Sécurité dans les réseaux informatiques

Exercices+ Solutions

Vos ennemies connaissent les failles de sécurité de vos systèmes, les connaissez-vous?

Mohamed Mejri
Université Laval

October 18, 2016

Exercice 1 (Footprinting)

Questions

1. Quels sont les objectifs du footprinting?
2. Pourquoi les sites d'archivage de contenus web tels que `www.archive.com` sont des sources importantes d'informations pour un pirate?
3. Expliquer en donnant deux cas de figure concrets, comment des nouvelles économiques sur la cible peuvent aider un attaquant à atteindre ces objectifs?
4. Une machine peut-elle avoir deux noms DNS différents qui appartiennent à des domaines de premier niveau différents? Si oui, donner un exemple.
5. Décrire les trois étapes permettant la récupération de données relatives à `www.exemple.com` d'un annuaire `whois` .

Exercice 1

Réponses

1. Rassembler, sans contact "intrusif", le maximum d'informations sur la cible incluant : Le domaine, les emplacements physiques, les contacts (noms de personnes, téléphones, adresses courriel). Les intervalles des adresses IP, les masques des sous-réseaux.
2. Plusieurs informations pertinentes sur la cible telles que le nom et la version du serveur web, des noms et des coordonnées de personnes, pourraient être disponibles sur des vieilles versions de son site web.
3. Bonnes nouvelles, mauvaises mauvaises nouvelles, on en profite : recrutement->essayer de travailler; licenciement -> corrompre un employé en colère
4. www.google.com; www.google.fr

Exercice 1

Réponses

5. Demander au serveur S1=whois.iana.org, le nom du serveur S2 qui est responsable du domaine ".com" : `whois .com@S1`

   Demander au serveur S2, le nom R du registraire chez qui est enregistré `exemple.com` : `whois exemple.com@S2`

   Demander à R des informations sur `exemple.com` : `whois exemple.com@R`

Exercice 2 (Whois)

Question : Évaluer, de point de vu sécurité, l'enregistrement suivant donnant des données relatives à `wikipedia.org` dans l'annuaire `whois`.

```
Domain ID:  D51687756-LROR
Domain Name:  WIKIPEDIA.ORG
Created On:  13-Jan-2001 00:  12:  14 UTC
Last Updated On:  08-Jun-2007 05:  48:  52 UTC
Expiration Date:  13-Jan-2015 00:  12:  14 UTC
Sponsoring Registrar:  GoDaddy.com, Inc. (R91-LROR)
Status:  CLIENT DELETE PROHIBITED
Status:  CLIENT RENEW PROHIBITED
Status:  CLIENT TRANSFER PROHIBITED
Status:  CLIENT UPDATE PROHIBITED
Registrant ID:  GODA-09495921
Registrant Name:  DNS Admin
Registrant Organization:  Wikimedia Foundation, Inc.
Registrant Street1:  P.O. Box 78350
Registrant Street2:
Registrant Street3:
Registrant City:  San Francisco
Registrant State/Province:  California
Registrant Postal Code:  94107-8350
Registrant Country:  US
Registrant Phone:  +1.4158396885
Registrant Phone Ext.:
Registrant FAX:  +1.4158820495
Registrant FAX Ext.:
Registrant Email:  dns-admin@wikimedia.org
Admin ID:  GODA-29495921
Admin Name:  DNS Admin
```

Exercice 2 (Whois)

```
Admin Organization:  Wikimedia Foundation, Inc.
Admin Street1:  P.O. Box 78350
Admin Street2:
Admin Street3:
Admin City:  San Francisco
Admin State/Province:  California
Admin Postal Code:  94107-8350
Admin Country:  US
Admin Phone:  +1.4158396885
Admin Phone Ext.:
Admin FAX:  +1.4158820495
Admin FAX Ext.:
Admin Email:  dns-admin@wikimedia.org
Tech ID:  GODA-19495921
Tech Name:  DNS Admin
Tech Organization:  Wikimedia Foundation, Inc.
Tech Street1:  P.O. Box 78350
Tech Street2:
Tech Street3:
Tech City:  San Francisco
Tech State/Province:  California
Tech Postal Code:  94107-8350
Tech Country:  US
Tech Phone:  +1.4158396885
Tech Phone Ext.:
Tech FAX:  +1.4158820495
Tech FAX Ext.:
Tech Email:  dns-admin@wikimedia.org
Name Server:  NS0.WIKIMEDIA.ORG
Name Server:  NS1.WIKIMEDIA.ORG
Name Server:  NS2.WIKIMEDIA.ORG
```

Exercice 2

Réponses :

- Positifs :
  - Pas de noms de personnes (noms de rôles) même dans les adresses courriels
  - Un P.O. Box au lieu de l'adresse physique
- Point à revoir : Donner un numéro "1 800" au lieu d'un numéro de téléphone directe

Exercice 3 (Fragmentation)

Question : Choisir les réponses correctes dans la liste suivante :

☐ Quand le TTL d'un datagramme expire, un message ARP sera envoyé à la source
☐ Quand on est obligé de fragmenter un datagramme et son bit MF est mis à 1, alors on le détruit et on envoi un message ICMP à la source
☐ Quand on est obligé de fragmenter un datagramme et son bit DF est mis à 0, alors on le détruit et on envoi un message ICMP à la source
☒ Le dernier fragment d'un datagramme a son bit MF positionné à 0
☒ Un fragment d'un datagramme peut, à son tour, être fragmenté

Exercice 4 (SCAN)

Question : Choisir les réponses correctes dans la liste suivante :

☐ Un scan de type TCP-ACK passe mieux un pare-feu qu'un scan de type TCP-SYN
☐ Un scan de type TCP-ACK permet de dévoiler si un port UDP est ouvert
☐ Un scan de type TCP-ACK permet de dévoiler si un port TCP est ouvert
☒ Un ping de type TCP-ACK permet de découvrir si une machine est active
☐ Le protocole ARP permet des découvrir des ports TCP ouverts sur une machine

Exercice 5 (SCAN)

Question : Choisir les réponses correctes dans la liste suivante :

☐ Un scan UDP est plus rapide qu'un scan TCP parce que UDP est un protocole plus léger
☒ Un scan UDP permet de dévoiler si un serveur DNS est présent sur un réseau cible
☒ Un scan TCP permet de dévoiler si un serveur DNS est présent sur un réseau cible
☐ Un scan de type TCP-Null est plus furtif qu'un scan de type TCP-syn

Exercice 6 (SCAN)

Question : Choisir les réponses correctes dans la liste suivante :

☐ Un TCP-SYN scan consiste à envoyer un SYN attendre un SYN-ACK et envoyer un END
☒ Un TCP-SYN scan consiste à envoyer un SYN attendre un SYN-ACK puis envoyer un RST
☐ Un TCP-SYN scan consiste à envoyer un SYN attendre un SYN-ACK puis envoyer un ACK
☐ L'envoi d'un SYN retourne un END/ACK quand le port est fermé
☒ L'envoi d'un SYN peut retourner un ICMP de type 3 quand le port est fermé

Exercice 7 (SCAN)

Question : Choisir les réponses correctes dans la liste suivante :

☒ À l'intérieur d'un réseau Intranet, la technique la plus recommandée pour découvrir les machines actives est le protocole ARP
☐ À l'intérieur d'un réseau Intranet, la technique la plus recommandée pour découvrir les machines actives est le ping via ICMP
☐ À l'intérieur d'un réseau Intranet, la technique la plus recommandée pour découvrir les machines actives est l'envoie d'un ACK sur le port 80
☒ Le sacn d'un réseau à partir d'Intranet nous donne des résultats plus fiables qu'un scan via Internet

Exercice 8 (Traceroute)

Question : Choisir les réponses correctes dans la liste suivante :

☐ *Traceroute* est un outil qui bloque la route à un pirate qui scan des ports
☒ *Traceroute* est un outil qui nous aide à découvrir la route qui nous sépare d'une cible
☒ *Traceroute* est un outil qui nous aide à découvrir le périmètre d'une cible
☐ *Traceroute* se base sur le protocole ARP pour faire son travail
☒ *Traceroute* se base sur le protocole ICMP pour faire son travail

Exercice 9 (SMTP)

Question : Choisir les réponses correctes dans la liste suivante :

☐ Le protocole SNMP permet de découvrir si un réseau est accessible
☐ Le protocole SMTP permet de découvrir les processus qui tournent sur une machine
☒ Le protocole SNMP permet de découvrir les services sur une machine
☒ Le protocole SNMP permet de dévoiler les sites récemment visités par une cible
☐ Le protocole SMTP permet de voir le mémoire cache ARP d'une machine cible
☒ Le protocole SMTP permet de dévoiler si un serveur courriel permet le relai de message
☐ Un administrateur ne peut rien faire pour limiter le relai de pourriel

Exercice 10 (Enregistrements DNS)

Le serveur DNS d'une compagnie *A* contient les enregistrements suivants :

```
@ garage.com.     IN    SOA      ns1 hostmaster
                                 (
                                 17 ;serial
                                 86400 ;refresh
                                 21600 ;retry
                                 3600000 ;expire
                                 3600 ;negative ttl
                                 )
                  IN    NS       ns1.garage.com.
                  IN    NS       ns2.garage.com.
                  IN    MX       10 hercule.garage.com
ns1               IN    A        192.93.0.7
ns2               IN    A        192.93.0.41
ftp               IN    CNAME    asus
www               IN    CNAME    Jupiter
asus              IN    A        192.134.4.2
hercule           IN    A        192.168.4.3
Jupiter           IN    A        192.168.4.5
```

1. Quel est le nom de la zone DNS?
2. Quelle est l'adresse courriel de la personne responsable de cette zone?
3. Cette zone admet-elle un serveur courriel? si oui quelle est son adresse IP?
4. Quelle est l'adresse IP du serveur web de cette zone?
5. Quelle est l'adresse IP du serveur ftp de cette zone?
6. Quel enregistrement doit-on y ajouter pour que l'adresse www.canada.garage.com puisse être publiée comme l'URL de l'adresse web de cette entreprise?

Exercice 10 (Enregistrements DNS)

Réponses

1. Le nom du domaine de la zone est garage.com
2. hostmaster@garage.com
3. Oui, c'est hercule.garage.com. Son adresse IP est 192.168.4.3
4. C'est 192.168.4.5
5. C'est 192.134.4.2
6. C'est un enregistrement de type CNAME comme :

```
www.canada  IN  CNAME  Jupiter
```

Exercice 11 (Analyse de trafic)

La figure suivante donne des informations recueillies par un pirate en utilisant Wireshark.

Time	Source	Destination	Prot	Info
27.276263	171.14.73.164	171.14.15.7	DNS	Standard query A pop.laposte.net
27.315813	171.14.15.7	171.14.73.164	DNS	Standard query response A 81.255.54.11
27.316163	171.14.73.164	81.255.54.11	TCP	1126 > 110 [SYN] Seq=977216899 Ack=0 Win=5840 Len=0
27.384516	81.255.54.11	171.14.73.164	TCP	110 > 1126 [SYN, ACK] Seq=3895972264 Ack=977216900 Win=1460 Len=0
27.384600	171.14.73.164	81.255.54.11	TCP	1126 > 110 [ACK] Seq=977216900 Ack=3895972265 Win=5840 Len=0
27.444270	81.255.54.11	171.14.73.164	POP	Response: +OK POP3 server ready <0244B046B9D1@mx.laposte.net>
27.444341	171.14.73.164	81.255.54.11	TCP	1126 > 110 [ACK] Seq=977216900 Ack=3895972356 Win=5840 Len=0
27.444659	171.14.73.164	81.255.54.11	POP	Request: AUTH
27.498087	81.255.54.11	171.14.73.164	TCP	110 > 1126 [ACK] Seq=3895972356 Ack=977216906 Win=33304 Len=0
27.498687	81.255.54.11	171.14.73.164	POP	Response: +OK list of SASL extensions follows
27.499482	171.14.73.164	81.255.54.11	POP	Request: USER sarah.courci
27.551613	81.255.54.11	171.14.73.164	POP	Response: +OK Password required
27.584095	171.14.73.164	81.255.54.11	TCP	1126 > 110 [ACK] Seq=977216926 Ack=3895972426 Win=5840 Len=0
27.707559	00:30:7b:96:0a:4c	ff:ff:ff:ff:ff:ff	ARP	Who has 171.14.73.238? Tell 171.14.73.1
27.777012	08:00:20:a9:29:15	ff:ff:ff:ff:ff:ff	ARP	Who has 171.14.73.21? Tell 171.14.73.148
27.779493	00:30:7b:96:0a:4c	01:00:0c:dd:dd:dd	CGMP	Cisco Group Management Protocol
28.158396	00:10:83:fd:64:96	ff:ff:ff:ff:ff:ff	ARP	Who has 171.14.73.26? Tell 171.14.73.51
32.092320	00:03:47:68:5d:06	ff:ff:ff:ff:ff:ff	ARP	Who has 171.14.73.55? Tell 171.14.73.53
32.133948	171.14.73.137	171.14.73.255	BROWSER	Host Announcement KUIKPC15, Workstation, Server, NT Workstation
32.677003	08:00:20:a9:29:15	ff:ff:ff:ff:ff:ff	ARP	Who has 171.14.73.21? Tell 171.14.73.148
33.092263	00:03:47:68:5d:06	ff:ff:ff:ff:ff:ff	ARP	Who has 171.14.73.55? Tell 171.14.73.53
33.340910	171.14.73.73	171.14.73.255	Portmap	V2 CALLIT Call XID 0x3aff2436 dup XID 0x3aff2436
33.546360	171.14.73.164	81.255.54.11	POP	Request: PASS PLToueb
33.594457	81.255.54.11	171.14.73.164	TCP	110 > 1126 [ACK] Seq=3895972426 Ack=977216940 Win=33304 Len=0
33.676956	08:00:20:a9:29:15	ff:ff:ff:ff:ff:ff	ARP	Who has 171.14.73.21? Tell 171.14.73.148
33.678269	81.255.54.11	171.14.73.164	POP	Response: +OK 861 messages
33.678328	171.14.73.164	81.255.54.11	TCP	1126 > 110 [ACK] Seq=977216940 Ack=3895972444 Win=5840 Len=0
33.678585	171.14.73.164	81.255.54.11	POP	Request: STAT
33.726794	81.255.54.11	171.14.73.164	POP	Response: +OK 861 4068180
33.753155	171.14.73.164	81.255.54.11	POP	Request: LIST
33.814650	81.255.54.11	171.14.73.164	POP	Response: +OK
33.815116	171.14.73.164	81.255.54.11	TCP	1126 > 110 [ACK] Seq=977216952 Ack=3895975357 Win=11584 Len=0
33.816302	171.14.73.164	81.255.54.11	TCP	1126 > 110 [ACK] Seq=977216952 Ack=3895978005 Win=17376 Len=0
33.865467	171.14.73.164	81.255.54.11	TCP	1126 > 110 [ACK] Seq=977216952 Ack=3895980653 Win=23168 Len=0

Exercice 11 (Analyse de trafic)

Questions

1. Comment a-t-il paramétré son interface réseau pour intercepter ce trafic?
2. Quelles données intéressantes le pirate a-t-il pu récupérées?
3. Comment pourra-t-il les exploiter?

Exercice 11

Réponses

1. L'interface réseau est paramétrée en *promiscuous mode* (c'est-à-dire qu'elle écoute tous les paquets, même ceux qui ne lui sont pas directement destinés). Sous Unix par exemple, la commande : `ifconfig eth0 promisc` permet de configurer l'interface eth0 en mode promiscuous.
2. Les données les plus intéressantes sont :
   - Les trames 27.276263 et 27.315813 montrent que la machine 171.14.73.164 a fait une requête au serveur DNS 171.14.15.7 afin d'obtenir l'adresse IP du serveur du courriel "pop.laposte.net" (81.255.54.11)
   - Les trames 27.499482 et 33.546360 montre que l'utilisateur de la machine 171.14.73.164 a envoyé son *login* `sarah.courci` et son mot de passe `PLToueb`

Exercice 11

Réponses

3 Le pirate peut lire les courriels de Sarah Courci sur le serveur "pop.laposte.net". Il peut également tester si elle utilise le même *login* et mot de passe pour se connecter sur sa machine ou sur d'autres serveurs.

Exercice 12 (Scanning)

Question

L'attaquant a envoyé un paquet TCP ACK sur le port 80 de la cible, mais il n'a pas reçu de réponses. Que peut-il déduire à propos du port ciblé?

1. Ouvert
2. Fermé
3. Filtré
4. On ne peut pas répondre à la question à partir des informations données

Réponse : Il s'agit d'un port filtré. En effet, la réponse devrait être RST indépendamment si le port est ouvert ou il est fermé.

Exercice 13 (Scanning)

Question

L'attaquant a envoyé un paquet TCP SYN sur le port 80 de la cible, mais il n'a pas reçu de réponses. Que peut-il déduire à propos du port ciblé?

1. Ouvert
2. Fermé
3. Filtré
4. On ne peut pas répondre à la question à partir des informations données

Réponse : Il s'agit d'un port filtré. En effet, la réponse devrait être SYN/ACK si le port est ouvert et RST/ACK si le port est fermé.

Exercice 14 (Analyse du trafic)

Question Analyser la trace suivante

No. .	Time	Source	Destination	Protocol	Source Port	Dest. Port	Info
1	0.000000	10.1.0.2	10.1.0.1	TCP	2294	1	2294 > 1 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
2	0.000290	10.1.0.1	10.1.0.2	TCP	1	2294	1 > 2294 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3	0.006753	10.1.0.2	10.1.0.1	TCP	2296	2	2296 > 2 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
4	0.006890	10.1.0.1	10.1.0.2	TCP	2	2296	2 > 2296 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
5	0.012702	10.1.0.2	10.1.0.1	TCP	2298	3	2298 > 3 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
6	0.012809	10.1.0.1	10.1.0.2	TCP	3	2298	3 > 2298 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7	0.017518	10.1.0.2	10.1.0.1	TCP	2300	4	2300 > 4 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
8	0.017627	10.1.0.1	10.1.0.2	TCP	4	2300	4 > 2300 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
9	0.022309	10.1.0.2	10.1.0.1	TCP	2302	5	2302 > 5 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
10	0.022443	10.1.0.1	10.1.0.2	TCP	5	2302	5 > 2302 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11	0.027259	10.1.0.2	10.1.0.1	TCP	2304	6	2304 > 6 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
12	0.027386	10.1.0.1	10.1.0.2	TCP	6	2304	6 > 2304 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
13	0.033003	10.1.0.2	10.1.0.1	TCP	2306	7	2306 > 7 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
14	0.033260	10.1.0.1	10.1.0.2	TCP	7	2306	7 > 2306 [SYN, ACK] Seq=0 Ack=1 Win=8191 Len=0 MSS=1460
15	0.033484	10.1.0.2	10.1.0.1	TCP	2306	7	2306 > 7 [ACK] Seq=1 Ack=1 Win=8760 Len=0
16	0.038277	10.1.0.2	10.1.0.1	TCP	2308	8	2308 > 8 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
17	0.038519	10.1.0.1	10.1.0.2	TCP	8	2308	8 > 2308 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
18	0.043487	10.1.0.2	10.1.0.1	TCP	2310	9	2310 > 9 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
19	0.043832	10.1.0.1	10.1.0.2	TCP	9	2310	9 > 2310 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
20	0.044043	10.1.0.2	10.1.0.1	TCP	2310	9	2310 > 9 [ACK] Seq=1 Ack=1 Win=8760 Len=0
21	0.049285	10.1.0.2	10.1.0.1	TCP	2312	10	2312 > 10 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
22	0.049539	10.1.0.1	10.1.0.2	TCP	10	2312	10 > 2312 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	0.055083	10.1.0.2	10.1.0.1	TCP	2314	11	2314 > 11 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
24	0.055193	10.1.0.1	10.1.0.2	TCP	11	2314	11 > 2314 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
25	0.061076	10.1.0.2	10.1.0.1	TCP	2316	12	2316 > 12 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
26	0.061192	10.1.0.1	10.1.0.2	TCP	12	2316	12 > 2316 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	0.757918	10.1.0.2	10.1.0.1	TCP	2360	34	2360 > 34 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
28	0.757959	10.1.0.2	10.1.0.1	TCP	2368	38	2368 > 38 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
29	0.757978	10.1.0.2	10.1.0.1	TCP	2376	42	2376 > 42 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
30	0.757995	10.1.0.2	10.1.0.1	TCP	2362	35	2362 > 35 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
31	0.758012	10.1.0.2	10.1.0.1	TCP	2370	39	2370 > 39 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
32	0.758029	10.1.0.2	10.1.0.1	TCP	2378	43	2378 > 43 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
33	0.758046	10.1.0.2	10.1.0.1	TCP	2364	36	2364 > 36 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
34	0.758063	10.1.0.2	10.1.0.1	TCP	2372	40	2372 > 40 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
35	0.758081	10.1.0.2	10.1.0.1	TCP	2380	44	2380 > 44 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
36	0.758097	10.1.0.2	10.1.0.1	TCP	2366	37	2366 > 37 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
37	0.758114	10.1.0.2	10.1.0.1	TCP	2374	41	2374 > 41 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
38	0.758130	10.1.0.2	10.1.0.1	TCP	2382	45	2382 > 45 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=0 TSV=0 TSER=0

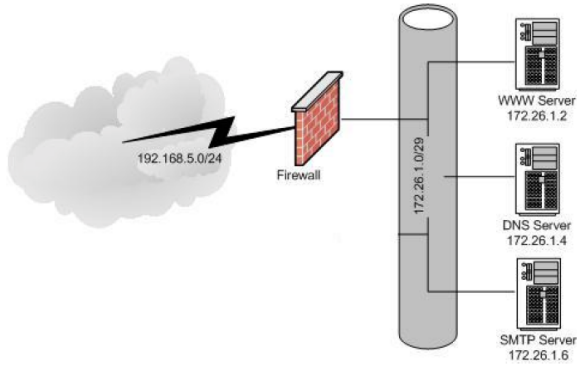
Exercice 14

Réponse

- *Tcp connect* des ports entre 1-12;
  - Le port 7 est ouvert
  - Le port 9 est ouvert
- *Tcp connect* des ports entre 34-45: Les ports entre 34 et 45 sont filtrés

Exercice 15 (Analyse du trafic)

Ayant le réseau suivant avec un pare-feu avec état, analysez la trace suivante



Firewall Ruleset

pass from any to 172.26.1.2 proto tcp port 80 keep state
pass from any to 172.26.1.4 proto tcp port 53 keep state
pass from any to 172.26.1.6 proto tcp port 25 keep state
drop all

Our command:

nmap –sP –PS80 172.26.1.0/29

tcpdump Output:

```
11:03:11.198359 192.168.5.20.49989 > 172.26.1.0.http: S 3857711107:3857711107(0) win 1024
11:03:11.198465 192.168.5.20.49989 > 172.26.1.1.http: S 3508535339:3508535339(0) win 1024
11:03:11.198506 192.168.5.20.49989 > 172.26.1.2.http: S 1017118803:1017118803(0) win 1024
11:03:11.198544 192.168.5.20.49989 > 172.26.1.3.http: S 832045179:832045179(0) win 1024
11:03:11.198582 192.168.5.20.49989 > 172.26.1.4.http: S 2873622691:2873622691(0) win 1024
11:03:11.198620 192.168.5.20.49989 > 172.26.1.5.http: S 1101529291:1101529291(0) win 1024
11:03:11.198658 192.168.5.20.49989 > 172.26.1.6.http: S 99614963:99614963(0) win 1024
11:03:11.198696 192.168.5.20.49989 > 172.26.1.7.http: S 3741843739:3741843739(0) win 1024
11:03:11.199453 172.26.1.2.http > 192.168.5.20.49989: S 92167158:92167158(0) ack
1017118804 win 5840 <mss 1460> (DF)
```

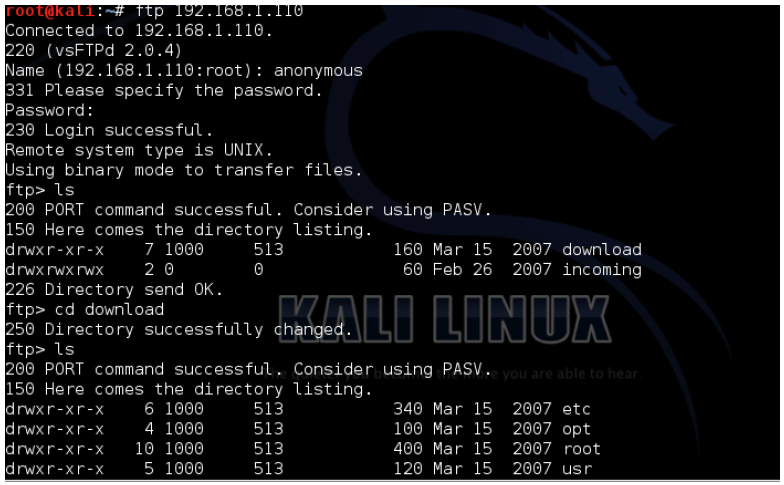
Exercice 15

Réponse

- La commande nmap a permis d'envoyer des demandes d'ouverture de connexion (TCP SYN) sur le port 80 (http) à toutes les machines du réseau 172.26.1.0/29 qui sont (172.26.1.1, 172.26.1.2,172.26.1.3, 172.26.1.4, 172.26.1.5 et 172.26.1.6)
- Le pare-feu bloque tout vers le port http à l'exception de celui destiné à la machine 172.26.1.2
- Donc, seule la machine 172.26.1.2 qui reçu sa demande d'ouverture de connexion et qui a repondu par SYN/ACK
- À partir de la machine 172.26.2.20, on peut conclure que la machine 172.26.1.2 est active et que le port 80 est ouvert
- Cette commande ne permet de rien conclure sur les autres machines

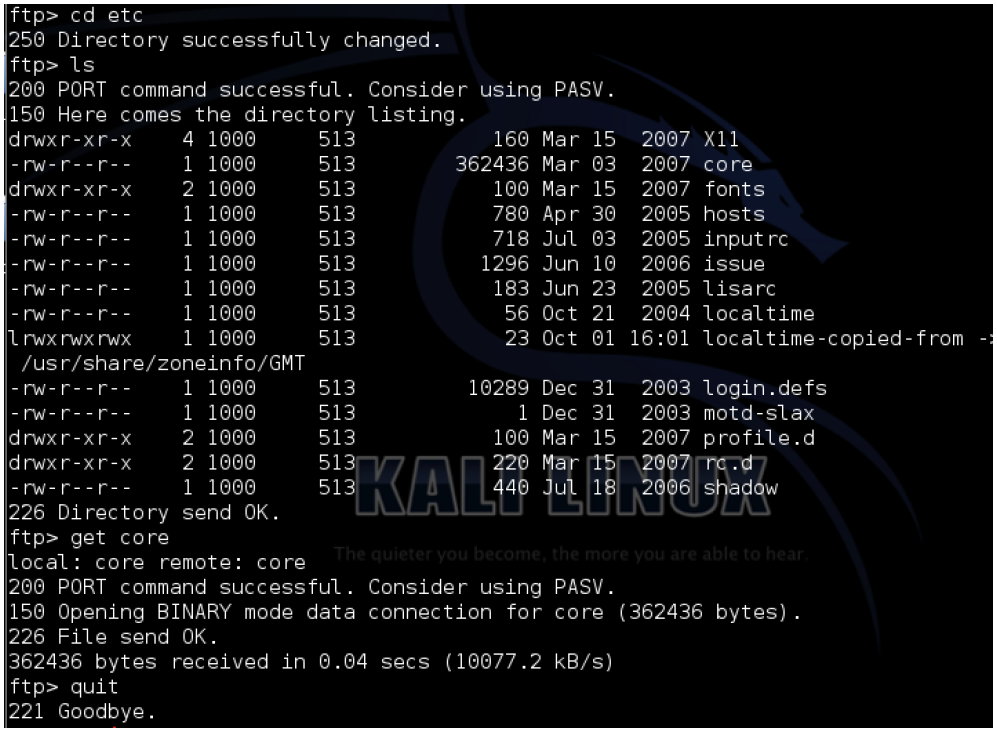
Exercice 16 (FTP)

Question : Décrire l'activité suivante d'un pirate : donner l'objectif, les actions et la conclusion



Exercice 16 (FTP)

(suite)



Exercice 16 (FTP)

(suite)

Exercice 16 (FTP)

Réponse :

Objectif : Énumération du service FTP à la recherche de mots de passe hachés

Actions :

- scanner la machine 192.168.1.110 (M110) à la recherche d'un service ftp
- vérifier si le serveur ftp de M110 permet une connexion anonyme
- naviguer dans les répertoires de M110 à la recherche de fichiers importants
- récupération du fichier core
- visualisation du contenu du fichier core qui montre des mots de passe hachés

Conclusion : L'énumération de serveur ftp de la machine M110 a permis au pirate de mettre la main sur des informations précieuses comme des mots de passe hachés

Exercice 17 (SMTP)

Question : Décrire l'activité suivante d'un pirate : donner l'objectif, les actions et la conclusion

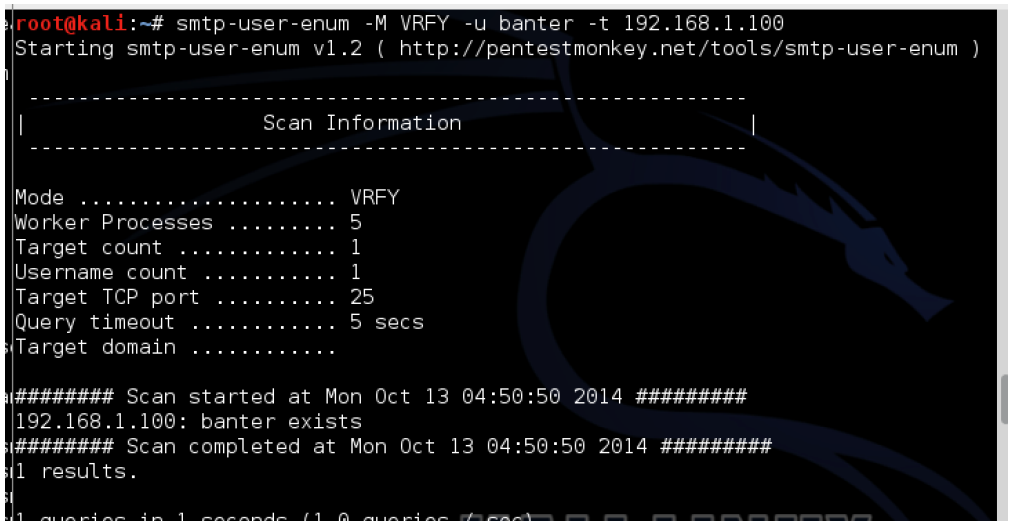
```
root@kali:~# nmap 192.168.1.100

Starting Nmap 6.47 ( http://nmap.org ) at 2014-10-13 04:26 EDT
Nmap scan report for 192.168.1.100
Host is up (0.0014s latency).
Not shown: 992 filtered ports
PORT    STATE  SERVICE
20/tcp  closed ftp-data
21/tcp  open   ftp
22/tcp  open   ssh
25/tcp  open   smtp
80/tcp  open   http
110/tcp open   pop3
143/tcp open   imap
443/tcp closed https
MAC Address: 00:0C:29:3D:20:53 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 17.52 seconds
```

Exercice 17 (SMTP)

(suite)



Exercice 17 (SMTP)

Réponse :

Objectif : Énumération du service SMTP à la recherche d'adresses courriel valides

Actions :

- scanner la machine 192.168.1.110 (M110) à la recherche d'un service smtp
- consulter le site web de M110 à la recherche d'adresses courriel. (adresse trouvée : banterb@herot.net)
- vérifier via, l'outil smtp-use-enum, si le nom figurant dans l'adresse courriel du site web (banterb) est un utilisateur valide du serveur SMTP de M110

Conclusion : le pirate a découvert un utilisateur (banterb) valide pour le serveur SMTP de la machine M110