ENSEEIHT **TLSSEC**
Formation TLSSEC **Examen**

Attaque et sécurisation des couches OSI

18 novembre 2019

Cet examen dure 1h45. Les documents ne sont pas autorisés. Le barème est donné à titre indicatif.

---

1 Dénis de service distribué

Question 1.1 (2 points)

Quels seraient les principes d'une attaque d'UDP flooding pour maximiser son efficacité et ses chances de succès ?

Question 1.2 (3 points)

Un serveur a une file d'attente pour enregistrer les connexions TCP semi-ouvertes de 512 entrées. Ce serveur reçoit des requêtes SYN (demandes d'ouverture de connexion TCP) selon une loi de Poisson de moyenne 10. On considère que le timer d'attente de la finalisation de l'ouverture de connexion est fixe et égal à 20 secondes.

Quelles seraient les caractéristiques d'une attaque de SYN flooding qui réduirait à moins de 1% la probabilité d'établissement d'une connexion légitime ?

2 Couches 1 à 4 du modèle OSI

Question 2.1 (vulnérabilités IP, 3 points)

Donnez les principes d'un dénis de service simple, appelé le *smurfing*, qui peut être exécuté localement ou à distance, l'encontre d'une routeur ou d'un hôte, à l'aide du protocole ICMP / echo request. Proposez une variante qui devrait pouvoir fonctionner sur les réseaux actuels.

Quelles contremesures simples peuvent être appliquées contre ce type d'attaque ? Sur quels équipements réseaux et à quel niveau OSI ?

En supposant que les piles IP ne sont pas protégées, quelle variante, encore plus efficace et générale peut-être exécutée en manipulant spécifiquement l'adressage au niveau IP, et permettant d'attaque plusieurs hôtes et routeurs en même temps ?

Quelle contremesures simple peuvent être proposées dans ce deuxième cas ? Au niveau IP et / ou liaison de données ?

Question 2.2 (3 points)

Voici la spécification de deux services réseaux :

— `chargen 19/udp` :
In the UDP implementation of the protocol, the server sends a UDP datagram containing a random number (between 0 and 512) of characters every time it receives a datagram from the connecting host [1].

— `echo 7/udp` :
A host may connect to a server that supports the Echo Protocol using the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP) on the well-known port number 7. The server sends back an identical copy of the data it received [2].

À l'aide de ces deux services, comment construire une attaque simple générant un trafic ayant une augmentation à caractère linéaire ?

À caractère exponentiel ?

Question 2.3 (2 points)

Décrire succinctement le service rendu par un serveur DHCP.

Quelle attaque simple, ciblant uniquement ce protocole, peut être menée pour rendre l'accès à ce service indisponible ?

Quelle attaque sur ce même protocole peut-être ensuite menée après cette première attaque ?

Proposer une contremesure simple contre la premiere attaque (dénis de service).

Question 2.4 (2 points)

Le protocole SMB permet de négocier la méthode d'authentification de l'utilisateur. Le client envoie une liste de protocoles d'authentification qu'il supporte au serveur. Le serveur reçoit les protocoles et impose une méthode parmi celles qui ont été envoyées, en précisant si possible le "paramétrage d'aspects de sécurité".

Exemple d'envoi de la liste des protocoles d'authentification supportés par le client :

```
Negotiate Protocol Request (0x72)
Word Count (WCT): 0
Byte Count (BCC): 155
Requested Dialects
  Dialect: PC NETWORK PROGRAM 1.0
  Dialect: MICROSOFT NETWORKS 1.03
  Dialect: MICROSOFT NETWORKS 3.0
  Dialect: LANMAN1.0
  Dialect: LM1.2X002
  Dialect: DOS LANMAN2.1
  Dialect: LANMAN2.1
  Dialect: Samba
  Dialect: NT LANMAN 1.0
```

```
  Dialect: NT LM 0.12
```

Le serveur sélectionne un des protocoles listés et précise / configure la sécurité du protocole d'authentification choisi :

```
Negotiate Protocol Response (0x72)
  Word Count (WCT): 17
  Selected Index: 8: NT LANMAN 1.0
  Security Mode: 0x01, Mode
    .... ...1 = Mode: USER security mode
    .... ..1. = Password: ENCRYPTED password
    .... .0.. = Signatures: Security signatures NOT enabled
    .... 0... = Sig Req: Security signatures NOT required
[..]
```

Comment peut on attaquer la confidentialité du mot de passe d'un utilisateur s'authentifiant en se situant dans le même réseau qu'un serveur et un client SMB. Décrire brièvement l'attaque en 3 ou 4 étapes.

Quelles contremesures simples peut on appliquer à cette vulnérabilité protocolaire ?

Question 2.5 (1 points)

Samba est la mise en œuvre de SMB la plus utilisée par les systèms UNIX. Même si le protocole se base sur le système de gestion des utilisateurs local à l'hôte, Samba n'utilise pas la gestion locale des mots de passe pour authentifier les utilisateurs. En effet, la commande `smbpassword` permet de gérer les mots de passes d'accès au service SMB.

Décrire en une phrase un objectif de sécurité lié à la différenciation du système de mot de passe. Faites le parallèle avec la question précédente.

3 Couche application

Question 3.1 (1 points)

Comment est-ce que les réponses DNS sont "authentifiées" par un solveur récursif ou un *stub resolveur* (client final) ?
Nota bene : remarquez bien l'emploi des guillemets pour authentification :)

Question 3.2 (2 points)

Un empoisonnement DNS a pour objectif de modifier le cache DNS d'un serveur récursif victime avec des enregistrements controllés par un attaquant. La première classe d'attaque DNS publiée a consisté à modifier l'enregistrement **A** qui associe un nom de domaine à une adresse IP, dont la résolution a été demandé par une requête récursive.

Cette attaque est mise en œuvre en répondant à une requête de lecture d'un enregistrement envoyé par un serveur DNS recursif victime, avant le serveur responsable de la zone intérrogée. Ainsi, la réponse malveillante est acceptée et entre dans le DNS du serveur récursif victime, qui utilisera celui-ci jusqu'à son expiration donnée par l'attribut *Time To Live* de l'enregistrement.

Décrire succinctement la différence fondamentale entre l'attaque *DNS poisonning* de kaminsky et un *DNS poisonning* classique :

— quelle mécanique DNS est visée ?
— quel type d'enregistrement est par conséquent modifié ? (**A**, **MX**, **NS**, ...)
— quelle est la principale raison ayant motivé l'amélioration de l'attaque classique par Kaminsky ?
— quelle technique utilise-t-il pour maximiser ses chances de succès.

Question 3.3 (1 points)

Quel sont les trois enregistrement DNSSEC qui servent à sécuriser la délégation de zone DNS parmi les enregistrements suivants :

— **NSEC** : *Next SECure*
— **RRSIG** : *Ressource Record SIGnature*
— **DNSKEY** : *DNS KEY*
— **DS** : *Delegation Signer*

Décrire en une phrase la mécanique sous-jacente.

Quels sont les enregistrements DNS signés dans ce cadre ?

4 Références

[1] `https://en.wikipedia.org/wiki/Character_Generator_Protocol`
[2] `https://en.wikipedia.org/wiki/Echo_Protocol`