HAMDI REDOUTE AMGHAR GR:9

LOCQMEN MAXIME MOURAD

JALON 3

07 Juin 2023

Copie d'écran de la fenêtre terminal « metasploit » avec la liste de l'ensemble des services identifiés suite à la commande msf6 > services.

```
msf6 > services
Services
========

host            port  proto  name  state  info
----            ----  -----  ----  -----  ----
192.168.99.1    22    tcp    ssh   open
192.168.99.1    53    tcp    dns   open
192.168.99.1    53    udp    dns   open
192.168.99.1    67    udp          open
192.168.99.1    139   tcp    smb   open
192.168.99.1    445   tcp    cifs  open
192.168.99.1    901   tcp          open
192.168.99.1    8080  tcp          open
192.168.99.7    22    tcp    ssh   open
192.168.99.7    139   tcp    smb   open
192.168.99.7    445   tcp    cifs  open
192.168.99.7    901   tcp          open
192.168.99.7    8080  tcp          open
192.168.99.10   22    tcp    ssh   open
192.168.99.10   53    tcp    dns   open
192.168.99.10   53    udp    dns   open
192.168.99.10   80    tcp          open
192.168.99.10   139   tcp    smb   open
```

```
192.168.99.10  445   tcp   cifs  open
192.168.99.10  901   tcp         open
192.168.99.10  8080  tcp         open
192.168.99.13  22    tcp   ssh   open
192.168.99.13  80    tcp         open
192.168.99.13  139   tcp   smb   open
192.168.99.13  445   tcp   cifs  open
192.168.99.13  901   tcp         open
192.168.99.13  8080  tcp         open
192.168.99.18  22    tcp   ssh   open
192.168.99.18  25    tcp         open
192.168.99.18  139   tcp   smb   open
192.168.99.18  143   tcp         open
192.168.99.18  445   tcp   cifs  open
192.168.99.18  901   tcp         open
192.168.99.18  8080  tcp         open
```

Copie d'écran de la fenêtre terminal « metasploit » avec la liste des cve du port 53.

```
msf6 > vulns -p 53

Vulnerabilities
===============

Timestamp            Host          Name                                                  References
---------            ----          ----                                                  ----------
2023-06-07 07:23:01 UTC  192.168.99.1   DNS Server Zone Transfer Information Disclosure (AXFR)          CVE-1999-0532,NSS-10595
2023-06-07 07:23:02 UTC  192.168.99.1   DNS Server BIND version Directive Remote Version Detection  IAVT-0001-T-0583,NSS-10028
2023-06-07 07:23:03 UTC  192.168.99.1   DNS Server Version Detection          IAVT-0001-T-0937,NSS-72779
2023-06-07 07:23:03 UTC  192.168.99.1   DNS Server hostname.bind Map Hostname Disclosure              NSS-35371
2023-06-07 07:23:03 UTC  192.168.99.1   DNS Server Detection          NSS-11002
2023-06-07 07:23:03 UTC  192.168.99.1   DNS Server Detection          NSS-11002
2023-06-07 07:23:11 UTC  192.168.99.10  DNS Server Zone Transfer Information Disclosure (AXFR)          CVE-1999-0532,NSS-10595
```

2023-06-07 07:23:12 UTC 192.168.99.10 DNS Server BIND version Directive Remote Version Detection IAVT-0001-T-0583,NSS-10028
2023-06-07 07:23:12 UTC 192.168.99.10 DNS Server Version Detection IAVT-0001-T-0937,NSS-72779
2023-06-07 07:23:12 UTC 192.168.99.10 DNS Server hostname.bind Map Hostname Disclosure NSS-35371
2023-06-07 07:23:12 UTC 192.168.99.10 DNS Server Detection NSS-11002
2023-06-07 07:23:12 UTC 192.168.99.10 DNS Server Detection NSS-11002

Copie d'écran de la fenêtre terminal « metasploit » avec la liste des exploits possibles en lien avec le ou les cve détectés.

msf6 > search CVE-1999-0532

Matching Modules
==========

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/gather/enum_dns		normal	No	DNS Record Scanner and Enumerator

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/gather/enum_dns

Pour obtenir plus d'exploit il faut juste changer le nom du CVE.