Université de Tlemcen Faculté des Sciences Dept. Informatique	Module Sécurité Informatique L3 Année universitaire 2017/2018 C. BEKARA bekarach@gmail.com

TD 3 Corrigé : Attaques Réseaux

Exercice 1: Attaque par DoS 1

Soit un protocole de communication **X** se déroulant entre un client (machine) **A** et un serveur (machine) **B**, afin de fournir un service donné

Ce protocole opère au-dessus d'**UDP**, où la taille de la requête émise est de **27** octet, alors que la taille de la réponse correspondante est de **270** octets

Questions:

Q1 - Expliquer comment ce protocole peut être exploité pour lancer une attaque de type déni de service (DoS) contre une troisième machine victime **C?**

R1: L'attaquant usurpe l'identité de C et envoi une requête (27 B) au serveur, ce dernier enverra la réponse (270 B) à la victime C. C'est ce qu'on appelle une attaque de DoS par amplification

Q2 - Supposant maintenant que le protocole de communication X opère sous TCP, est ce que l'attaque de type DoS est toujours réalisable aussi simplement ?

R2: Si le protocole X fonctionne au-dessus de TCP, l'attaquant devra d'abord établir une connexion TCP avec le serveur avant de pouvoir envoyer la requête. L'établissement de la connexion requiert 3 messages:

SYN : envoyé de l'attaquant (en usurpant l'@ IP de la victime) au serveur avec un numéro de séquence aléatoire X généré par l'attaquant

SYN-ACK: envoyé du serveur à la victime **C** contenant X+1 ainsi qu'un numéro de séquence aléatoire **Y** généré par le serveur

ACK; envoyé de l'attaquant (en usurpant l'@ IP de la victime) au serveur contenant X+1 et **Y+1**

La difficulté ici réside à la capacité de l'attaquant à deviner/retrouver **Y**. Si l'attaquant ne se trouve pas dans le réseau de C ou Serveur, l'attaque a très peu de chance d'aboutir

Q3 - Revenant à la **Q1**. Supposant que l'attaquant possède une bande passante de **512 kbps**, qu'il peut exploiter pleinement pour son attaque. Selon vous, qu'elle sera la bande passante qui pourra être utilisé par l'attaque côté **C**?

R3: Après calcul, la bande passante consommé par l'attaque peut atteindre **5120kbps**

Q4 - Maintenant, supposant que la victime **C** dispose d'une bande passante de **10 Mbps.** Selon vous, quel est la bande passante minimale dont doit disposer l'attaquant afin que son attaque sature la totalité de la bande passante de l'utilisateur ?

R4: après calcul, la bande passante minimal dédié à l'attaque côté attaquant est de **1Mbps**

Exercice 2: Attaque par DoS 2

Le protocole PING, permet entre autres de tester la connectivité d'une machine sur un réseau. Il est basé sur l'envoi d'une requête "Echo Request" envoyé et la réception d'une réponse "Echo Reply".

En générale une requête PING est destiné a une machine cible, mais peut aussi être destiné à l'ensemble des machines d'un même sous/réseau, dans le cas où ceci n'est pas interdit par l'administrateur réseau

Q: Expliquez comment le PING peut être exploité par un attaquant, pour lancer une attaque de type DoS contre une machine du même un sous/réseau

R: l'attaquant enverra un PING (Echo Request) avec comme@ source l'@ IP de la machine victime (usurpation de son identité), et comme @ destination @ IP de diffusion (Broadcast) du sous-réseau auquel appartient la victime. L'ensemble des nœuds de ce même sous-réseau enverront leurs réponses (Echo Reply) à la victime

Exercice 3: ARP/IP Spoofing

Le protocole ARP (Adress Resolution Protocol) est un protocole qui fait la correspondance entre l'**@IP** (couche 3) d'une machine et son **@MAC** (couche 2). Deux machines se trouvant dans le même sous réseau, et communicant de façon direct -sans passer par un routeur/gateway- doivent posséder ou savoir l'@MAC de l'autre machine, autrement la communication ne peut avoir lieu

ARP fonctionne en mode Requête/Réponse, grâce aux deux messages suivants :

- **ARP Request Who-has (@IP, ?@MAC)**: qui possède l'@IP suivante? --> envoyé à l'ensemble du s/réseau par celui qui veut joindre une machine dont l'@IP est incluse dans la requête

- **ARP Reply Is-At (@IP, @MAC)**: l'@IP en question se trouve à l'@MAC indiqué en réponse --> envoyé par la machine concerné soit à la machine ayant envoyé la requête ou à l'ensemble des machines du s/réseau → ce paquet peut aussi être envoyé même si une ARP requête n'a pas été envoyé

Suite aux ARP Request/Reply, chaque machine du s/réseau maintient un cache contenant la correspondance **@IP/@MAC** des autres machine du sous-réseau, **le cache est rafraîchit périodiquement (les entrées sont supprimés au bout d'un temps T d'inactivité)**

Questions :

Q1 Expliquez comment l'usurpation d'identité d'une machine **A** (usurpation @ IP) du s/réseau peut avoir lieu par un attaquant **C** se trouvant dans le même sous réseau, afin que les paquets normalement envoyés à **A** soient reçu par **C** ? Étant donné les informations suivantes :

@IP_A: 192.168.1.20; **@MAC_A**: 00:25:47:F5:22:21

@MAC_C: 00:26:47:F5:23:22

R1: l'attaquant va envoyer **ARP Reply Is-At (@IP_A**, **@MAC_C**) soit à l'ensemble du réseau dans le cas où il veut détourner tout le trafic envoyé à **A**, où une machine particulière dans le cas où il veut juste détourner le

trafic envoyé à **A** depuis cette machine.

Par conséquent, les machines recevant ce message vont mettre à jour leur table ARP en associant **@IP_A** à l'**@MAC_C**. Ainsi, les paquets envoyés à **A** auront comme @ MAC destination **@MAC_C**, le commutateur interconnectant les machines va commuter ces paquets au port sur lequel est connecté la machine de l'attaquant **C**

Q2- Est ce que l'attaque d'usurpation peut se dérouler avec succès si la machine victime **A est** opérationnelle/joignable au même moment de l'attaque ?

R2 : L'attaque risque de ne pas se dérouler avec succès, car **A** va envoyer **ARP Reply Is-At (@IP_A, @MAC_A)**, résultant ainsi en la restauration à l'état saint des caches des autres nœuds du réseau, et donc l'acheminement des paquets envoyés à A par le commutateur au port sur lequel est connecté A. Dans ce cas, l'attaquant doit au-préalable lancer une attaque de type DoS contre A pour qu'il soit injoignable.

Q3- Selon vous, dans un réseau privé comment l'attaquant peut faire pour que tout le trafic du sous réseau quittant le s/réseau vers l'extérieur (ex: Internet) passe par lui?

R3: L'attaquant peut usurper l'@IP de la Gateway en diffusant **ARP Reply Is-At (@IP_Gateway**, **@MAC_C**), ce qui impliquera, que tous les paquets envoyés à la Gateway seront reçus par l'attaquant

Q4- En lien avec la **Q4)**. On suppose que notre réseau dispose d'un serveur DNS se trouvant sur Internet (ex: 8.8.8.8/8.8.4.4). Une attaque de type "DNS spoofing" consiste à falsifier les réponses DNS (Non de domaine <-> @ IP). Expliquer comment une telle attaque peut avoir lieu ?

R4 : L'attaquant doit réaliser une attaque de type MITM (homme au milieu) entre la Gateway et une machine victime **A**. L'idée est qu'une requête DNS légitime reçoit une réponse DNS falsifiée/modifiée. En effectuant l'attaque indiquée dans 3, l'attaquant va voir transiter par lui tout le trafic sortant vers Internet, et en particulier une requête DNS <Nom domaine, ?> venant d'une machine **A**. Par la suite, l'attaquant va usurper l'**@IP_A** et envoyer la requête DNS à la vraie Gateway (voir **R1**). La Gateway va recevoir la réponse DNS <Nom Domaine, @IP>, et puis l'envoyer à l'@IP_A, mais comme l'@MAC destination est celle de @MAC_C, lé réponse sera reçue par l'attaquant C. Ce dernier va falsifier la réponse DNS <Nom Domaine, $@IP_{falsifiée}$> puis l'envoyer à A en se faisant passer pour la Gateway.

Exercice 4 (La cryptographie au service de la sécurité : Fonction de hachage)

Soit H une fonction de hachage définie comme suit :

$H: \{0,1\}^* \rightarrow \{0,1\}^{128}$

Q1) Quelle est la taille du message sur lequel opère H ? Quel est la taille de l'empreinte/haché ?

R1: Taille message quelconque, taille haché/empreinte 128 bits

Q2) H étant résistante aux collisions, selon vous est-ce que ceci est en absolue (On ne pourra jamais trouver deux messages M_1, M_2 où $H(M_1)=H(M_2)$?

R2: Non H n'est pas résistante aux collision en Absolue (théoriquement) mais elle est résistante aux collision en pratique (il faudra énormément de temps et de ressources pour trouver une collision. En effet, on peut avoir 2^{128} hachés différents, pour lesquels au maximum 2^{128} messages différents peuvent exister sans qu'il y est de

collision (chacun de ces messages à un haché unique). Toute fois au-delà de 2^{128} messages une collision aura surement lieu car il ne reste plus de haché non consommé.

Q2-1) Si on suppose que le calcul d'un haché nécessite 10^{-12} secondes, au bout de combien de temps on est assuré de trouver une collision ?

R2-1) au bout de $2^{128}*10^{-12}$ s

Q3) répéter **Q2**) en supposant que la taille du haché généré est 256/386/512 bits, Que peut-on conclure concernant la taille du haché ?

R3: plus la taille du haché augmente, plus la fonction de hachage est plus robuste et plus le risque de collision diminue considérablement.

Q4) H protège l'intégrité des données, uniquement contre les erreurs de transmissions et non pas contre les modifications intentionnels pourquoi ?

Car un attaquant peut facilement intercepter le message **M**, le modifier en **M'** puis calculer **m'=H(M')** et envoyer **M'**,**m'** au récepteur, qui ne pourra pas détecter la modification