de mots de passe déchiffrées mettent en évidence une politique de complexité des mots de passe insuffisante. Si la résolution de noms multicast ne peut être désactivée, il est fortement recommandé d'implémenter une solution de contrôle d'accès réseau (NAC) combinée à une liste blanche d'applications pour limiter la portée de ce type d'attaques.

SEC-002 : Mauvaise configuration de sécurité – Réutilisation des mots de passe des comptes administrateurs locaux (Critique)

Description	HATI a exploité des empreintes de mots de passe (hashes) d'administrateurs locaux pour accéder à d'autres machines du réseau via une attaque de type pass-the-hash. Ces empreintes ont été récupérées à partir des accès obtenus grâce au compte compromis mentionné dans la vulnérabilité SEC-001. Les attaques pass-the-hash permettent de s'authentifier sur une machine sans connaître le mot de passe associé, simplement en utilisant la hash. Ainsi, la réutilisation du même mot de passe administrateur local (et donc du même hash) sur plusieurs postes rend ces systèmes vulnérables à des compromissions en cascade. En s'appuyant sur cette technique, HATI a réussi à compromettre environ 50 machines au sein du siège social. Cette compromission a permis d'escalader les privilèges et d'accéder à d'autres comptes, menant à la compromission complète du contrôleur de domaine.
Risque	Vraisemblance : Élevée – Cette attaque est particulièrement efficace dans les environnements où les mots de passe administrateurs locaux sont réutilisés sur plusieurs machines. Impact : Très Élevé – L'exploitation de cette faille permet à un attaquant de progresser latéralement et verticalement au sein du réseau, jusqu'à la compromission du domaine.
Système concerné	Tous
Outils utilisés	Impacket, Netexec
Références	• MITRE CAPEC-644 – Pass-the-Hash Attack • Pentest Tales – TCM Security

Preuve

Figure 3 : Hash du compte administrateur local utilisé pour accéder à la machine

Recommandations

- Mettre en place des mots de passe uniques pour chaque compte administrateur local sur les machines.
- Appliquer rigoureusement le principe du moindre privilège pour limiter les utilisateurs administrateurs locaux.
- Considérer la mise en œuvre d'une solution de gestion des accès à privilèges (PAM – Privileged Access Management).
- Pour des recommandations détaillées concernant la remédiation et la détection, se référer aux directives MITRE associées.

SEC-003 : Gestion insuffisante des comptes à privilèges – Kerberoasting (Critique)

Description	HATI a récupéré l'ensemble des noms principaux de service (SPN) des utilisateurs depuis le contrôleur de domaine de ACME en utilisant un compte utilisateur standard (SEC-001) dans le cadre d'une attaque de type Kerberoasting. Cette extraction des SPN a permis à HATI de casser les mots de passe de 4 comptes. Aucun compte de service ne s'est avéré fonctionner avec des privilèges d'administrateur de domaine. Cependant, certains comptes utilisateurs ont été observés en tant que services, ce qui constitue une mauvaise pratique.
Risque	Probabilité : Élevée – Tout compte joint au domaine est en mesure de requêter les SPN des utilisateurs. Impact : Élevé – L'exploitation des SPN permet d'obtenir les empreintes des mots de passe des comptes sensibles et de les casser hors-ligne.
Système concerné	Tous
Outils utilisés	Impacket, Hashcat
Références	• Détails sur le Kerberoasting : https://adsecurity.org/?p=2293 • Group Managed Service Accounts Overview

Preuve

Account	Location	Password
[redacted]	[redacted]	[redacted]
	$MSSQLSvc/	
	$MSSQLSvc/	
adfs	$host/adfs	
sqladmin	$MSSQLSvc/UKSQL01	

Figure 14: Comptes de service crackés

Recommandations

- Utiliser des Group Managed Service Accounts (GMSA) pour les services à privilèges. Ces comptes permettent de garantir des mots de passe longs, complexes et renouvelés automatiquement à intervalles réguliers.
- Lorsque l'utilisation de GMSA n'est pas possible, protéger les comptes sensibles à l'aide d'une solution de coffre-fort de mots de passe (Password Vaulting).
- TCMS recommande également de configurer une journalisation d'alerte sur les contrôleurs de domaine, en surveillant les événements Windows Event ID 4769 lors de la demande de tickets de service Kerberos.
  Bien que ce type d'alerte puisse générer de nombreux faux positifs, il constitue une mesure de détection supplémentaire.
- Adapter les règles de votre solution de SIEM (Security Information and Event Management) afin de générer des alertes sur des volumes anormaux de requêtes SPN par un utilisateur.

SEC-004 : Accès non authentifié à des partages SMB (Modéré)

Description	ACME expose plusieurs serveurs avec des partages de fichiers accessibles sans authentification.
Risque	Probabilité : Modérée – Un attaquant peut découvrir ces partages à l'aide de techniques de reconnaissance basiques et discrètes. Impact : Modéré – Ces partages peuvent entraîner des fuites d'informations permettant à un attaquant d'obtenir des renseignements sur l'environnement interne.
Système concerné	10.x.x.x
Outils utilisés	Nessus, smbclient
Références	• NIST SP800-53r4 AC-6(3) – Principe du moindre privilège • NIST SP800-53r4 SC-4 – Contrôle des informations dans les ressources partagées

Preuve

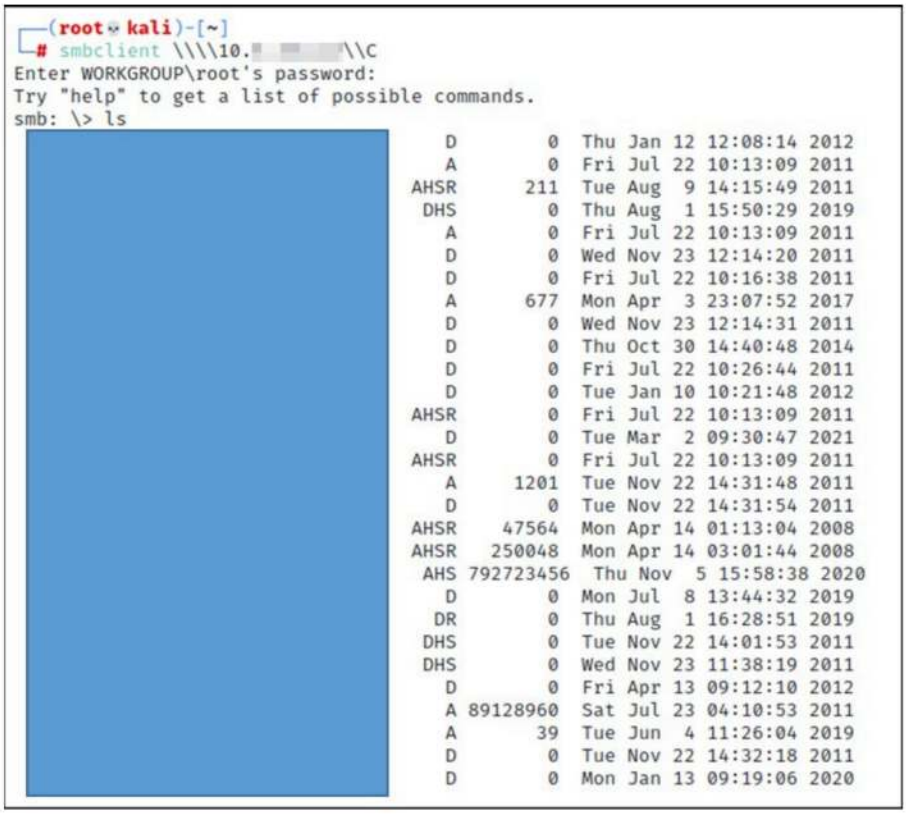


Figure 19 : Accès non authentifié à un partage

Recommandations

- Désactiver le partage SMB si celui-ci n'est pas nécessaire, ou bien configurer le partage pour exiger une authentification.
- L'activation de l'authentification protégera la confidentialité des données stockées sur ces partages.
- Il est également recommandé d'exporter les journaux d'authentification vers une solution SIEM, afin de permettre aux équipes de réponse à incident de détecter et analyser d'éventuelles tentatives de connexion par force brute.

SEC-005 : Absence de bannière légale d'avertissement (Faible)

Description	Les systèmes d'ACME n'affichent pas de bannière légale d'avertissement lors des connexions via les interfaces SSH et les portails web internes. Ce type de message permet de notifier aux utilisateurs (légitimes ou non) que l'accès au système est restreint et surveillé, et que toute tentative d'accès non autorisée est interdite. L'absence de bannière ne constitue pas en soi une vulnérabilité technique, mais peut compliquer la prise de mesures légales en cas d'intrusion, notamment pour démontrer la notion d'accès non autorisé.
Risque	Vraisemblance : Faible – L'absence de bannière n'est pas en soi un vecteur d'attaque, mais peut avoir des implications en cas d'incident. Impact : Faible – L'impact est principalement juridique et réputationnel. Il s'agit d'une non-conformité par rapport aux bonnes pratiques de sécurité et recommandations réglementaires.
Système concerné	• Serveurs SSH internes • Portails web internes (intranet, admin interfaces)
Outils utilisés	Netcat (nc) pour test de bannière SSH
Références	• ANSSI – Guide des bonnes pratiques d'hygiène informatique (PRIS 13) • NIST SP800-53 r4 AC-8 – System Use Notification • CIS Controls v8 – Control 16.12 (Legal Banner)

Preuve

```
$ nc server.acme.local 22
SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.9
```

Figure 1 : Connexion SSH sans bannière d'avertissement

Recommandations

- Mettre en place une bannière légale d'avertissement sur toutes les interfaces d'accès (SSH, portails web internes, etc.).
- S'assurer que la bannière précise clairement les conditions d'accès et les conséquences juridiques en cas d'accès non autorisé.
- Vérifier la bonne prise en compte de la bannière lors des connexions pour garantir sa visibilité avant toute authentification.
- Pour des recommandations détaillées concernant la mise en œuvre et la conformité, se référer aux guides ANSSI et NIST SP800-53 AC-8.

SEC-006 : Chemin vers l'accès Administrateur du Domaine (Informatif)

Les étapes ci-dessous décrivent comment HATI a obtenu un accès Administrateur du Domaine. Chaque étape est accompagnée de recommandations pour réduire les risques associés.

Étape	Action	Recommandation
1	Empoisonnement des réponses LLMNR afin d'obtenir le hash NetNTLMv2 d'un utilisateur réseau standard	Désactiver la résolution de noms multicast (LLMNR) via une stratégie de groupe (GPO).
2	Cassage hors-ligne des hashs NTLM des comptes administrateurs 'production' et 'john.doe'	Renforcer la complexité des mots de passe. Activer l'authentification multi-facteur (MFA). Mettre en place une solution de gestion des comptes à privilèges (PAM). Utiliser un filtre de mots de passe.
3	Utilisation du mot de passe du compte 'production' pour accéder à plusieurs machines du réseau	Restreindre les privilèges d'administrateur local et appliquer le principe du moindre privilège.
4	Extraction des hashs sur les machines compromises pour récupérer le mot de passe en clair du compte 'Bartender'	Renforcer la complexité des mots de passe.
5	Les droits excessifs du compte 'Bartender' permettent l'accès à un grand nombre de machines sur le réseau	Restreindre les privilèges d'administrateur local et appliquer le principe du moindre privilège.
6	Extraction des hashs sur les machines compromises pour récupérer le mot de passe en clair d'un compte Administrateur du Domaine	Renforcer la complexité des mots de passe.
7	Utilisation des identifiants découverts pour se connecter au contrôleur de domaine	

Recommandations

Examiner en détail les actions et recommandations listées ci-dessus.

Scans et Rapports Supplémentaires

HATI fournit à tous ses clients l'intégralité des données collectées durant les tests. Cela inclut les fichiers Nessus ainsi que les résultats complets des scans de vulnérabilités dans des formats détaillés. Ces rapports contiennent les résultats bruts des analyses ainsi que des vulnérabilités supplémentaires qui n'ont pas été exploitées.

Ces rapports permettent d'identifier des problématiques d'hygiène de sécurité qui nécessitent une attention particulière, bien qu'elles soient moins susceptibles de conduire directement à une compromission. Ils représentent néanmoins des opportunités d'amélioration.

Confidentiel - Fin du rapport