Sophie Valentin, Mathieu Bivert

Rapport des TDs du cours de Sécurité Réseau par Bruno Martin

2 février 2013

Table des matières

1 Topologie **3**

2 Configuration de la passerelle **3**
2.1 Tests 3

3 Configuration du serveur web **3**
3.1 Tests 3

4 Configuration serveur (smtp+imaps) et client (gpg) email **3**
4.1 Tests 4

5 Configuration VPN **4**
5.1 Tests 4

6 OpenVAS & Metasploit **4**

1 Topologie

2 Configuration de la passerelle

Une passerelle (gateway) est un homme du milieu reliant deux réseaux distincts. Dans le cas présent, la machine *passerelle* doit faire communiquer les deux réseaux SLAN et LAN Travaux Pratiques.

La passerelle doit être capable de router du traffic :

```
(passerelle)# echo 1 > /proc/sys/net/ipv4/ip_forward
```

L'IP Masquerade (Network Address Translation) doit être activée. Cette fonctionnalité modifie les entêtes IPs du traffic passant par *passerelle* afin de rendre invisibles, au niveau IP, les machines de LAN Travaux Pratiques depuis l'extérieur.

```
(passerelle)# iptables -t nat -A POSTROUTING -o eth0 -s 192.168.2.0/24 -j MASQUERADE
```

Enfin, syslogd doit être activé afin de logger les activités d'iptables

```
(passerelle)# apt-get install inetutils-syslogd
(passerelle)# edit /etc/syslog.conf # logs dans /var/log/kernel.log
(passerelle)# services syslog
```

2.1 Tests

On choisit un client, par exemple *client-bsd*, on lui retire l'interface réseau connectée à SLAN, et on s'assure que la machine est bien connectée sur LAN Travaux Pratiques, et qu'elle peut communiquer avec la passerelle. Enfin, on s'assure qu'il est possible de contacter le serveur et les Internets.

```
(client-bsd)# ifconfig em1 down # ou em0
(client-bsd)# ifconfig em0      # ou em1
(client-bsd)# ping passerelle.cs.sr
(client-bsd)# netstat -r
(client-bsd)# ping -c3 google.fr
```

On vérifie les logs sur la passerelle :

```
(passerelle)# tail -f /var/log/kernel.log
```

serveur telnet. mitm depuis backtrack. ssh. nmap

essai ssh avec mitm ? (normalement il affiche un message du genre "SOMEONE MAY BE ON THE CABLE !")

3 Configuration du serveur web

3.1 Tests

4 Configuration serveur (smtp+imaps) et client (gpg) email

La figure 1 donne un exemple simple de routage d'email, faisant intervenir 3 pièces logicielles :

MTA Mail Transfer Agent (eg. serveur SMTP), qui route les emails de domaines en domaines jusqu'à arriver à bonne destination ;

MDA Mail Delivery Agent (eg. serveur IMAP(s)), qui délivre les emails aux MUAs qui lui demandent ;

MUA Mail User Agent c'est le client email, dont le rôle principal est de récupérer les emails depuis un MDA, et d'en envoyer à un MTA ;

D'autres agents optionnels peuvent venir s'y greffer.

En pratique, on installe et configure postfix sur *passerelle*.

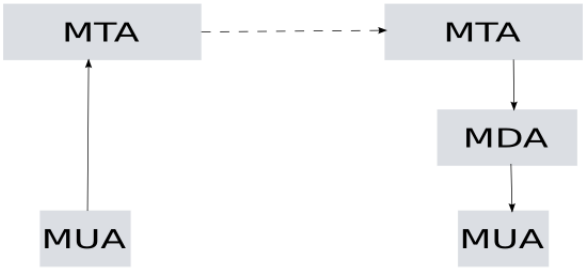

FIGURE 1 – Un MUA envoie un email à un MTA, qui le forward jusqu'à un MTA final, qui le transmet à un MDA. Enfin, le MUA du destinataire récupère l'email depuis ce MDA

4.1 Tests

5 Configuration VPN

5.1 Tests

6 OpenVAS & Metasploit