Cybersécurité des services informatiques

PROFESSEURS : MR JOBARD

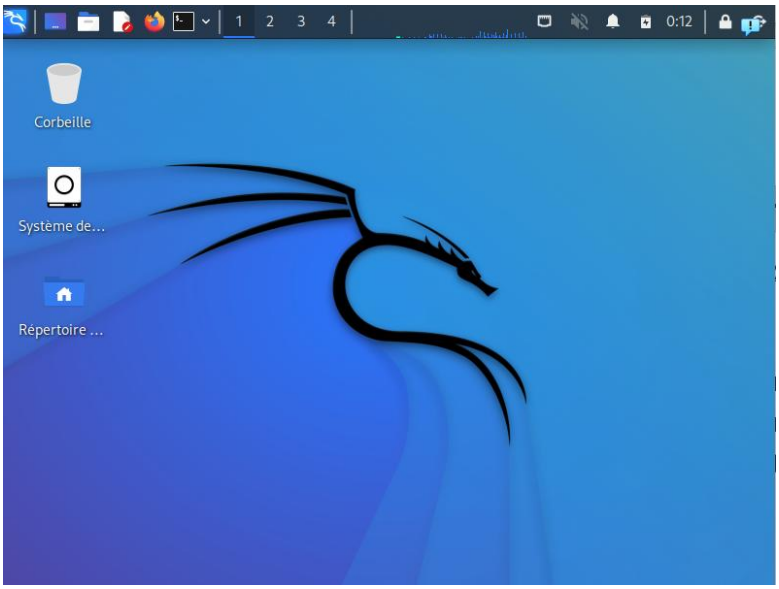
TP N°3 : Cookies

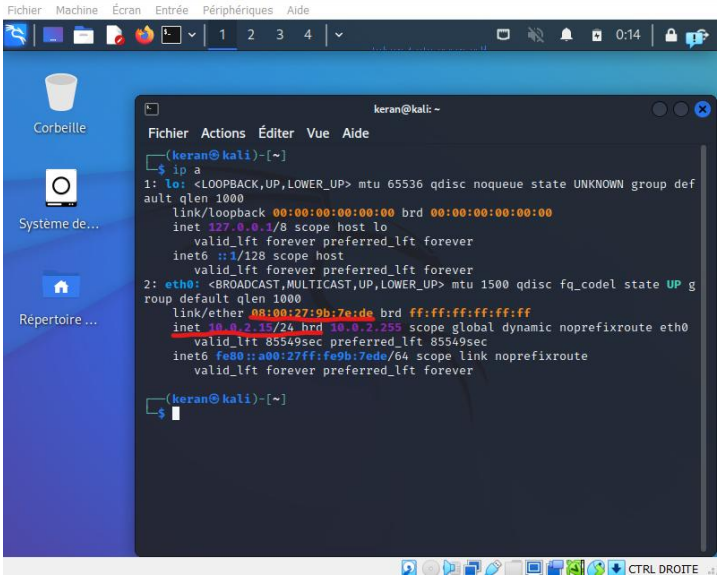
Objectif : Objectif : découvrir l'intérêt de sécuriser correctement une machine sous Windows ou Linux et savoir se protéger en se mettant à la place de l'attaquant via Kali Linux.

Introduction :

Dans le contexte actuel où les cybermenaces se multiplient, sécuriser correctement une machine, qu'elle fonctionne sous Windows ou Linux, est devenu une nécessité impérieuse. La protection de nos systèmes informatiques contre les attaques malveillantes est essentielle pour préserver l'intégrité, la confidentialité et la disponibilité des données. L'objectif de cette démarche est de découvrir l'intérêt de mettre en place des mesures de sécurité robustes et de comprendre les techniques utilisées par les attaquants pour mieux se protéger.

Pour ce faire, nous allons explorer l'utilisation de Kali Linux, une distribution spécialisée dans les tests d'intrusion et l'évaluation de la sécurité. En se mettant à la place de l'attaquant, nous pourrons identifier les vulnérabilités potentielles de nos systèmes et apprendre à les renforcer. Cette approche proactive nous permet non seulement de comprendre les méthodes employées par les cybercriminels, mais aussi d'élaborer des stratégies de défense plus efficaces. Ainsi, en nous familiarisant avec les outils et techniques de Kali Linux, nous serons mieux préparés à anticiper et contrer les menaces qui pèsent sur nos machines et nos réseaux.

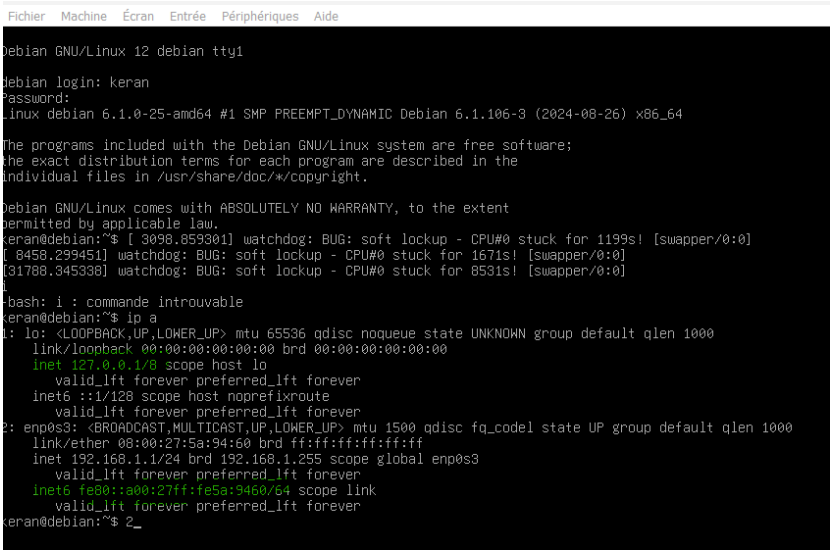


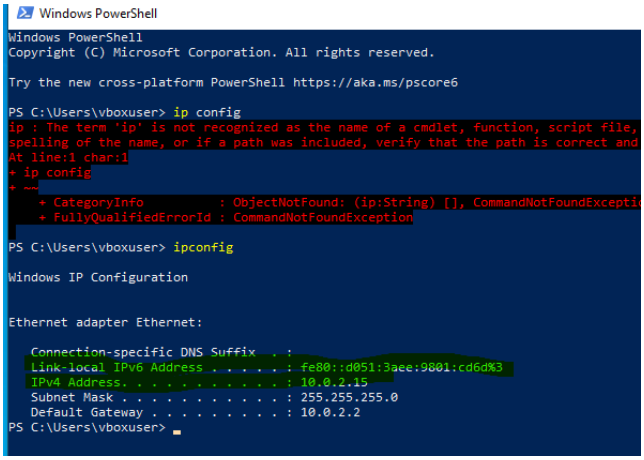


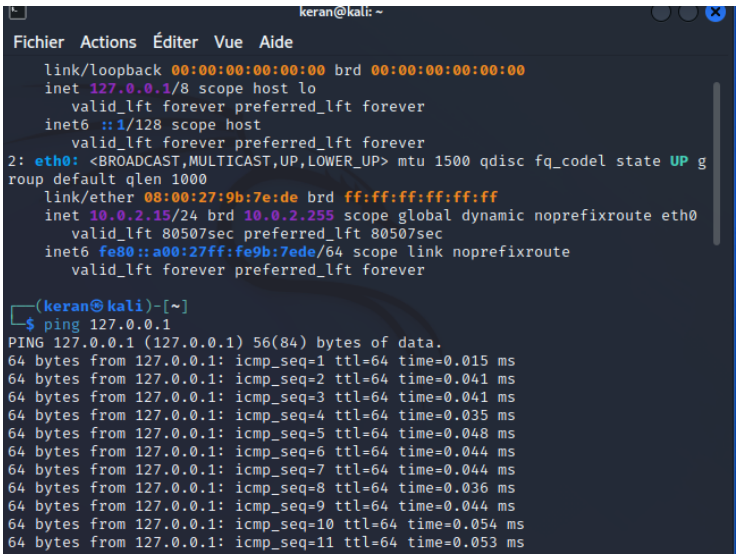
Ethernet Interface (eth0)

MAC Adress : 08 :00 :27 :9b :7e :de

IPv4 : 10.0.2.15


Fichier Machine Écran Entrée Périphériques Aide
Debian GNU/Linux 12 debian tty1
debian login: keran
Password:
Linux debian 6.1.0-25-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.106-3 (2024-08-26) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
keran@debian:~$ [3098.859301] watchdog: BUG: soft lockup - CPU#0 stuck for 1199s! [swapper/0:0]
[8458.299451] watchdog: BUG: soft lockup - CPU#0 stuck for 1671s! [swapper/0:0]
[31788.345338] watchdog: BUG: soft lockup - CPU#0 stuck for 8531s! [swapper/0:0]
i
-bash: i : commande introuvable
keran@debian:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:5a:94:60 brd ff:ff:ff:ff:ff:ff
inet 192.168.1.1/24 brd 192.168.1.255 scope global enp0s3
valid_lft forever preferred_lft forever
inet6 fe80::a00:27ff:fe5a:9460/64 scope link
valid_lft forever preferred_lft forever
keran@debian:~$ 2_


Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\Users\vboxuser> ip config
ip : The term 'ip' is not recognized as the name of a cmdlet, function, script file,
spelling of the name, or if a path was included, verify that the path is correct and
At line:1 char:1
+ ip config
+ ~~
+ CategoryInfo : ObjectNotFound: (ip:String) [], CommandNotFoundExceptio
+ FullyQualifiedErrorId : CommandNotFoundException
PS C:\Users\vboxuser> ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::d051:3aee:9801:cd6d%3
IPv4 Address. . . . . : 10.0.2.15
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.0.2.2
PS C:\Users\vboxuser>

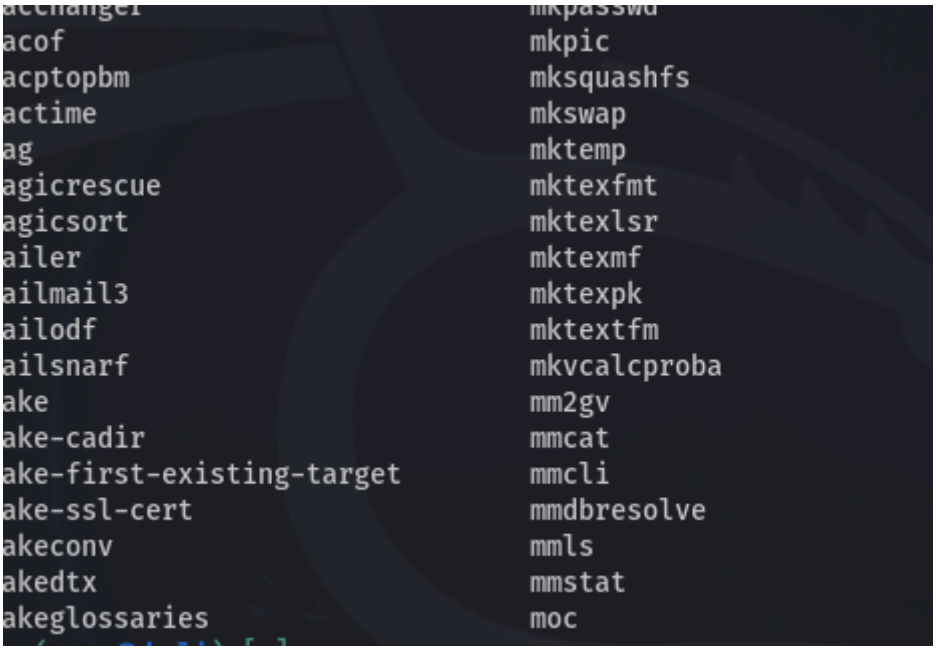

keran@kali: ~
Fichier Actions Éditer Vue Aide
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
link/ether 08:00:27:9b:7e:de brd ff:ff:ff:ff:ff:ff
inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
valid_lft 80507sec preferred_lft 80507sec
inet6 fe80::a00:27ff:fe9b:7ede/64 scope link noprefixroute
valid_lft forever preferred_lft forever
(keran㉿kali)-[~]
$ ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.041 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.041 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.035 ms
64 bytes from 127.0.0.1: icmp_seq=5 ttl=64 time=0.048 ms
64 bytes from 127.0.0.1: icmp_seq=6 ttl=64 time=0.044 ms
64 bytes from 127.0.0.1: icmp_seq=7 ttl=64 time=0.044 ms
64 bytes from 127.0.0.1: icmp_seq=8 ttl=64 time=0.036 ms
64 bytes from 127.0.0.1: icmp_seq=9 ttl=64 time=0.044 ms
64 bytes from 127.0.0.1: icmp_seq=10 ttl=64 time=0.054 ms
64 bytes from 127.0.0.1: icmp_seq=11 ttl=64 time=0.053 ms

```
debian:~$ ping 192.168.140.139
192.168.140.139 (192.168.140.139) 56(84) bytes of data.
tes from 192.168.140.139: icmp_seq=1 ttl=64 time=0.625 ms
tes from 192.168.140.139: icmp_seq=2 ttl=64 time=0.508 ms
tes from 192.168.140.139: icmp_seq=3 ttl=64 time=0.499 ms
tes from 192.168.140.139: icmp_seq=4 ttl=64 time=0.462 ms
tes from 192.168.140.139: icmp_seq=5 ttl=64 time=0.395 ms
tes from 192.168.140.139: icmp_seq=6 ttl=64 time=0.458 ms
tes from 192.168.140.139: icmp_seq=7 ttl=64 time=0.500 ms
tes from 192.168.140.139: icmp_seq=8 ttl=64 time=0.553 ms

 Stoppé                  ping 192.168.140.139
```

```
debian:~$ ping 192.168.140.141
192.168.140.141 (192.168.140.141) 56(84) bytes of data.
tes from 192.168.140.141: icmp_seq=1 ttl=128 time=1.23 ms
tes from 192.168.140.141: icmp_seq=2 ttl=128 time=0.735 ms
tes from 192.168.140.141: icmp_seq=3 ttl=128 time=0.661 ms
tes from 192.168.140.141: icmp_seq=4 ttl=128 time=0.583 ms
tes from 192.168.140.141: icmp_seq=5 ttl=128 time=0.675 ms
tes from 192.168.140.141: icmp_seq=6 ttl=128 time=1.05 ms
tes from 192.168.140.141: icmp_seq=7 ttl=128 time=0.498 ms
tes from 192.168.140.141: icmp_seq=8 ttl=128 time=0.530 ms
tes from 192.168.140.141: icmp_seq=9 ttl=128 time=0.640 ms
tes from 192.168.140.141: icmp_seq=10 ttl=128 time=0.614 ms
tes from 192.168.140.141: icmp_seq=11 ttl=128 time=0.504 ms
tes from 192.168.140.141: icmp_seq=12 ttl=128 time=0.563 ms
tes from 192.168.140.141: icmp_seq=13 ttl=128 time=0.481 ms
tes from 192.168.140.141: icmp_seq=14 ttl=128 time=0.586 ms
tes from 192.168.140.141: icmp_seq=15 ttl=128 time=0.525 ms
tes from 192.168.140.141: icmp_seq=16 ttl=128 time=0.579 ms
tes from 192.168.140.141: icmp_seq=17 ttl=128 time=0.549 ms
tes from 192.168.140.141: icmp_seq=18 ttl=128 time=0.571 ms
tes from 192.168.140.141: icmp_seq=19 ttl=128 time=0.641 ms
tes from 192.168.140.141: icmp_seq=20 ttl=128 time=0.509 ms
tes from 192.168.140.141: icmp_seq=21 ttl=128 time=0.601 ms
tes from 192.168.140.141: icmp_seq=22 ttl=128 time=0.526 ms
```

L'exécutable de macchanger se trouve habituellement dans le dossier /usr/bin.



Si deux machines d'un même réseau partagent la même adresse MAC, cela peut entraîner des conflits, provoquer une instabilité du réseau ou rendre certaines machines inaccessibles.

Problèmes de sécurité :

Modifier une adresse MAC peut être utilisé pour contourner des mécanismes de contrôle d'accès réseau basés sur les adresses MAC.

Cette pratique peut également servir à dissimuler l'identité d'un attaquant lors d'activités malveillantes sur un réseau.

Risques de détection :

Des systèmes de détection d'intrusion ou des outils comme arpwatch peuvent identifier des modifications non autorisées d'adresses MAC.

Enjeux liés à l'utilisation de macchanger sous Kali Linux :

Changer une adresse MAC peut entraîner des conflits sur le réseau, poser des problèmes de sécurité et augmenter les risques de détection.

Voici des mesures pour réduire ces risques :

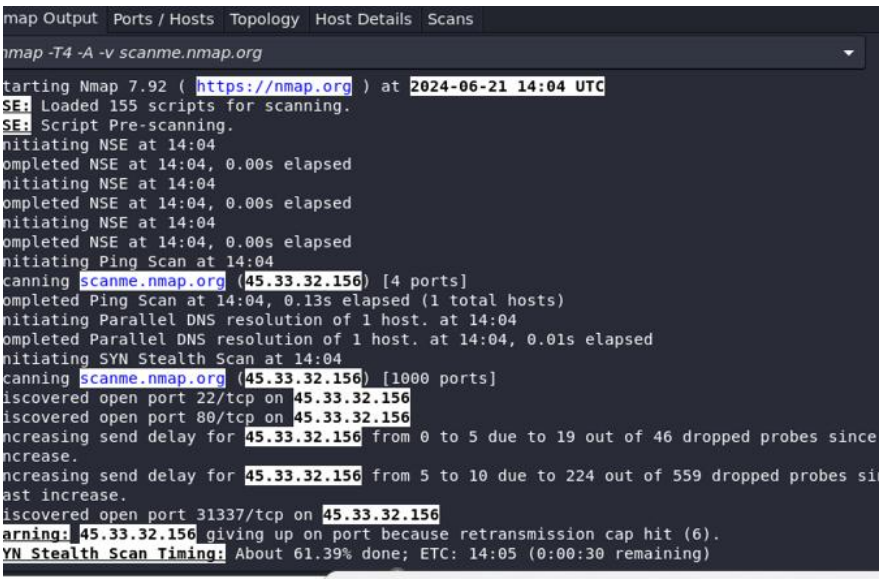
Mesures de protection :

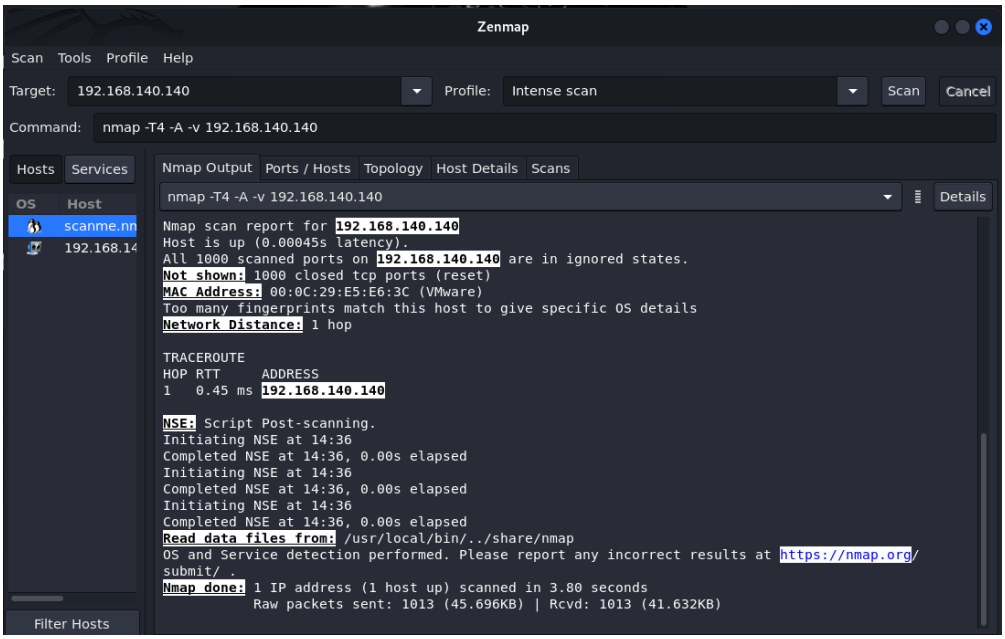
Utiliser des adresses MAC uniques : Évitez les conflits en sélectionnant des adresses MAC qui ne sont pas déjà utilisées sur le réseau.

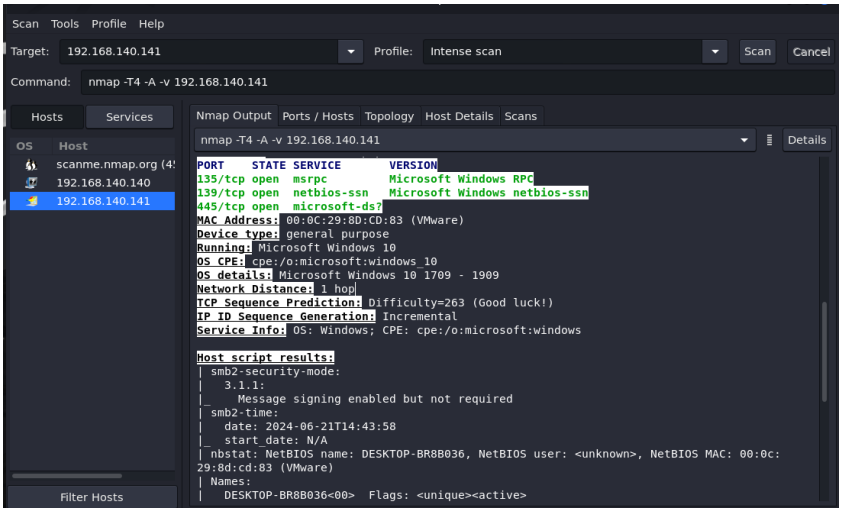
Surveillez les changements : Employez des outils comme arpwatch pour suivre les modifications des adresses MAC.

Configurer des contrôles d'accès : Implémentez des listes blanches sur les équipements réseau pour limiter les connexions aux appareils autorisés.

Ces précautions permettent de minimiser les impacts potentiels liés à la modification des adresses MAC.




Zenmap
Scan Tools Profile Help
Target: 192.168.140.140
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 192.168.140.140
Hosts
Services
OS
Host
scanme.nn
192.168.14
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v 192.168.140.140
Details
Nmap scan report for 192.168.140.140
Host is up (0.00045s latency).
All 1000 scanned ports on 192.168.140.140 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:0C:29:E5:E6:3C (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
TRACEROUTE
HOP RTT ADDRESS
1 0.45 ms 192.168.140.140
NSE: Script Post-scanning.
Initiating NSE at 14:36
Completed NSE at 14:36, 0.00s elapsed
Initiating NSE at 14:36
Completed NSE at 14:36, 0.00s elapsed
Initiating NSE at 14:36
Completed NSE at 14:36, 0.00s elapsed
Read data files from: /usr/local/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.80 seconds
Raw packets sent: 1013 (45.696KB) | Rcvd: 1013 (41.632KB)
Filter Hosts


Scan Tools Profile Help
Target: 192.168.140.141
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 192.168.140.141
Hosts
Services
OS
Host
scanme.nmap.org (4
192.168.140.140
192.168.140.141
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v 192.168.140.141
Details
PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds?
MAC Address: 00:0C:29:8D:CD:83 (VMware)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 1909
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Host script results:
| smb2-security-mode:
| 3.1.1:
|_ Message signing enabled but not required
| smb2-time:
| date: 2024-06-21T14:43:58
|_ start_date: N/A
| nbstat: NetBIOS name: DESKTOP-BR8B036, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:
29:8d:cd:83 (VMware)
| Names:
| DESKTOP-BR8B036<00> Flags: <unique><active>
Filter Hosts