

Fait par Raphaël GEAY

I. Récolte d'informations

Adresses IP de ta machine

Prompt :

```
PS C:\Users\rapha> ipconfig
```

Résultats :

Carte réseau sans fil Wi-Fi :


```
Suffixe DNS propre à la connexion. . . :  
Adresse IPv6 de liaison locale. . . . : fe80::b5ab:a77f:acbe:9670%17  
Adresse IPv4. . . . . : 10.33.76.106  
Masque de sous-réseau. . . . . : 255.255.240.0  
Passerelle par défaut. . . . . : 10.33.79.254
```

Carte Ethernet Ethernet 2 :

```
Suffixe DNS propre à la connexion. . . :  
Adresse IPv6 de liaison locale. . . . : fe80::c6b4:c787:e1a8:a1f2%9  
Adresse IPv4. . . . . : 192.168.56.1  
Masque de sous-réseau. . . . . : 255.255.255.0  
Passerelle par défaut. . . . . :
```

Adresse de la carte wifi : 10.33.76.106

Adresse de la carte ethernet : 192.168.56.1

 Si t'as un accès internet normal, d'autres infos sont forcément dispos...

Prompt :

```
PS C:\Users\rapha> ipconfig /all
```

Résultats :

Carte réseau sans fil Wi-Fi :

```
Suffixe DNS propre à la connexion. . . :  
Description. . . . . : Intel(R) Wireless-AC 9560 160MHz  
Adresse physique . . . . . : 96-96-E4-BF-CC-80  
DHCP activé. . . . . : Oui  
Configuration automatique activée. . . : Oui  
Adresse IPv6 de liaison locale. . . . : fe80::b5ab:a77f:acbe:9670%17(préfééré)  
Adresse IPv4. . . . . : 10.33.76.106(préfééré)  
Masque de sous-réseau. . . . . : 255.255.240.0  
Bail obtenu. . . . . : vendredi 27 septembre 2024 09:01:54  
Bail expirant. . . . . : samedi 28 septembre 2024 09:01:54  
Passerelle par défaut. . . . . : 10.33.79.254  
Serveur DHCP . . . . . : 10.33.79.254  
IAID DHCPv6 . . . . . : 295081700  
DUID de client DHCPv6. . . . . : 00-03-00-01-96-96-E4-BF-CC-80  
Serveurs DNS. . . . . : 8.8.8.8  
                        1.1.1.1  
NetBIOS sur Tcpip. . . . . : Activé
```

Adresse de la passerelle : 10.33.79.254

Adresse IP du serveur DNS : 8.8.8.8

Adresse IP du serveur DHCP : 10.33.79.254

🌟 BONUS : Détermine s'il y a un pare-feu actif sur ta machine

Prompt :

```
PS C:\Users\rapha> Get-NetFirewallProfile
```

Résultats :

```
Name                : Domain  
Enabled              : True  
  
[...]  
  
Name                : Private  
Enabled              : True  
  
[...]  
  
Name                : Public  
Enabled              : True
```

Oui il existe un pare-feu actif sur le PC.

Prompt :

```
PS C:\Users\rapha> Get-NetFirewallRule
```

Résultats :

```
Name : {11812B0A-7903-4E90-A37E-7F8CD10639C8}
DisplayName : Windows Feature Experience Pack
Description : Windows Feature Experience Pack
DisplayGroup : Windows Feature Experience Pack
Group :
@{MicrosoftWindows.Client.CBS_1000.22700.1041.0_x64__cw5n1h2txyewy?ms-
resource://Micros
oftWindows.Client.CBS/resources/ProductPkgDisplayName}
Enabled : True
Profile : Domain, Private
Platform : {6.2+}
Direction : Inbound
Action : Allow
EdgeTraversalPolicy : Block
LooseSourceMapping : False
LocalOnlyMapping : False
Owner : S-1-5-21-3008062837-198257508-3391260086-1001
PrimaryStatus : OK
Status : La règle a été analysée à partir de la banque.
(65536)
EnforcementStatus : NotApplicable
PolicyStoreSource : PersistentStore
PolicyStoreSourceType : Local
RemoteDynamicKeywordAddresses : {}
PolicyAppId :
```

II. Utiliser le réseau

 Envoie un ping vers...

Prompt :

```
PS C:\Users\rapha> ping 10.33.76.106
```

Résultats :

```
Envoi d'une requête 'Ping' 10.33.76.106 avec 32 octets de données :
Réponse de 10.33.76.106 : octets=32 temps<1ms TTL=64
Réponse de 10.33.76.106 : octets=32 temps<1ms TTL=64
```

```
Réponse de 10.33.76.106 : octets=32 temps<1ms TTL=64
Réponse de 10.33.76.106 : octets=32 temps<1ms TTL=64
```

Statistiques Ping pour 10.33.76.106:

Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

Prompt :

```
PS C:\Users\rapha> ping 127.0.0.1
```

Résultats :

```
Envoi d'une requête 'Ping' 127.0.0.1 avec 32 octets de données :
Réponse de 127.0.0.1 : octets=32 temps<1ms TTL=64
Réponse de 127.0.0.1 : octets=32 temps<1ms TTL=64
Réponse de 127.0.0.1 : octets=32 temps<1ms TTL=64
Réponse de 127.0.0.1 : octets=32 temps<1ms TTL=64
```

Statistiques Ping pour 127.0.0.1:

Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms



On continue avec ping. Envoie un ping vers...

Prompt :

```
PS C:\Users\rapha> ping 10.33.79.254
```

Résultats :

```
Envoi d'une requête 'Ping' 10.33.79.254 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
```

Statistiques Ping pour 10.33.79.254:

Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),

Prompt :

```
PS C:\Users\rapha> ping 10.33.79.243
```

Résultats :

```
Envoi d'une requête 'Ping' 10.33.79.243 avec 32 octets de données :  
Délai d'attente de la demande dépassé.  
Délai d'attente de la demande dépassé.  
Délai d'attente de la demande dépassé.  
Délai d'attente de la demande dépassé.
```

```
Statistiques Ping pour 10.33.79.243:
```

```
Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
```

Prompt :

```
PS C:\Users\rapha> ping youtube.com
```

Résultats :

```
Envoi d'une requête 'ping' sur youtube.com [172.217.20.206] avec 32 octets de données :
```

```
Réponse de 172.217.20.206 : octets=32 temps=15 ms TTL=117
```

```
Réponse de 172.217.20.206 : octets=32 temps=16 ms TTL=117
```

```
Réponse de 172.217.20.206 : octets=32 temps=21 ms TTL=117
```

```
Réponse de 172.217.20.206 : octets=32 temps=20 ms TTL=117
```

```
Statistiques Ping pour 172.217.20.206:
```

```
Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
```

```
Durée approximative des boucles en millisecondes :
```

```
Minimum = 15ms, Maximum = 21ms, Moyenne = 18ms
```

Faire une requête DNS à la main

Prompt :

```
PS C:\Users\rapha> nslookup www.thinkerview.com
```

Résultats :

```
Serveur :   lan.home  
Address:  192.168.1.1
```

```
Réponse ne faisant pas autorité :  
Nom :      www.thinkerview.com  
Addresses: 2a06:98c1:3121::2  
           2a06:98c1:3120::2  
           188.114.97.2  
           188.114.96.2
```

Prompt :

```
PS C:\Users\rapha> nslookup www.wikileaks.org
```

Résultats :

```
Serveur :   lan.home  
Address:  192.168.1.1
```

```
Réponse ne faisant pas autorité :  
Nom :      wikileaks.org  
Addresses: 51.159.197.136  
           80.81.248.21  
Aliases:   www.wikileaks.org
```

Prompt :

```
PS C:\Users\rapha> nslookup www.torproject.org
```

Résultats :

```
Serveur :   lan.home  
Address:  192.168.1.1
```

```
Réponse ne faisant pas autorité :  
Nom :      www.torproject.org  
Addresses: 2620:7:6002:0:466:39ff:fe32:e3dd  
           2a01:4f9:c010:19eb::1  
           2620:7:6002:0:466:39ff:fe7f:1826  
           2a01:4f8:fff0:4f:266:37ff:feae:3bbc  
           2a01:4f8:fff0:4f:266:37ff:fe2c:5d19  
           95.216.163.36  
           116.202.120.165
```

```
116.202.120.166
204.8.99.146
204.8.99.144
```

IV. Network scanning et adresses IP



Effectue un scan du réseau auquel tu es connecté

Prompt :

```
PS C:\Users\rapha> nmap -sn -PR 192.168.56.1
```

Résultats :

```
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-05 23:00 Paris, Madrid (heure
d'été)
Nmap scan report for 192.168.56.1
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```



Changer d'adresse IP

Prompt :

```
PS C:\Users\rapha> ipconfig
```

Résultats :

Carte réseau sans fil Wi-Fi :

```
Suffixe DNS propre à la connexion. . . : home
Adresse IPv6. . . . . : 2a01:cb19:8dc:e200:5659:b50e:6caf:32d1
Adresse IPv6 temporaire . . . . . : 2a01:cb19:8dc:e200:7c2a:f9bd:d286:3c0e
Adresse IPv6 de liaison locale. . . . : fe80::6946:bde1:1df1:bd24%17
Adresse IPv4. . . . . : 192.168.1.200
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : fe80::aed7:5bff:fe10:5c70%17
                                192.168.1.1
```

Ma nouvelle adresse IP : 192.168.1.200