

Travaux pratiques – Tracer une route

Objectifs

Partie 1 : vérifier la connectivité réseau à l'aide de la commande ping

Partie 2 : effectuer le suivi d'une route vers un serveur distant à l'aide de l'outil Traceroute

Partie 3 : effectuer le suivi d'une route vers un serveur distant à l'aide de l'outil web Traceroute

Contexte

Le suivi d'une route répertorie chaque appareil de routage qui achemine un paquet de la source à la destination sur un réseau. Ce logiciel de suivi s'exécute généralement dans une ligne de commande comme suit :

```
tracert <nom du réseau de destination ou adresse du périphérique final>
```

(Systèmes Microsoft Windows) ou

```
traceroute <nom du réseau de destination ou adresse du périphérique final>
```

(Unix et systèmes identiques)

L'outil **traceroute** (ou **tracert**) est souvent utilisé pour dépanner les réseaux. En affichant la liste des routeurs traversés, il permet à l'utilisateur d'identifier le chemin pris pour atteindre une destination particulière sur le réseau ou les interréseaux. Chaque routeur représente un point de connexion entre deux réseaux par lequel a été transféré le paquet de données. Le nombre de routeurs correspond au nombre de « tronçons » effectués par les données depuis la source jusqu'à la destination.

La liste affichée permet d'identifier les problèmes de flux de données lors de la tentative d'accès à un service tel qu'un site Web. Elle permet également d'effectuer des tâches telles que le téléchargement de données. Si plusieurs sites web (miroirs) sont disponibles pour le même fichier de données, il est possible de tracer chaque miroir pour déterminer le plus rapide.

Deux commandes traceroute entre la même source et la même destination exécutées à des moments différents peuvent produire des résultats différents. Cela s'explique par le « maillage » des réseaux interconnectés. Ceux-ci bénéficient du fait qu'Internet et les protocoles Internet sont capables de choisir différents chemins pour envoyer des paquets.

Les outils de traçage de route basés sur une interface en ligne de commande sont généralement intégrés au système d'exploitation du périphérique final.

Scénario

Via une connexion Internet, vous allez utiliser deux programmes de suivi de route pour examiner le chemin Internet menant aux réseaux de destination. Tout d'abord, vous allez vérifier la connectivité à un site web. Ensuite, vous allez utiliser l'utilitaire **traceroute** sur la ligne de commande Linux. Enfin, vous allez utiliser un outil traceroute basé sur le web (<http://www.monitis.com/traceroute/>).

Ressources requises

- Poste de travail virtuel CyberOps

- Accès Internet

Partie 1 : Vérifier la connectivité réseau à l'aide de la commande ping

Pour effectuer le suivi de la route jusqu'à un réseau distant, la machine virtuelle doit disposer d'une connexion à Internet opérationnelle.

- Démarrez le poste de travail virtuel CyberOps. Connectez-vous à la machine virtuelle avec les informations d'identification suivantes :

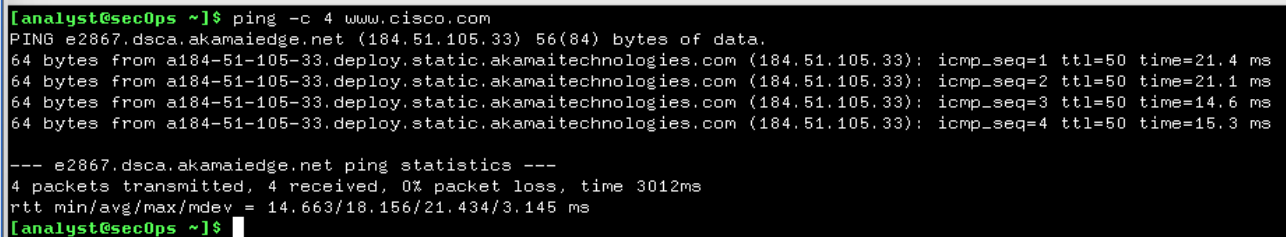
Nom d'utilisateur : **analyst**

Mot de passe : **cyberops**

- Ouvrez une fenêtre de terminal dans la machine virtuelle pour envoyer une requête ping à un serveur distant, tel que www.cisco.com.

```
[analyst@secOps ~]$ ping -c 4 www.cisco.com
PING e2867.dsca.akamaiedge.net (184.24.123.103) 56(84) bytes of data.
64 bytes from a184-24-123-103.deploy.static.akamaitechnologies.com (184.24.123.103): icmp_seq=1 ttl=59 time=13.0 ms
64 bytes from a184-24-123-103.deploy.static.akamaitechnologies.com (184.24.123.103): icmp_seq=2 ttl=59 time=12.5 ms
64 bytes from a184-24-123-103.deploy.static.akamaitechnologies.com (184.24.123.103): icmp_seq=3 ttl=59 time=14.9 ms
64 bytes from a184-24-123-103.deploy.static.akamaitechnologies.com (184.24.123.103): icmp_seq=4 ttl=59 time=11.9 ms

--- e2867.dsca.akamaiedge.net ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms rtt
min/avg/max/mdev = 11.976/13.143/14.967/1.132 ms
```



```
[analyst@secOps ~]$ ping -c 4 www.cisco.com
PING e2867.dsca.akamaiedge.net (184.51.105.33) 56(84) bytes of data.
64 bytes from a184-51-105-33.deploy.static.akamaitechnologies.com (184.51.105.33): icmp_seq=1 ttl=50 time=21.4 ms
64 bytes from a184-51-105-33.deploy.static.akamaitechnologies.com (184.51.105.33): icmp_seq=2 ttl=50 time=21.1 ms
64 bytes from a184-51-105-33.deploy.static.akamaitechnologies.com (184.51.105.33): icmp_seq=3 ttl=50 time=14.6 ms
64 bytes from a184-51-105-33.deploy.static.akamaitechnologies.com (184.51.105.33): icmp_seq=4 ttl=50 time=15.3 ms

--- e2867.dsca.akamaiedge.net ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3012ms
rtt min/avg/max/mdev = 14.663/18.156/21.434/3.145 ms
[analyst@secOps ~]$
```

- La première ligne affiche le nom de domaine complet (FQDN) e2867.dsca.akamaiedge.net. Elle est suivie de l'adresse IP 184.24.123.103. Cisco héberge le même contenu web sur différents serveurs dans le monde entier (appelés miroirs). Par conséquent, selon votre emplacement géographique, le nom de domaine complet et l'adresse IP seront différents.

Quatre requêtes ping ont été envoyées et une réponse a été reçue pour chaque requête ping. Étant donné que chaque requête ping a reçu une réponse, la perte de paquets correspond à 0 %. En moyenne, il a fallu 3005 ms (3005 millisecondes) pour acheminer les paquets sur le réseau. Une milliseconde correspond à 1/1 000^e de seconde. Vos résultats seront probablement différents.

Partie 2 : Effectuer le suivi d'une route vers un serveur distant à l'aide de l'outil Traceroute

Maintenant que l'accessibilité de base a été vérifiée à l'aide de l'outil ping, il est utile d'examiner de plus près chaque segment de réseau qui est traversé.

Suivant la taille de votre fournisseur d'accès Internet (FAI) et l'emplacement des hôtes source et de destination, les routes tracées peuvent passer par des sauts et des FAI différents. Chaque « saut » représente un routeur. Un routeur est un type d'ordinateur spécialisé qui permet de diriger le trafic sur Internet. Imaginez que vous effectuez un voyage en voiture dans plusieurs pays en utilisant de nombreuses autoroutes. À plusieurs endroits pendant le voyage, vous arrivez à des embranchements sur la route où vous avez la possibilité de choisir entre plusieurs autoroutes. Maintenant, imaginez qu'à chaque embranchement sur la route se trouve un dispositif qui vous oriente vers l'autoroute correcte vous permettant ainsi d'accéder à votre destination finale. C'est exactement le rôle d'un routeur pour les paquets sur un réseau.

Étant donné que les ordinateurs communiquent avec des nombres décimaux ou hexadécimaux, plutôt qu'avec des mots, les routeurs sont identifiés grâce à leur adresse IP. L'outil **traceroute** indique le chemin emprunté par un paquet de données sur le réseau pour atteindre sa destination finale. L'outil **traceroute** vous donne également une idée de la vitesse du trafic sur chaque segment du réseau. Des paquets sont envoyés à chaque routeur sur le chemin et le temps de retour est mesuré en millisecondes.

Pour ce faire, c'est l'outil **traceroute** qui est utilisé.

- a. À l'invite du terminal, tapez **traceroute www.cisco.com**.

```
[analyst@secOps ~]$ traceroute www.cisco.com traceroute to www.cisco.com
(184.24.123.103), 30 hops max, 60 byte packets
 1 192.168.1.1 (192.168.1.1) 6.527 ms 6.783 ms 6.826 ms
 2 10.39.176.1 (10.39.176.1) 27.748 ms 27.533 ms 27.480 ms
 3 100.127.65.250 (100.127.65.250) 27.864 ms 28.570 ms 28.566 ms
 4 70.169.73.196 (70.169.73.196) 29.063 ms 35.025 ms 33.976 ms
 5 fedlbbbrj01.xe110.0.rd.sd.cox.net (68.1.0.155) 39.101 ms 39.120 ms 39.108 ms
 6 a184-24-123-103.deploy.static.akamaitechnologies.com (184.24.123.103) 38.004
ms 13.583 ms 13.612 ms
```

```
[analyst@secOps ~]$ traceroute www.cisco.com
traceroute to www.cisco.com (184.51.105.33), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.365 ms  0.329 ms  0.303 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

Sur mon pc :

```
C:\Users\teopa>tracert www.cisco.com

Détermination de l'itinéraire vers e2867.dsca.akamaiedge.net [184.51.105.33]
avec un maximum de 30 sauts :

 1    3 ms    4 ms    4 ms  GateToHell.csnd.fr [10.203.0.254]
 2    4 ms    5 ms    4 ms  10.207.0.219
 3    5 ms    5 ms    7 ms  static-qvn-qvo-080092.business.bouyguestelecom.com [89.91.80.92]
 4   16 ms    6 ms    6 ms  31.33.19.2
 5    *      *      *    Délai d'attente de la demande dépassé.
 6    *      *      *    Délai d'attente de la demande dépassé.
 7    *      *      *    Délai d'attente de la demande dépassé.
 8    *      *      *    Délai d'attente de la demande dépassé.
 9    *      *      *    Délai d'attente de la demande dépassé.
10    *      *      *    Délai d'attente de la demande dépassé.
11    *      *      *    Délai d'attente de la demande dépassé.
12    *      *      *    Délai d'attente de la demande dépassé.
13   33 ms   11 ms   12 ms  a184-51-105-33.deploy.static.akamaitechnologies.com [184.51.105.33]

Itinéraire déterminé.
```

- b. Si vous souhaitez enregistrer la sortie de traceroute dans un fichier texte pour l'examiner ultérieurement, utilisez le caret de droite (>), nommez le fichier de la sortie comme il convient, puis enregistrez-le dans le répertoire actuel. Dans cet exemple, la sortie de traceroute est enregistrée dans le fichier /home/analyst/cisco-traceroute.txt.

Travaux pratiques – Tracer une route

```
[analyst@secOps ~]$ traceroute www.cisco.com > cisco-traceroute.txt
```

Vous pouvez maintenant saisir la commande **cat cisco-traceroute.txt** pour afficher la sortie de traceroute stockée dans le fichier texte.

```
[analyst@secOps ~]$ traceroute www.cisco.com > cisco-traceroute.txt
[analyst@secOps ~]$ cat cisco-traceroute.txt
traceroute to www.cisco.com (184.51.105.33), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.483 ms  0.428 ms  0.375 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

- c. Exécutez l'outil traceroute et enregistrez ses résultats pour l'un des sites web suivants. Il s'agit des sites web des organismes d'enregistrement Internet locaux de différentes parties du monde :

Afrique : **www.afrinic.net**

Australie : **www.apnic.net**

Europe : **www.ripe.net**

Amérique du Sud : **www.lacnic.net**

Remarque : il est possible que certains de ces routeurs sur la route ne répondent pas à traceroute.

Travaux pratiques – Tracer une route

```
--
[analyst@secOps ~]$ traceroute www.afrinic.net
traceroute to www.afrinic.net (196.216.2.6), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.366 ms  0.139 ms  0.100 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

Sur mon pc :

```
C:\Users\teopa>tracert www.afrinic.net

Détermination de l'itinéraire vers www.afrinic.net [196.216.2.6]
avec un maximum de 30 sauts :

 1    4 ms    6 ms    4 ms  GateToHell.csnd.fr [10.203.0.254]
 2    4 ms    4 ms    4 ms  10.207.0.219
 3   22 ms    5 ms    5 ms  static-qvn-qvo-080092.business.bouyguestelecom.com [89.91.80.92]
 4    *      11 ms    6 ms  31.33.19.2
 5    *      *      *      Délai d'attente de la demande dépassé.
 6    *     1620 ms    *      89.89.102.46
 7    *      *      *      Délai d'attente de la demande dépassé.
 8   27 ms   17 ms   17 ms  62.34.2.249
 9    *     23 ms   16 ms  la28.bsr01-lil.net.bbox.fr [212.194.171.71]
10   24 ms   22 ms   24 ms  80.249.213.52
11    *      *      *      Délai d'attente de la demande dépassé.
12    *      *      *      Délai d'attente de la demande dépassé.
13  205 ms  207 ms  251 ms  esr1-isd-crl-te0-0-26.wolcomm.net [197.157.77.97]
14  207 ms  197 ms  196 ms  197.157.64.195
15  207 ms  272 ms  196 ms  www.afrinic.net [196.216.2.6]
```

Partie 3 : Effectuer le suivi d'une route vers un serveur distant à l'aide de l'outil web Traceroute

- Ouvrez un navigateur web dans la machine virtuelle et accédez à <http://www.monitis.com/traceroute/>.

Travaux pratiques – Tracer une route

- b. Saisissez l'adresse du site que vous souhaitez remplacer **Exemple : google.com** et appuyez sur **Start Test**.

Visual Trace Route Tool

Traceroute your website and troubleshoot network problems, it's FREE!

Simply enter the URL or the IP address in the form to perform a traceroute to your website from the US, Europe and Asia simultaneously. Identify and isolate network connectivity issues now!

Example: google.com

Start Test

Pour ce TP j'ai utilisé ce site : <https://gsuite.tools/fr>.

traceroute to google.com (**142.250.187.238**), 30 hops max

Hop	Host	IP	Time (ms)
1	dgw1-wan-uk-lon1.ipv4.upcloud.com	83.136.248.1	0.153ms
2	100.69.37.17	100.69.37.17	0.270ms
3	172.17.255.225	172.17.255.225	0.271ms
4	172.17.255.249	172.17.255.249	10.731ms
5	195.66.224.125	195.66.224.125	0.771ms
6	192.178.97.181	192.178.97.181	0.729ms
7	142.251.54.47	142.251.54.47	0.711ms
8	lhr25s34-in-f14.1e100.net	142.250.187.238	0.678ms

```
C:\Users\teopa>tracert www.google.fr
```

```
Détermination de l'itinéraire vers www.google.fr [142.250.179.99]  
avec un maximum de 30 sauts :
```

```
 1  12 ms    4 ms    3 ms  GateToHell.csnd.fr [10.203.0.254]  
 2  20 ms    5 ms    4 ms  10.207.0.219  
 3  10 ms    5 ms    6 ms  static-qvn-qvo-080092.business.bouyguestelecom.com [89.91.80.92]  
 4  *        *      11 ms  31.33.19.2  
 5  *        *      *      Délai d'attente de la demande dépassé.  
 6  *        *      *      Délai d'attente de la demande dépassé.  
 7  *        *      *      Délai d'attente de la demande dépassé.  
 8  *        20 ms  18 ms  i15-lef01-t2-62-34-3-228.ft.lns.abo.bbox.fr [62.34.3.228]  
 9  23 ms    12 ms   13 ms  72.14.204.68  
10  15 ms    15 ms   20 ms  216.239.40.79  
11  28 ms    21 ms   17 ms  142.251.49.137  
12  31 ms    13 ms   12 ms  par21s20-in-f3.1e100.net [142.250.179.99]
```

```
Itinéraire déterminé.
```

- c. Vérifiez l'emplacement géographique des sauts correspondants. Qu'avez-vous remarqué concernant le chemin ?

J'ai remarqué qu'il existe différente route, c'est pourquoi ils sont différent car ils ont pas les même

Remarques générales

En quoi la sortie de traceroute est-elle différente lorsque vous accédez à www.cisco.com à partir du terminal (voir la partie 2) plutôt qu'à partir du site web en ligne ? (Vos résultats peuvent varier selon votre emplacement géographique et selon le FAI fournissant la connexion de votre école.)

En résumé, la sortie de la commande traceroute peut varier selon que vous l'exécutez à partir d'un terminal sur votre ordinateur ou à partir d'un site web en ligne en raison de facteurs tels que l'emplacement géographique, le fournisseur d'accès Internet, les politiques de routage et la charge du réseau. Ces variations peuvent entraîner des chemins différents empruntés par les paquets sur Internet, des adresses IP différentes pour chaque saut et des délais de réponse variables. En somme, la diversité des chemins et des conditions du réseau peut influencer la sortie de traceroute et ses résultats.