Fadi ALOUANI

BTS SIO 1
groupe 1
B3
20/11/25

Exercice d'application

Sommaire

Introduction

Dans ce TP, nous avons étudié comment protéger l’identité numérique d’une entreprise et comment un empoisonnement DNS peut détourner les utilisateurs vers un faux site. Nous avons également vu comment mettre en place une signature électronique fiable. L’objectif était de comprendre les risques et d’apprendre les solutions techniques pour sécuriser les services.

Fadi ALOUANI

Protéger l'identité numérique contre l’empoisonnement du serveur DNS

1)Retrouver la composante de l’identité numérique visée par la cyberattaque de Tradec

La cyberattaque vise l’identité des services en ligne de Tradec, plus précisément :
l’identité du serveur DNS et l’authenticité des adresses IP associées aux services de Tradec.
L’objectif de l’attaquant est de tromper les utilisateurs en leur faisant croire qu’ils accèdent aux services de Tradec alors qu’ils sont redirigés vers un faux serveur.
Donc :La composante visée : l’identité technique de Tradec (serveur DNS / résolution de nom).

2)Décrivez brièvement chaque étape de la cyberattaque contre Tradec

Étape 1 – Observation et préparation
Un laboratoire détecte une attaque suspecte ciblant un site Web commercialisé par Tradec.
L’attaquant tente d’empoisonner le serveur DNS afin de détourner les clients vers un faux site hébergé en Belgique.

Étape 2 – Compromission du DNS
L’attaquant envoie au serveur DNS compromis une fausse entrée de résolution qui associe le nom www.tradec.com à une adresse IP frauduleuse.

Étape 3 – Redirection des utilisateurs
Les utilisateurs accèdent au faux site Web sans s’en rendre compte.
Ce faux site recueille des informations sensibles (ex. identifiants et mots de passe).

Étape 4 – Exploitation des données volées
L’attaquant récupère les informations afin de potentiellement usurper des comptes ou nuire à Tradec.

Fadi ALOUANI

Simuler un empoisonnement DNS

2 Régler l'adresse IP du poste du salarié

D'après l'annexe 2 :
Adresse IP : 192.168.1.10
Passerelle : 192.168.1.254
DNS légitime : 192.168.1.250

3 Vérifier que le poste accède normalement au serveur DNS

Depuis le poste :

- ping 192.168.1.250
- nslookup tradec.com 192.168.1.250
  ? La résolution doit renvoyer l'adresse IP du vrai serveur Web Tradec : 172.16.1.2.

4 Simuler l'empoisonnement DNS

L'attaquant insère dans son serveur DNS pirate une fausse entrée :

- tradec.com → 172.16.1.200 (faux serveur)

Puis il détourne le client en modifiant son DNS :
DNS piraté : 172.16.1.254
Conséquence : les requêtes nslookup tradec.com donnent maintenant 172.16.1.200 → faux site.

5 Rédiger les synthèses des tests réalisé depuis le poste du salarié

Test	Résultat attendu	Interprétation
Ping vrai site	Réponse correcte	Le site réel est accessible
Ping faux site	Réponse incorrecte ou différente	Le pirate a un serveur actif
Nslookup avant attaque	172.16.1.2	Résolution normale
Nslookup après attaque	172.16.1.200	DNS empoisonné

6 Expliquez comment sécuriser le DNS dans l'entreprise

Mesures à mettre en place :
Utiliser DNSSEC pour signer les enregistrements DNS
Restreindre l'accès aux serveurs DNS internes
Filtrer les mises à jour DNS
Surveiller les logs DNS
Utiliser des serveurs redondants et sécurisés
Bloquer les DNS externes non autorisés

Fadi ALOUANI

Déployer la signature électronique comme moyen de preuve

1) Sous quelles conditions la signature électronique est recevable ?

La signature est recevable si :
Elle repose sur un certificat électronique reconnu
L'identité du signataire est clairement vérifiable
Le signataire a accepté explicitement l'acte
L'intégrité du document est garantie (non modifié)
La solution respecte le règlement eIDAS

2) Rôle de la signature électronique et comment la vérifier

Rôle :
Garantir l'identité du signataire
Assurer l'intégrité du document
Assurer la non-répudiation (le signataire ne peut nier)
Vérification :

- Contrôle du certificat émis par l'autorité de confiance
- Vérification de la clé publique
- Vérification de l'empreinte du document
- Lecture du cachet numérique indiquant le statut de validité

3) Avantages pour Fortunee et pour les clients

Pour Fortunee (la banque) :

- Gain de temps et réduction des coûts
  Suppression du papier
  Traçabilité complète
  Réduction des litiges
  Amélioration de l'image moderne et sécurisée

Pour les clients :

- Signature à distance
  Simplicité et rapidité
  Plus sûr qu'une signature manuscrite
  Consultation et stockage faciles des documents

4) Risques rencontrés par la banque lors de la signature :

- Certificat expiré ou invalide
- Utilisation frauduleuse du certificat (vol d'identité numérique)
- Mauvaise conservation des données
- Défaut de conformité eIDAS
- Infection d'un poste client au moment de la signature
- Litiges si le client nie son consentement

Conclusion

Ce TP m’a permis de comprendre le fonctionnement d’une attaque DNS et les moyens de s’en protéger, ainsi que l’utilité de la signature électronique pour garantir l’identité et l’intégrité d’un document. J’ai pu mettre en pratique ces notions et mieux comprendre leur importance pour la sécurité informatique d’une organisation.