R401 — Contrôle

Exercice 1: Questions générales (15 points)

Q. 1 Un pare-feu sans état (stateless) peut-il bloquer (ou laisser passer) un paquet arrivant en réponse à un précédent paquet ?

A non B oui

Q. 2 Parmi les plages suivantes, laquelle peut être utilisée pour un réseau privé ?

A 192.168.0.0/24 B 128.0.0.0/8 C 1.2.3.0/24 D 127.0.0.0/8 E 172.192.0.0/16

Q. 3 Comment s'appelle la base de données recensant des failles de sécurité ?

A CVE B ScanDB C FailDB D Fail-VE E Mitre

Q. 4 Parmi ceux-ci lequel ne fait pas partie des propriété fondamentales en terme de sécurité ?

A disponibilité B intégrité C traçabilité D confidentialité E reproductibilité

Q. 5 Quelle catégorie d'IDS *ne peut pas* détecter de nouvelles attaques (i.e., celles exploitant des failles non répertoriées) ?

A ceux basés sur les spécifications B ceux basés sur les signatures C ceux basés sur les anomalies

Q. 6 Comment appelle-t-on une passerelle de niveau applicatif ?

A VPN B gateway C NAT D proxy E IDS F IPS

Q. 7 Quelle propriété fondamentale de la sécurité est violée lorsqu'un attaquant peut altérer une ressource (p.ex., un fichier) privée d'un utilisateur ?

A disponibilité B confidentialité C traçabilité D intégrité E reproductibilité

Q. 8 Quel type de balayage nmap permet de découvrir le type de pare-feu (stateless ou stateful) protégeant une cible ?

A XMAS B ACK C IDLE D FIN E NULL F SYN

Q. 9 Parmi les attaques suivantes, laquelle cible *spécifiquement* les serveurs web ?

A smurf B SYN flood C ping of death D land E XSS F DNS spoof

Q. 10 À quelle catégorie d'outils l'outil *fail2ban* appartient-il ?

A VPN B IPS C proxy D anti-virus E pare-feu

Q. 11 Sur un réseau privé avec une DMZ quel type d'hôtes place-t-on sur la DMZ ?

A des serveurs privés B des machines d'utilisateurs C des serveurs publics

Q. 12 Comment appelle-t-on un équipement avec des failles de sécurité volontaires utilisé pour tromper un attaquant ?

A rootme B proxy C honeypot D fake E lure F IPS

Q. 13 À quelle catégorie d'attaques l'attaque *land* appartient-elle ?

A brute force B DoS C man-in-the-middle D usurpation/spoofing E wabbit

Q. 14 Une passerelle NAT peut uniquement modifier les IP apparaissant dans l'en-tête IP mais jamais dans les données.

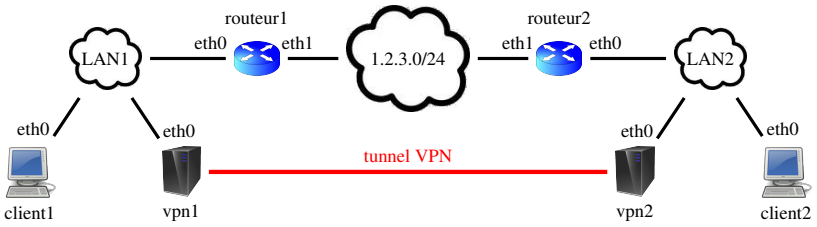
A faux B vrai

Q. 15 Comment s'appelle un pare-feu applicatif spécialisé dans la protection d'applications web ?

A FWW B WEBW C HTTPFW D WAF E HTTPS

Exercice 2: Tunnel VPN de niveau 2 (6 points)

Soit le réseau ci-dessous avec les IP associées aux interfaces:



Hôte	Interface	IP
client1	eth0	10.1.0.1
vpn1	eth0	10.1.0.100
routeur1	eth0	10.1.0.254
client2	eth0	10.2.0.1
vpn2	eth0	10.2.0.100
routeur2	eth0	10.2.0.254

On a mis en place un tunnel VPN entre vpn1 et vpn2 pour interconnecter les clients des deux réseaux locaux LAN1 et LAN2. On suppose dans cet exercice:

- que le tunnel est de *niveau 2* ;
- que vpn1 et vpn2 utilisent UDP pour transporter leurs données ;
- et enfin que le chiffrement n'altère pas la taille des données.

Rappels: en-tête + FCS ethernet = 26 octets ; en-tête IP = en-tête TCP = 20 octets ; et en-tête UDP = en-tête ICMP = 8 octets.

Q. 16 Quel masque doit-on choisir pour LAN1 et LAN2 (avec les IP données dans le tableau et étant donné que le tunnel est de niveau 2) pour les interfaces des deux LAN ? (Si plusieurs masques sont possibles on choisira le plus long.)

A un autre masque B /8 C /16 D /24

Q. 17 Le client2 peut-il recevoir une requête ARP ayant pour source client1 ?

A non B oui

Q. 18 Quel route faut-il ajouter sur client1 (avec `route add`) pour qu'il puisse communiquer avec client2 par le tunnel (Dans ces commandes `N` doit être remplacé par le masque choisi précédemment.) ?

A 10.2.0.0/N via 10.1.0.254
B 10.0.0.0/N via 10.1.0.1
C 10.0.0.0/N via 10.1.0.100
D 10.2.0.0/N via 10.1.0.100
E 10.0.0.0/N via 10.1.0.254
F aucune route n'est nécessaire

Q. 19 Est-il nécessaire d'exécuter la commande `sysctl net.ipv4.ip_forward=1` sur vpn1 et vpn2 ?

A oui B non

Q. 20 (*2 pt*) L'hôte client1 envoie un message ICMP encapsulant 100 octets de données. Quelle sera, en octets, la taille de la trame contenant ce message sur le tunnel ?

A 162 B 202 C 228 D 208 E 154 F 182 G une autre valeur

Exercice 3: Tunnel VPN de niveau 3 (6 points)

On se place dans le même contexte que dans l'exercice précédent à ceci près que le tunnel est maintenant de *niveau 3*. Toutes les autres hypothèses restent valables.

Q. 21 Quel masque doit-on choisir pour LAN1 et LAN2 (avec les IP données dans le tableau et étant donné que le tunnel est de niveau 3) pour les interfaces des deux LAN ? (Si plusieurs masques sont possibles on choisira le plus long.)

A /16 B /8 C /24 D un autre masque

Q. 22 L'hôte client2 peut-il recevoir une requête ARP ayant pour source client1 ?

A oui B non

Q. 23 Quel route faut-il ajouter sur client1 (avec `route add`) pour qu'il puisse communiquer avec client2 par le tunnel (Dans ces commandes `N` doit être remplacé par le masque choisi précédemment.) ?

A 10.2.0.0/N via 10.1.0.100
B 10.0.0.0/N via 10.1.0.254
C 10.2.0.0/N via 10.1.0.254
D 10.0.0.0/N via 10.1.0.100
E 10.0.0.0/N via 10.1.0.1
F aucune route n'est nécessaire

Q. 24 Est-il nécessaire d'exécuter la commande `sysctl net.ipv4.ip_forward=1` sur vpn1 et vpn2 ?

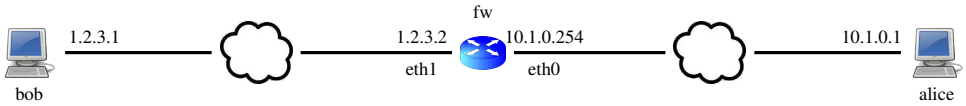
A non B oui

Q. 25 (*2 pt*) L'hôte client1 envoie un message ICMP encapsulant 100 octets de données. Quelle sera, en octets, la taille de la trame contenant ce message sur le tunnel ?

A 162 B une autre valeur C 182 D 208 E 202 F 154 G 228

Exercice 4: Filtrage avec iptables (8 points)

Soit le réseau suivant:



On exécute sur le routeur fw le script ci-dessous.

```
iptables -P FORWARD DROP
iptables -P INPUT   ACCEPT
iptables -P OUTPUT  ACCEPT
iptables -A INPUT -i eth1 -j DROP
iptables -A FORWARD -m state --state ESTABLISHED -j ACCEPT
iptables -A FORWARD -o eth1 -m state --state NEW -p tcp -j ACCEPT
iptables -A FORWARD -o eth1 -m state --state NEW -p tcp --dport 400 -j DROP
iptables -A FORWARD -p icmp -j ACCEPT
```

Une fois le script exécuté, indiquez, pour toutes les questions de cet exercice, si la commande fonctionne (oui) ou pas (non). On considérera qu'une commande fonctionne si aucun des paquets transmis lors de son exécution n'est filtré par fw. On supposera que toutes les conditions sont par ailleurs remplies pour que les commandes fonctionnent (adresses et routes bien configurées, serveurs en écoute, ...).

Q. 26 Sur fw: `ping 1.2.3.1`

A non B oui

Q. 27 Sur alice: `echo salut | nc 1.2.3.1 400`

A oui B non

Q. 28 Sur bob: `echo salut | nc 10.1.0.1 22`

A non B oui

Q. 29 Sur alice: `ping 1.2.3.1`

A non B oui

Q. 30 Sur alice: `echo salut | nc -u 1.2.3.1 123` (`-u` = mode UDP)

A oui B non

Q. 31 Sur alice: `ping 10.1.0.254`

A oui B non

Q. 32 Sur bob: `ping 1.2.3.2`

A oui B non

Q. 33 Sur alice: `echo salut | nc 1.2.3.1 80`

A non B oui

Exercice 5: NAT avec iptables (4 points)

On reprend le réseau de l'exerice précédent mais on exécute maintenant sur fw le script ci-dessous.

```
iptables -P FORWARD DROP
iptables -A FORWARD -i eth0 -j ACCEPT
iptables -A FORWARD -i eth1 -m state --state ESTABLISHED -j ACCEPT
```

Q. 34 Le pare-feu mis en place grâce à ce script est-il stateful ou stateless ?

A stateless B stateful C impossible à dire

Q. 35 On veut maintenant mettre en place des règles de translation d'adresse sur fw pour que le réseau 10.1.0.0/24 (celui de Alice) utilise l'IP publique de fw (1.2.3.2). Quelle commande faut-il rajouter pour cela au script ?

A `iptables -t nat -A POSTROUTING -o eth1 -j SNAT --to 1.2.3.2`
B `iptables -t nat -A POSTROUTING -o eth1 -j DNAT --to 1.2.3.2`
C `iptables -t nat -A PREROUTING -o eth1 -j DNAT --to 1.2.3.2`
D `iptables -t nat -A PREROUTING -o eth1 -j SNAT --to 1.2.3.2`
E `iptables -t nat -A FORWARD -o eth1 -j DNAT --to 1.2.3.2`
F `iptables -t nat -A FORWARD -o eth1 -j SNAT --to 1.2.3.2`

Q. 36 Après avoir mis en place la translation avec la commande précédente, on veut qu'un serveur TCP s'exécutant sur 10.1.0.1 et écoutant sur le port 25 soit accessible depuis le réseau public (1.2.3.0/24). Quelle commande faut-il rajouter pour cela au script ?

A `iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 25 -j DNAT --to 10.1.0.1`
B `iptables -t nat -A POSTROUTING -i eth1 -p tcp --dport 25 -j SNAT --to 10.1.0.1`
C `iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 25 -j SNAT --to 10.1.0.1`
D `iptables -t nat -A POSTROUTING -i eth1 -p tcp --dport 25 -j DNAT --to 10.1.0.1`
E `iptables -t nat -A PREROUTING -o eth0 -p tcp --dport 25 -j DNAT --to 10.1.0.1`
F `iptables -t nat -A FORWARD -i eth1 -p tcp --dport 25 -j SNAT --to 10.1.0.1`

Q. 37 Après avoir exécuté la commande de la question précédente, faut-il modifier une autre chaîne pour que fw accepte de router les paquets lorsque bob contacte 1.2.3.2 sur le port 25 ?

A oui: INPUT B oui: POSTROUTING C non D oui: FORWARD

Exercice 6: Snort et fail2ban (4 points)

Q. 38 (*1.5 pt*) Quelle règle snort permet de détecter une requête HTTP de type DELETE sur une ressource du répertoire `/img` ?

A `alert tcp any any -> any any (dport: http; uricontent: "DELETE /img";)`
B aucune proposition ne convient
C `alert http any any -> any 80 (content: "DELETE"; uricontent: "/img";)`
D `alert udp,tcp any any -> any 80 (content: "DELETE /img";)`
E `alert tcp any any -> any 80 (content: "DELETE"; uricontent: "/img";)`

Q. 39 Sur quel données fail2ban se base-t-il pour bannir des hôtes ?

A les règles iptables B les règles snort C les fichiers de log D les paquets capturés

Q. 40 (*1.5 pt*) Quelle règle snort permet de détecter un scan XMAS (bits P, U et F activés) en provenance du réseau 2.4.8.0/24 ?

A `alert icmp 2.4.8.0/24 any -> any any (flags: "PUF";)`
B `alert tcp 2.4.8.0/24 any -> any any (flags: "PUF";)`
C `alert udp 2.4.8.0/24 any -> any any (flags: "PUF";)`
D `alert udp 2.4.8.0/24 any -> any any (content: "PUF";)`
E `alert tcp any any -> 2.4.8.0/24 any (content: "PUF";)`

Feuille de réponses

Prénom et nom :

Q. 1 [A] [B]
Q. 2 [A] [B] [C] [D] [E]
Q. 3 [A] [B] [C] [D] [E]
Q. 4 [A] [B] [C] [D] [E]
Q. 5 [A] [B] [C]
Q. 6 [A] [B] [C] [D] [E] [F]
Q. 7 [A] [B] [C] [D] [E]
Q. 8 [A] [B] [C] [D] [E] [F]
Q. 9 [A] [B] [C] [D] [E] [F]
Q. 10 [A] [B] [C] [D] [E]
Q. 11 [A] [B] [C]
Q. 12 [A] [B] [C] [D] [E] [F]
Q. 13 [A] [B] [C] [D] [E]
Q. 14 [A] [B]
Q. 15 [A] [B] [C] [D] [E]
Q. 16 [A] [B] [C] [D]
Q. 17 [A] [B]
Q. 18 [A] [B] [C] [D] [E] [F]
Q. 19 [A] [B]
Q. 20 [A] [B] [C] [D] [E] [F] [G]
Q. 21 [A] [B] [C] [D]
Q. 22 [A] [B]
Q. 23 [A] [B] [C] [D] [E] [F]
Q. 24 [A] [B]
Q. 25 [A] [B] [C] [D] [E] [F] [G]
Q. 26 [A] [B]
Q. 27 [A] [B]
Q. 28 [A] [B]
Q. 29 [A] [B]
Q. 30 [A] [B]
Q. 31 [A] [B]
Q. 32 [A] [B]
Q. 33 [A] [B]
Q. 34 [A] [B] [C]
Q. 35 [A] [B] [C] [D] [E] [F]
Q. 36 [A] [B] [C] [D] [E] [F]
Q. 37 [A] [B] [C] [D]
Q. 38 [A] [B] [C] [D] [E]
Q. 39 [A] [B] [C] [D]
Q. 40 [A] [B] [C] [D] [E]

R401 — Contrôle

Exercice 1: Questions générales (15 points)

Q. 1 À quelle catégorie d'attaques l'attaque *land* appartient-elle ?

A man-in-the-middle B DoS C wabbit D brute force E usurpation/spoofing

Q. 2 Une passerelle NAT peut uniquement modifier les IP apparaissant dans l'en-tête IP mais jamais dans les données.

A vrai B faux

Q. 3 Parmi les plages suivantes, laquelle peut être utilisée pour un réseau privé ?

A 172.192.0.0/16 B 192.168.0.0/24 C 1.2.3.0/24 D 127.0.0.0/8 E 128.0.0.0/8

Q. 4 Comment s'appelle un pare-feu applicatif spécialisé dans la protection d'applications web ?

A HTTPS B FWW C HTTPFW D WEBW E WAF

Q. 5 Sur un réseau privé avec une DMZ quel type d'hôtes place-t-on sur la DMZ ?

A des serveurs publics B des machines d'utilisateurs C des serveurs privés

Q. 6 Parmi ceux-ci lequel ne fait pas partie des propriété fondamentales en terme de sécurité ?

A reproductibilité B traçabilité C intégrité D confidentialité E disponibilité

Q. 7 Parmi les attaques suivantes, laquelle cible *spécifiquement* les serveurs web ?

A SYN flood B DNS spoof C land D ping of death E XSS F smurf

Q. 8 Un pare-feu sans état (stateless) peut-il bloquer (ou laisser passer) un paquet arrivant en réponse à un précédent paquet ?

A oui B non

Q. 9 Comment appelle-t-on un équipement avec des failles de sécurité volontaires utilisé pour tromper un attaquant ?

A honeypot B lure C IPS D proxy E rootme F fake

Q. 10 Quelle propriété fondamentale de la sécurité est violée lorsqu'un attaquant peut altérer une ressource (p.ex., un fichier) privée d'un utilisateur ?

A traçabilité B disponibilité C intégrité D reproductibilité E confidentialité

Q. 11 À quelle catégorie d'outils l'outil *fail2ban* appartient-il ?

A IPS B proxy C pare-feu D anti-virus E VPN

Q. 12 Quel type de balayage nmap permet de découvrir le type de pare-feu (stateless ou stateful) protégeant une cible ?

A IDLE B NULL C XMAS D FIN E SYN F ACK

Q. 13 Comment appelle-t-on une passerelle de niveau applicatif ?

A NAT B IPS C IDS D VPN E proxy F gateway

Q. 14 Quelle catégorie d'IDS *ne peut pas* détecter de nouvelles attaques (i.e., celles exploitant des failles non répertoriées) ?

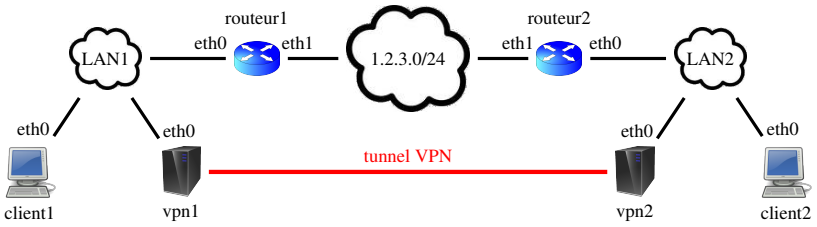
A ceux basés sur les spécifications B ceux basés sur les anomalies C ceux basés sur les signatures

Q. 15 Comment s'appelle la base de données recensant des failles de sécurité ?

A FailDB B ScanDB C CVE D Mitre E Fail-VE

Exercice 2: Tunnel VPN de niveau 2 (6 points)

Soit le réseau ci-dessous avec les IP associées aux interfaces:



Hôte	Interface	IP
client1	eth0	10.1.0.1
vpn1	eth0	10.1.0.100
routeur1	eth0	10.1.0.254
client2	eth0	10.2.0.1
vpn2	eth0	10.2.0.100
routeur2	eth0	10.2.0.254

On a mis en place un tunnel VPN entre vpn1 et vpn2 pour interconnecter les clients des deux réseaux locaux LAN1 et LAN2. On suppose dans cet exercice:

- que le tunnel est de *niveau 2* ;
- que vpn1 et vpn2 utilisent UDP pour transporter leurs données ;
- et enfin que le chiffrement n'altère pas la taille des données.

Rappels: en-tête + FCS ethernet = 26 octets ; en-tête IP = en-tête TCP = 20 octets ; et en-tête UDP = en-tête ICMP = 8 octets.

Q. 16 Quel masque doit-on choisir pour LAN1 et LAN2 (avec les IP données dans le tableau et étant donné que le tunnel est de niveau 2) pour les interfaces des deux LAN ? (Si plusieurs masques sont possibles on choisira le plus long.)

A /8 B /16 C un autre masque D /24

Q. 17 Le client2 peut-il recevoir une requête ARP ayant pour source client1 ?

A non B oui

Q. 18 Quel route faut-il ajouter sur client1 (avec `route add`) pour qu'il puisse communiquer avec client2 par le tunnel (Dans ces commandes `N` doit être remplacé par le masque choisi précédemment.) ?

A aucune route n'est nécessaire
B 10.2.0.0/N via 10.1.0.254
C 10.0.0.0/N via 10.1.0.100
D 10.0.0.0/N via 10.1.0.1
E 10.0.0.0/N via 10.1.0.254
F 10.2.0.0/N via 10.1.0.100

Q. 19 Est-il nécessaire d'exécuter la commande `sysctl net.ipv4.ip_forward=1` sur vpn1 et vpn2 ?

A non B oui

Q. 20 (*2 pt*) L'hôte client1 envoie un message ICMP encapsulant 100 octets de données. Quelle sera, en octets, la taille de la trame contenant ce message sur le tunnel ?

A une autre valeur B 208 C 162 D 182 E 154 F 202 G 228

Exercice 3: Tunnel VPN de niveau 3 (6 points)

On se place dans le même contexte que dans l'exercice précédent à ceci près que le tunnel est maintenant de *niveau 3*. Toutes les autres hypothèses restent valables.

Q. 21 Quel masque doit-on choisir pour LAN1 et LAN2 (avec les IP données dans le tableau et étant donné que le tunnel est de niveau 3) pour les interfaces des deux LAN ? (Si plusieurs masques sont possibles on choisira le plus long.)

A /24 B /16 C un autre masque D /8

Q. 22 L'hôte client2 peut-il recevoir une requête ARP ayant pour source client1 ?

A oui B non

Q. 23 Quel route faut-il ajouter sur client1 (avec `route add`) pour qu'il puisse communiquer avec client2 par le tunnel (Dans ces commandes `N` doit être remplacé par le masque choisi précédemment.) ?

A aucune route n'est nécessaire
B 10.0.0.0/N via 10.1.0.100
C 10.2.0.0/N via 10.1.0.100
D 10.0.0.0/N via 10.1.0.1
E 10.2.0.0/N via 10.1.0.254
F 10.0.0.0/N via 10.1.0.254

Pour votre examen, imprimez de préférence les documents compilés à l'aide de auto-multiple-choice.

Q. 24 Est-il nécessaire d'exécuter la commande `sysctl net.ipv4.ip_forward=1` sur vpn1 et vpn2 ?

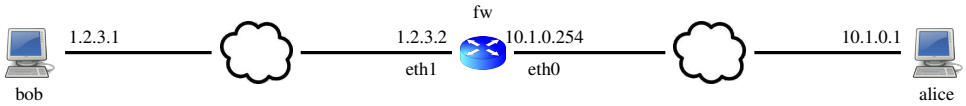
A oui B non

Q. 25 (*2 pt*) L'hôte client1 envoie un message ICMP encapsulant 100 octets de données. Quelle sera, en octets, la taille de la trame contenant ce message sur le tunnel ?

A 202 B 162 C 208 D 182 E 228 F 154 G une autre valeur

Exercice 4: Filtrage avec iptables (8 points)

Soit le réseau suivant:



On exécute sur le routeur fw le script ci-dessous.

```
iptables -P FORWARD DROP
iptables -P INPUT   ACCEPT
iptables -P OUTPUT  ACCEPT
iptables -A INPUT -i eth1 -j DROP
iptables -A FORWARD -m state --state ESTABLISHED -j ACCEPT
iptables -A FORWARD -o eth1 -m state --state NEW -p tcp -j ACCEPT
iptables -A FORWARD -o eth1 -m state --state NEW -p tcp --dport 400 -j DROP
iptables -A FORWARD -p icmp -j ACCEPT
```

Une fois le script exécuté, indiquez, pour toutes les questions de cet exercice, si la commande fonctionne (oui) ou pas (non). On considérera qu'une commande fonctionne si aucun des paquets transmis lors de son exécution n'est filtré par fw. On supposera que toutes les conditions sont par ailleurs remplies pour que les commandes fonctionnent (adresses et routes bien configurées, serveurs en écoute, . . .).

Q. 26 Sur alice: `echo salut | nc -u 1.2.3.1 123` (`-u` = mode UDP)

A oui B non

Q. 27 Sur alice: `echo salut | nc 1.2.3.1 400`

A non B oui

Q. 28 Sur alice: `echo salut | nc 1.2.3.1 80`

A non B oui

Q. 29 Sur alice: `ping 1.2.3.1`

A non B oui

Q. 30 Sur bob: `ping 1.2.3.2`

A oui B non

Q. 31 Sur fw: `ping 1.2.3.1`

A oui B non

Q. 32 Sur bob: `echo salut | nc 10.1.0.1 22`

A oui B non

Q. 33 Sur alice: `ping 10.1.0.254`

A non B oui

Exercice 5: NAT avec iptables (4 points)

On reprend le réseau de l'exerice précédent mais on exécute maintenant sur fw le script ci-dessous.

```
iptables -P FORWARD DROP
iptables -A FORWARD -i eth0 -j ACCEPT
iptables -A FORWARD -i eth1 -m state --state ESTABLISHED -j ACCEPT
```

Q. 34 Le pare-feu mis en place grâce à ce script est-il stateful ou stateless ?

A impossible à dire B stateful C stateless

Q. 35 On veut maintenant mettre en place des règles de translation d'adresse sur fw pour que le réseau 10.1.0.0/24 (celui de Alice) utilise l'IP publique de fw (1.2.3.2). Quelle commande faut-il rajouter pour cela au script ?

A `iptables -t nat -A PREROUTING -o eth1 -j DNAT --to 1.2.3.2`
B `iptables -t nat -A FORWARD -o eth1 -j SNAT --to 1.2.3.2`
C `iptables -t nat -A POSTROUTING -o eth1 -j SNAT --to 1.2.3.2`
D `iptables -t nat -A FORWARD -o eth1 -j DNAT --to 1.2.3.2`
E `iptables -t nat -A POSTROUTING -o eth1 -j DNAT --to 1.2.3.2`
F `iptables -t nat -A PREROUTING -o eth1 -j SNAT --to 1.2.3.2`

Q. 36 Après avoir mis en place la translation avec la commande précédente, on veut qu'un serveur TCP s'exécutant sur 10.1.0.1 et écoutant sur le port 25 soit accessible depuis le réseau public (1.2.3.0/24). Quelle commande faut-il rajouter pour cela au script ?

A `iptables -t nat -A POSTROUTING -i eth1 -p tcp --dport 25 -j DNAT --to 10.1.0.1`
B `iptables -t nat -A FORWARD -i eth1 -p tcp --dport 25 -j SNAT --to 10.1.0.1`
C `iptables -t nat -A PREROUTING -o eth0 -p tcp --dport 25 -j DNAT --to 10.1.0.1`
D `iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 25 -j DNAT --to 10.1.0.1`
E `iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 25 -j SNAT --to 10.1.0.1`
F `iptables -t nat -A POSTROUTING -i eth1 -p tcp --dport 25 -j SNAT --to 10.1.0.1`

Q. 37 Après avoir exécuté la commande de la question précédente, faut-il modifier une autre chaîne pour que fw accepte de router les paquets lorsque bob contacte 1.2.3.2 sur le port 25 ?

A oui: FORWARD B oui: INPUT C oui: POSTROUTING D non

Exercice 6: Snort et fail2ban (4 points)

Q. 38 (*1.5 pt*) Quelle règle snort permet de détecter un scan XMAS (bits P, U et F activés) en provenance du réseau 2.4.8.0/24 ?

A `alert tcp 2.4.8.0/24 any -> any any (flags: "PUF";)`
B `alert udp 2.4.8.0/24 any -> any any (content: "PUF";)`
C `alert udp 2.4.8.0/24 any -> any any (flags: "PUF";)`
D `alert icmp 2.4.8.0/24 any -> any any (flags: "PUF";)`
E `alert tcp any any -> 2.4.8.0/24 any (content: "PUF";)`

Q. 39 Sur quel données fail2ban se base-t-il pour bannir des hôtes ?

A les règles snort B les fichiers de log C les règles iptables D les paquets capturés

Q. 40 (*1.5 pt*) Quelle règle snort permet de détecter une requête HTTP de type DELETE sur une ressource du répertoire `/img` ?

A aucune proposition ne convient
B `alert tcp any any -> any any (dport: http; uricontent: "DELETE /img";)`
C `alert tcp any any -> any 80 (content: "DELETE"; uricontent: "/img";)`
D `alert http any any -> any 80 (content: "DELETE"; uricontent: "/img";)`
E `alert udp,tcp any any -> any 80 (content: "DELETE /img";)`

+2/5/50+

Feuille de réponses

Prénom et nom :

Q. 1 A B C D E
Q. 2 A B
Q. 3 A B C D E
Q. 4 A B C D E
Q. 5 A B C
Q. 6 A B C D E
Q. 7 A B C D E F
Q. 8 A B
Q. 9 A B C D E F
Q. 10 A B C D E
Q. 11 A B C D E
Q. 12 A B C D E F
Q. 13 A B C D E F
Q. 14 A B C
Q. 15 A B C D E
Q. 16 A B C D
Q. 17 A B
Q. 18 A B C D E F
Q. 19 A B
Q. 20 A B C D E F G

Q. 21 A B C D
Q. 22 A B
Q. 23 A B C D E F
Q. 24 A B
Q. 25 A B C D E F G
Q. 26 A B
Q. 27 A B
Q. 28 A B
Q. 29 A B
Q. 30 A B
Q. 31 A B
Q. 32 A B
Q. 33 A B
Q. 34 A B C
Q. 35 A B C D E F
Q. 36 A B C D E F
Q. 37 A B C D
Q. 38 A B C D E
Q. 39 A B C D
Q. 40 A B C D E

Pour votre examen, imprimez de préférence les documents compilés à l'aide de auto-multiple-choice.