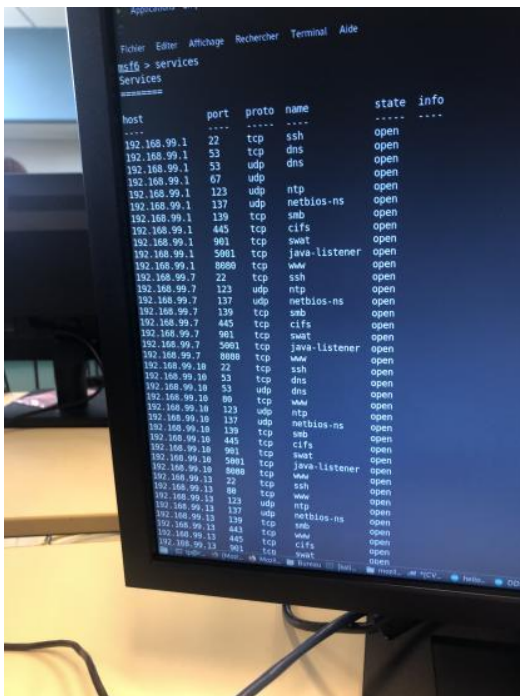
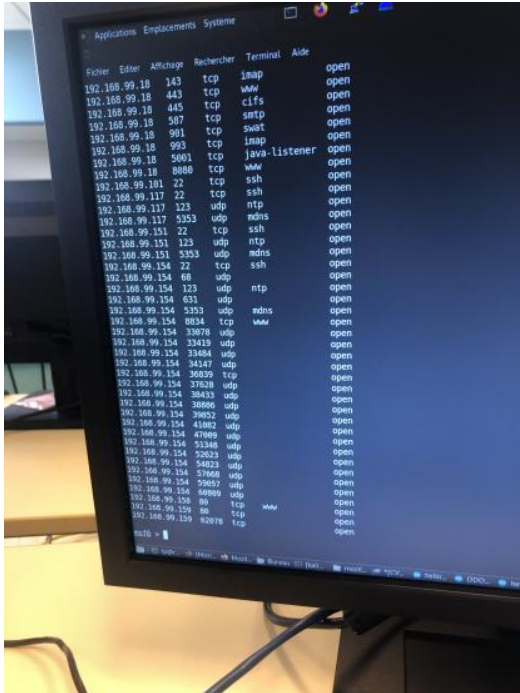


Jalon 3 :

- Le rapport d'audit fait par Nessus :

Le rapport est disponible en format txt sous ce lien : <https://we.tl/t-DfvqSf5h1A>

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



Le fichier en format txt est disponible sous ce lien : <https://we.tl/t-Q8bBrL3IYZ>

- 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
-----
2022-06-08 15:38:21 UTC 192.168.99.10 Nessus SYN scanner NSS-11219
2022-06-08 15:38:22 UTC 192.168.99.1 DNS Server BIND version Directive Remote Version Detection IAVT-0001-T-0583,NSS-10028
2022-06-08 15:38:22 UTC 192.168.99.1 DNS Server Version Detection IAVT-0001-T-0937,NSS-72779
2022-06-08 15:38:23 UTC 192.168.99.1 DNS Server hostname.bind Map Hostname Disclosure NSS-35371
2022-06-08 15:38:23 UTC 192.168.99.1 DNS Server Detection NSS-11002
2022-06-08 15:38:23 UTC 192.168.99.1 DNS Server Detection NSS-11002
2022-06-08 15:38:23 UTC 192.168.99.1 Nessus SYN scanner NSS-11219
2022-06-09 06:31:01 UTC 192.168.99.10 DNS Server BIND version Directive Remote Version Detection IAVT-0001-T-0583,NSS-10028
2022-06-09 06:31:01 UTC 192.168.99.10 DNS Server Version Detection IAVT-0001-T-0937,NSS-72779
2022-06-09 06:31:01 UTC 192.168.99.10 DNS Server hostname.bind Map Hostname Disclosure NSS-35371
2022-06-09 06:31:01 UTC 192.168.99.10 DNS Server Detection NSS-11002
2022-06-09 06:31:01 UTC 192.168.99.10 DNS Server Detection NSS-11002
2022-06-09 11:26:06 UTC 192.168.99.10 DNS Server Zone Transfer Information Disclosure (AXFR) CVE-1999-0532,NSS-10595
2022-06-09 11:26:07 UTC 192.168.99.1 DNS Server Zone Transfer Information Disclosure (AXFR) CVE-1999-0532,NSS-10595
```

- Copie d'écran de la fenêtre terminal « metasploit » avec la liste des exploits possibles en lien avec le ou les CVE détectées :

```
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
```