I. Récolte d'informations

Adresses IP de ta machine

Affiche l'adresse IP que ta machine a sur sa carte réseau WiFi

Commande :

- `ipconfig` ou `ipconfig /all`

Resultat :

```
PS C:\WINDOWS\system32> ipconfig /all

Carte réseau sans fil Wi-Fi :

   Suffixe DNS propre à la connexion. . . :
   Description. . . . . . . . . . . . . . : MediaTek MT7921 Wi-Fi 6 802.11ax PCIe
Adapter
   Adresse physique . . . . . . . . . . . : 34-6F-24-E2-DA-27
   DHCP activé. . . . . . . . . . . . . . : Oui
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . .: fe80::d31a:da20:d46:3687%12(préféré)
   Adresse IPv4. . . . . . . . . . . . . .: 10.33.78.234(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.240.0
   Bail obtenu. . . . . . . . . . . . . . : vendredi 27 septembre 2024 08:34:50
   Bail expirant. . . . . . . . . . . . . : samedi 28 septembre 2024 08:34:23
   Passerelle par défaut. . . . . . . . . : 10.33.79.254
   Serveur DHCP . . . . . . . . . . . . . : 10.33.79.254
   IAID DHCPv6 . . . . . . . . . . . : 137654052
   DUID de client DHCPv6. . . . . . . . : 00-01-00-01-2A-BE-AB-18-5C-60-BA-E4-58-
AB
   Serveurs DNS. . .  . . . . . . . . . . : 8.8.8.8
                                       1.1.1.1
   NetBIOS sur Tcpip. . . . . . . . . . . : Activé
```

Affiche l'adresse IP que ta machine a sur sa carte réseau ethernet :

Commande :

- `ipconfig /all`

Resultat :

```
PS C:\WINDOWS\system32> ipconfig /all

Carte Ethernet Ethernet :
```

```
   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :
   Description. . . . . . . . . . . . . . : Realtek Gaming GbE Family Controller
   Adresse physique . . . . . . . . . . . : 5C-60-BA-E4-58-AB
   DHCP activé. . . . . . . . . . . . . . : Oui
   Configuration automatique activée. . . : Oui
```

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

Affiche l'adresse IP de la passerelle du réseau local

Commande :

- `ipconfig /all`

Resultat Passerelle par défaut :

```
PS C:\WINDOWS\system32> ipconfig /all

Carte réseau sans fil Wi-Fi :

   Suffixe DNS propre à la connexion. . . :
   Description. . . . . . . . . . . . . . : MediaTek MT7921 Wi-Fi 6 802.11ax PCIe
Adapter
   Adresse physique . . . . . . . . . . . : 34-6F-24-E2-DA-27
   DHCP activé. . . . . . . . . . . . . . : Oui
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . .: fe80::d31a:da20:d46:3687%12(préféré)
   Adresse IPv4. . . . . . . . . . . . . .: 10.33.78.234(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.240.0
   Bail obtenu. . . . . . . . . . . . . . : vendredi 27 septembre 2024 08:34:50
   Bail expirant. . . . . . . . . . . . . : samedi 28 septembre 2024 08:34:23
   Passerelle par défaut. . . . . . . . . : 10.33.79.254
   Serveur DHCP . . . . . . . . . . . . . : 10.33.79.254
   IAID DHCPv6 . . . . . . . . . . . : 137654052
   DUID de client DHCPv6. . . . . . . . : 00-01-00-01-2A-BE-AB-18-5C-60-BA-E4-58-
AB
   Serveurs DNS. . .  . . . . . . . . . . : 8.8.8.8
                                       1.1.1.1
   NetBIOS sur Tcpip. . . . . . . . . . . : Activé
```

Affiche l'adresse IP du serveur DNS que connaît ton PC

Commande :

- `ipconfig /all`

resultat :

```
PS C:\WINDOWS\system32> ipconfig /all

Carte réseau sans fil Wi-Fi :

   Suffixe DNS propre à la connexion. . . :
   Description. . . . . . . . . . . . . . : MediaTek MT7921 Wi-Fi 6 802.11ax PCIe
Adapter
   Adresse physique . . . . . . . . . . . : 34-6F-24-E2-DA-27
   DHCP activé. . . . . . . . . . . . . . : Oui
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . .: fe80::d31a:da20:d46:3687%12(préféré)
   Adresse IPv4. . . . . . . . . . . . . .: 10.33.78.234(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.240.0
   Bail obtenu. . . . . . . . . . . . . . : vendredi 27 septembre 2024 08:34:50
   Bail expirant. . . . . . . . . . . . . : samedi 28 septembre 2024 08:34:23
   Passerelle par défaut. . . . . . . . . : 10.33.79.254
   Serveur DHCP . . . . . . . . . . . . . : 10.33.79.254
   IAID DHCPv6 . . . . . . . . . . . : 137654052
   DUID de client DHCPv6. . . . . . . . : 00-01-00-01-2A-BE-AB-18-5C-60-BA-E4-58-
AB
   Serveurs DNS. . .  . . . . . . . . . . : 8.8.8.8
                                       1.1.1.1
   NetBIOS sur Tcpip. . . . . . . . . . . : Activé
```

Affiche l'adresse IP du serveur DHCP que connaît ton PC

Commande :

- `ipconfig /all`

Resultat :

```
PS C:\WINDOWS\system32> ipconfig /all

Carte réseau sans fil Wi-Fi :

   Suffixe DNS propre à la connexion. . . :
   Description. . . . . . . . . . . . . . : MediaTek MT7921 Wi-Fi 6 802.11ax PCIe
Adapter
   Adresse physique . . . . . . . . . . . : 34-6F-24-E2-DA-27
   DHCP activé. . . . . . . . . . . . . . : Oui
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . .: fe80::d31a:da20:d46:3687%12(préféré)
   Adresse IPv4. . . . . . . . . . . . . .: 10.33.78.234(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.240.0
   Bail obtenu. . . . . . . . . . . . . . : vendredi 27 septembre 2024 08:34:50
   Bail expirant. . . . . . . . . . . . . : samedi 28 septembre 2024 08:34:23
   Passerelle par défaut. . . . . . . . . : 10.33.79.254
   Serveur DHCP . . . . . . . . . . . . . : 10.33.79.254
   IAID DHCPv6 . . . . . . . . . . . : 137654052
   DUID de client DHCPv6. . . . . . . . : 00-01-00-01-2A-BE-AB-18-5C-60-BA-E4-58-
```

```
AB
   Serveurs DNS. . .  . . . . . . . . . . . : 8.8.8.8
                                   1.1.1.1
   NetBIOS sur Tcpip. . . . . . . . . . . . : Activé
```

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

Commande :

```
$FWService = (Get-Service | ?{$_.Name -eq "mpssvc"});
$FWService | %{
 If($_.Status -eq "Running"){
     Write-Host "The $($_.DisplayName) service is running." -Foregroundcolor Green
     }Else{
     Write-Host "The $($_.DisplayName) service is stopped." -Foregroundcolor Red
     }
 };
```

Resultat :

```
PS C:\WINDOWS\system32> $FWService = (Get-Service | ?{$_.Name -eq "mpssvc"});
>> $FWService | %{
>>     If($_.Status -eq "Running"){
>>         Write-Host "The $($_.DisplayName) service is running." -Foregroundcolor
Green
>>         }Else{
>>         Write-Host "The $($_.DisplayName) service is stopped." -Foregroundcolor
Red
>>         }
>>     };
The Pare-feu Windows Defender service is running.
```

II. Utiliser le réseau

Envoie un ping vers...

Toi-même !

Commande :

- `ping 10.33.78.234`

Resultat :

```
   Envoi d’une requête 'Ping'  10.33.78.234 avec 32 octets de données :
Réponse de 10.33.78.234 : octets=32 temps<1ms TTL=128
Réponse de 10.33.78.234 : octets=32 temps<1ms TTL=128
Réponse de 10.33.78.234 : octets=32 temps<1ms TTL=128
Réponse de 10.33.78.234 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 10.33.78.234:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

Vers l'adresse IP `127.0.0.1`

Commande :

- ping `127.0.0.1`

Resultat :

```
PS C:\WINDOWS\system32> ping 127.0.0.1

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=128
Réponse de 127.0.0.1 : octets=32 temps<1ms TTL=128
Réponse de 127.0.0.1 : octets=32 temps<1ms TTL=128
Réponse de 127.0.0.1 : octets=32 temps<1ms TTL=128

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...

Ta passerelle !

Commande :

- ping `10.33.79.254`

Resultat :

```
PS C:\WINDOWS\system32> ping 10.33.79.254

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%),
```

Un(e) pote sur le réseau

Commande :

- ping 10.33.76.111

Resultat :

```
PS C:\WINDOWS\system32> ping 10.33.76.111

Envoi d’une requête 'Ping'  10.33.76.111 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 10.33.76.111:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
```

Un site internet

Commande :

- ping www.google.com

Resultat :

```
PS C:\WINDOWS\system32> ping www.google.com

Envoi d’une requête 'ping' sur www.google.com [142.250.75.228] avec 32 octets de
données :
Réponse de 142.250.75.228 : octets=32 temps=17 ms TTL=116
Réponse de 142.250.75.228 : octets=32 temps=17 ms TTL=116
Réponse de 142.250.75.228 : octets=32 temps=16 ms TTL=116
Réponse de 142.250.75.228 : octets=32 temps=17 ms TTL=116

Statistiques Ping pour 142.250.75.228:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 16ms, Maximum = 17ms, Moyenne = 16ms
```

Faire une requête DNS à la main

Commande :

- `nslookup www.thinkerview.com`

Resultat :

```
PS C:\WINDOWS\system32> nslookup www.thinkerview.com
>>
Serveur :   dns.google
Address:  8.8.8.8

Réponse ne faisant pas autorité :
Nom :    www.thinkerview.com
Addresses:  2a06:98c1:3121::7
          2a06:98c1:3120::7
          188.114.96.7
          188.114.97.7
```

```
PS C:\WINDOWS\system32> nslookup www.wikileaks.org
Serveur :   dns.google
Address:  8.8.8.8

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

```
PS C:\WINDOWS\system32> nslookup www.torproject.org
Serveur :   dns.google
Address:  8.8.8.8

Réponse ne faisant pas autorité :
Nom :    www.torproject.org
Addresses:  2a01:4f8:fff0:4f:266:37ff:fe2c:5d19
          2a01:4f8:fff0:4f:266:37ff:feae:3bbc
          2620:7:6002:0:466:39ff:fe32:e3dd
          2a01:4f9:c010:19eb::1
          2620:7:6002:0:466:39ff:fe7f:1826
          116.202.120.166
          204.8.99.144
          95.216.163.36
          116.202.120.165
          204.8.99.146
```

III. Sniffer le réseau

J'attends dans le dépôt git de rendu un fichier ping.pcap

Mon truc est lo

Livrez un deuxième fichier : dns.pcap

Mon truc 2 est lo

IV. Network scanning et adresses IP

Effectue un scan du réseau auquel tu es connecté

```
MAC Address: 7C:5A:1C:D3:D8:76 (Sophos)
Nmap scan report for 10.33.78.234
Host is up.
Nmap done: 4096 IP addresses (507 hosts up) scanned in 182.15 seconds
```

Changer d'adresse IP

```
Carte réseau sans fil Wi-Fi :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::d31a:da20:d46:3687%12
   Adresse IPv4. . . . . . . . . . . . . .: 10.33.70.116
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 10.33.79.254
```