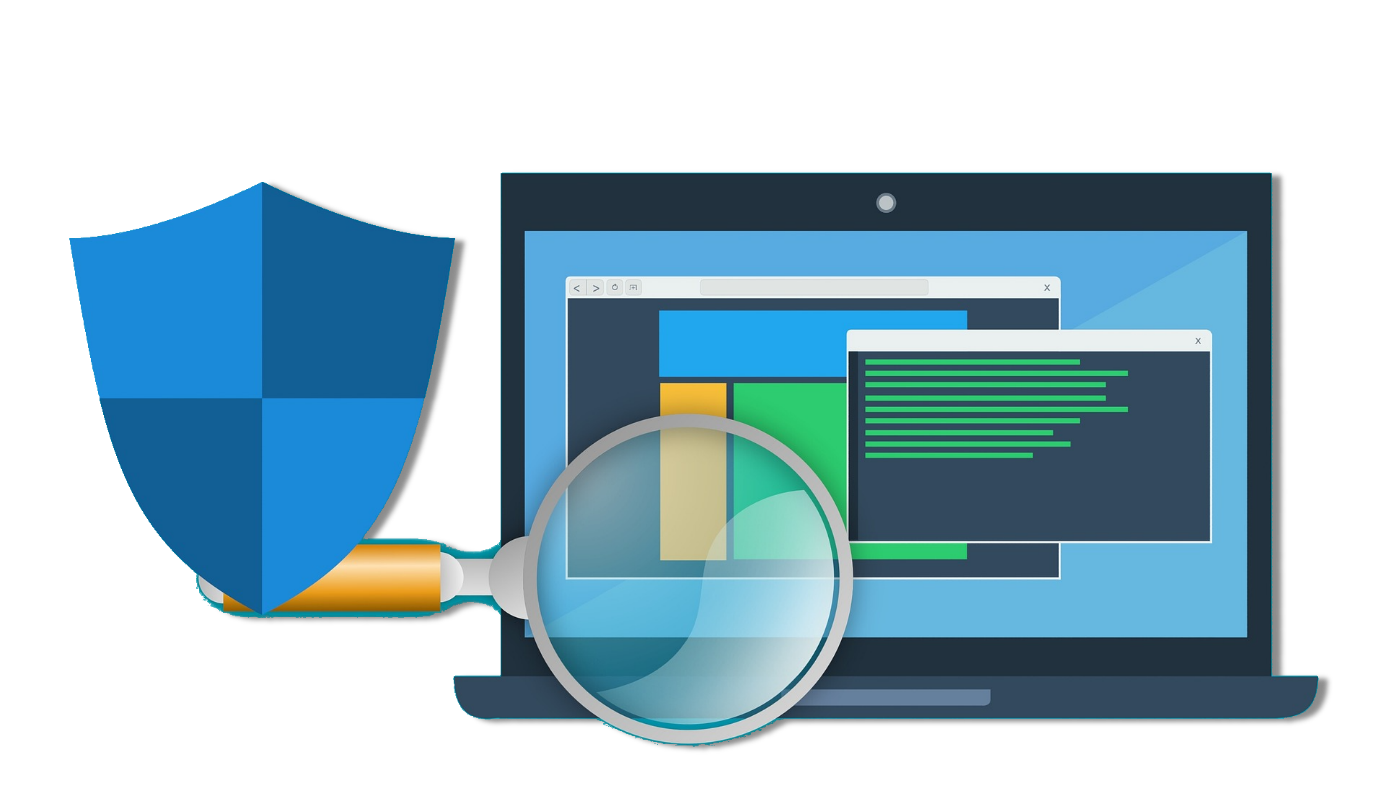
**Compte rendu**

**Semaine 18**



Réalisé par : Encadré par :

🌢 OTHMANE TAYBI 🌢 Mr. A.OMOR

NETWORK SCAN

And

ENUMERATION :

**🗹 NMAP :**

**🕉** NMAP alias Network Mapper est un outil open-source et très polyvalent pour les administrateurs système/réseau Linux. NMAP est utilisé pour explorer les réseaux, effectuer des analyses de sécurité, des audits de réseau et trouver des ports ouverts sur une machine distante. Il recherche les hôtes en direct, les systèmes d'exploitation, les filtres de paquets et les ports ouverts exécutés sur des hôtes distants.

**🗶** Utilisation de la commande NMAP :

root# nmap [Scan Type(s)] [Options] {target specification}

🌢 Installation NMAP sous Linux :

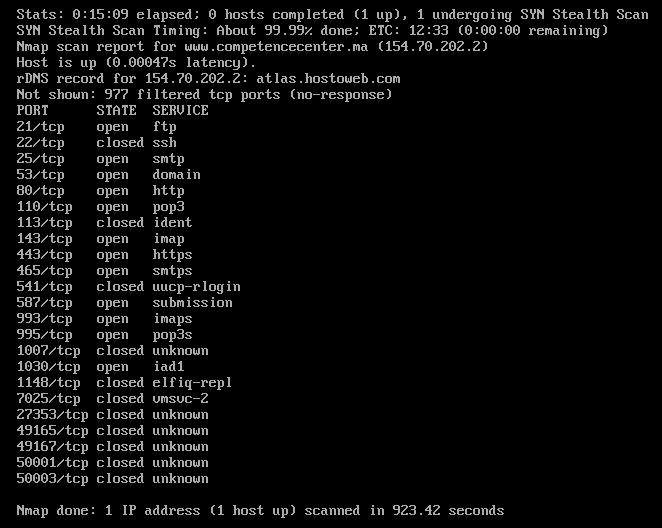
**🕉** Pour installerNMAP on taper la commande : sudo apt-get install nmap.

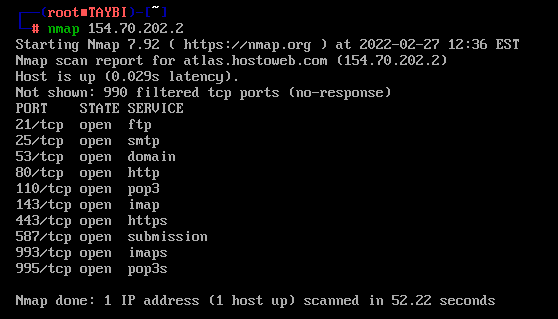
**🗹 Utilisation de la commande NMAP :**

🌢 Analyser un système avec le nom d'hôte et l'adresse IP :

**🕉** L'outil Nmap propose différentes méthodes pour analyser un système. Dans cet exemple, j'effectue une analyse en utilisant le nom d'hôte comme competencecenter.ma pour découvrir tous les ports, services et adresses MAC ouverts sur le système

 🌢 Scaner à l'aide du nom d'hôte :

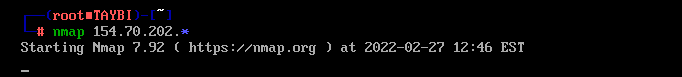


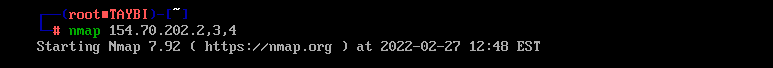
 🌢 Scaner à l'aide de l'adresse IP :

 🌢 Scaner plusieurs hôtes :

🌢 Scaner tout un sous-réseau :

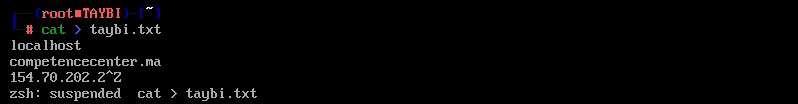
Pour analyser un sous-réseau entier ou une plage d'adresses IP en taper Nmap en fournissant le caractère générique \*.



🌢 Scaner plusieurs serveurs en utilisant le dernier octet de l'adresse IP :

🌢 Scaner la liste des hôtes à partir d'un fichier :

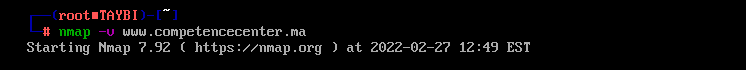
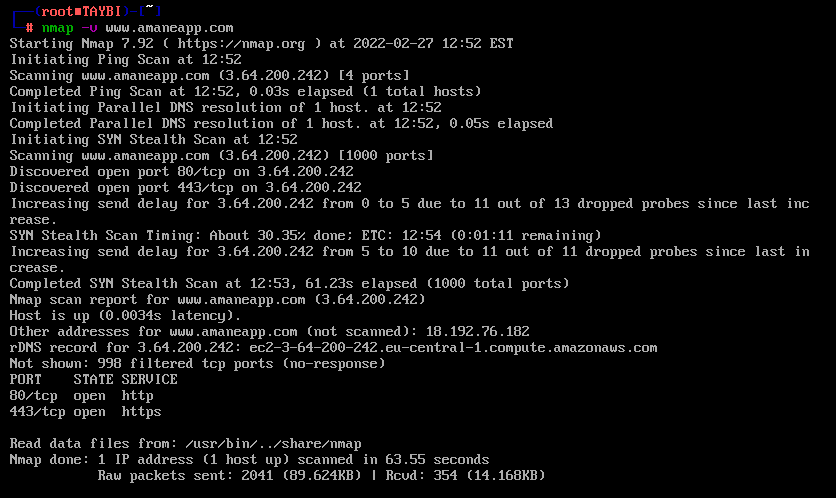
Si vous avez plus d'hôtes à analyser et que tous les détails de l'hôte sont écrits dans un fichier, vous pouvez directement demander à nmap de lire ce fichier et d'effectuer des analyses. Voyons comment faire cela.

On Crée un fichier texte qui s’appelé "taybi.txt" et définissez toutes les adresses IP ou le nom d'hôte du serveur que vous souhaitez analyser :

Ensuite, en taper la commande nmap avec l'option "iL" avec là pour analyser toutes les adresses IP répertoriées dans le fichier :

🌢 Analyser en utilisant des options :

🌢 Scaner en utilisant l'option "-v" :

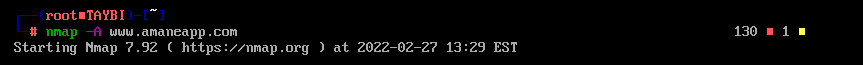
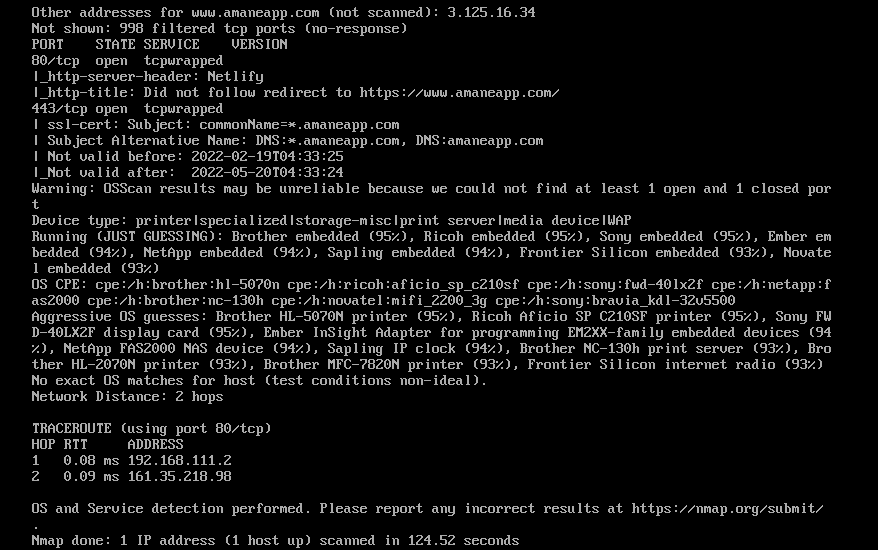
 la commande NMAP avec l'option "-v" donne des informations plus détaillées sur la machine distante

🌢 Analyser le réseau en excluant les hôtes distants :

En peux exclure certains hôtes lors d'une analyse complète du réseau ou lorsque vous analysez avec des caractères génériques avec l'option

"–exclude" :

🌢 Scaner les informations du système d'exploitation et Traceroute :

**🙟** Avec Nmap, vous pouvez détecter quel système d'exploitation et quelle version s'exécutent sur l'hôte distant. Pour activer la détection du système d'exploitation et de la version, l'analyse des scripts et le traceroute, nous pouvons utiliser l'option "-A" .

**🙟** Dans la sortie ci-dessus, vous pouvez voir que nmap est fourni avec l'empreinte TCP/IP du système d'exploitation s'exécutant sur des hôtes distants et étant plus précis sur le port et les services s'exécutant sur les hôtes distants.

🌢 Nous avons plusieurs options de la commande NMAP pour voir taper nmap --help



🌢 About Zenmap :

**Zenmap** **{ Nmap GUI }** est l'interface utilisateur graphique du scanner de sécurité Nmap et propose des centaines d'options. Il permet aux utilisateurs de faire des choses comme enregistrer des analyses et les comparer, afficher des cartes de topologie de réseau, afficher des affichages de ports exécutés sur un hôte ou tous les hôtes d'un réseau et stocker des analyses dans une base de données consultable.

🌢 Le BUT :

🌢 Hacking :

Bien que l'analyse des ports en soi ne soit pas illégale, les fonctionnalités de Nmap sont certainement utiles aux pirates malveillants qui recherchent des vulnérabilités à exploiter. Certaines utilisations du logiciel, en particulier sans autorisation, peuvent vous faire virer ou avoir des ennuis juridiques, même si vous effectuez une analyse de vulnérabilité à des fins bénignes.

il est toujours préférable de faire approuver vos analyses par les personnes appropriées de votre organisation

🌢 Protection :

finding open ports and detecting security risks.