Année 2023-2024

SAÉ Cyber 4.0 Sécurisation d'un SI

Tâche 7 Utilisation de scanneurs de vulnérabilité (13,5 points)

Liste des personnes impliquées avec pourcentage de répartition	

Estimation du temps passé sur cette tâche en heure-homme :

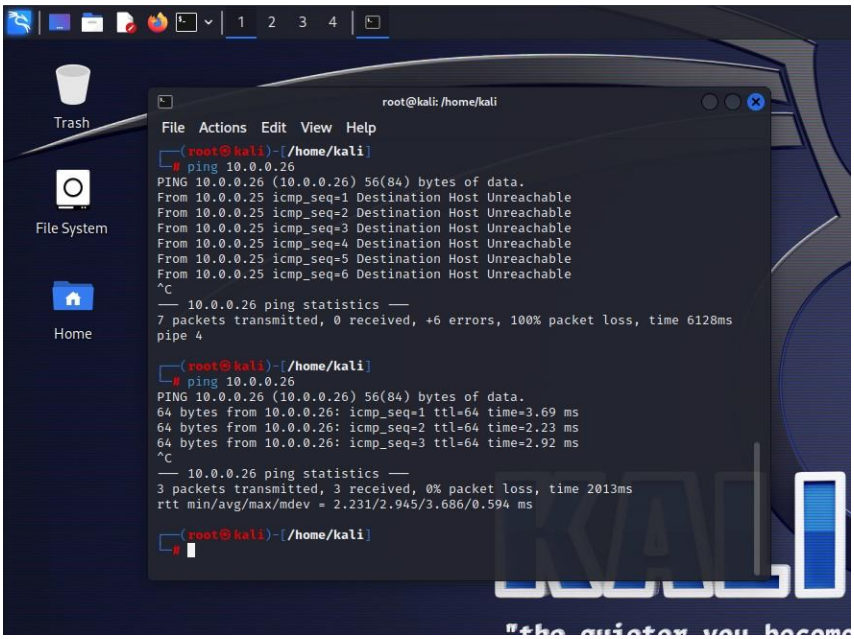
Objectif : Réaliser plusieurs évaluations de la sécurité des serveurs

Installez dans la DMZ une machine/VM metasploitable :

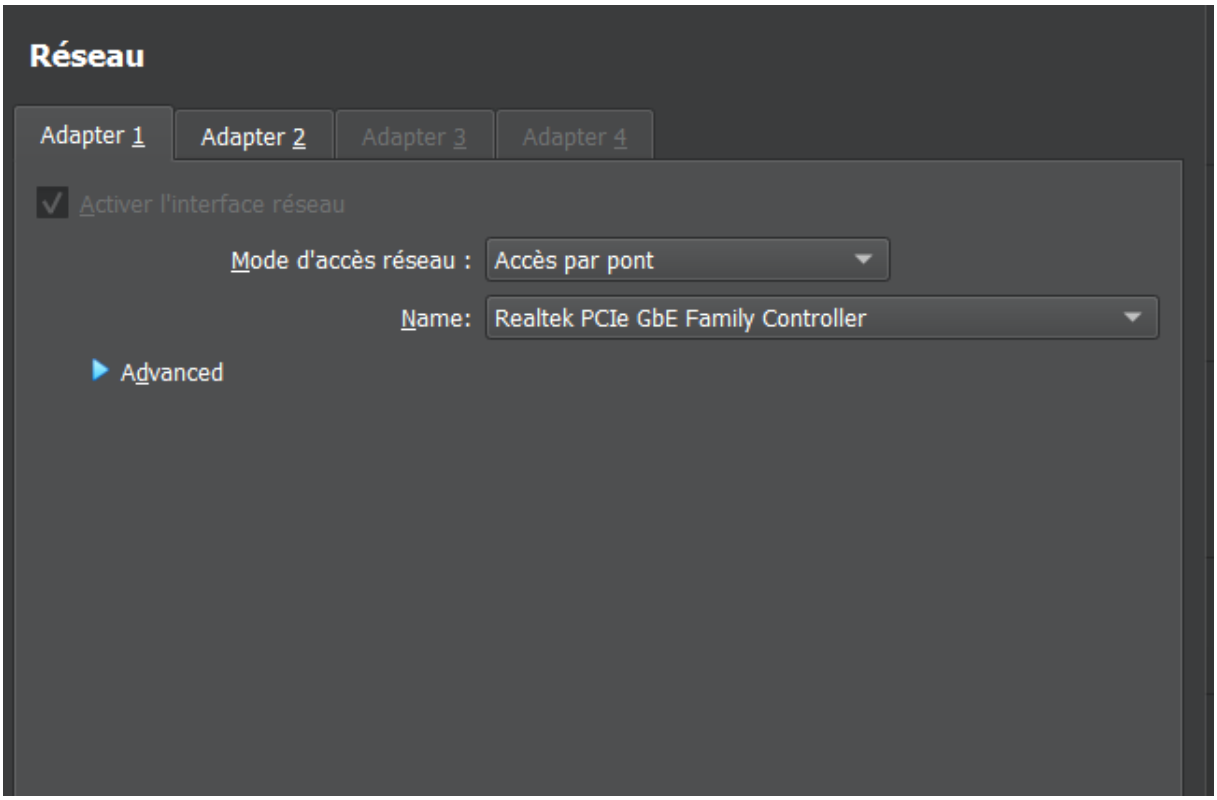
Dans le cadre de notre projet, nous avons opté pour l'utilisation de VirtualBox afin de créer des environnements simulés sur l'ordinateur. Au sein de VirtualBox, nous avons configuré deux espaces de travail virtuels sur 2 machines physiques différentes. Le premier espace est dédié à l'utilisation du programme Métasploit, conçu pour détecter les failles dans les systèmes informatiques. Le second espace est fondé sur Kali Linux, un système d'exploitation regorgeant d'outils dédiés à tester la sécurité des réseaux informatiques.

```
Not enough information: "dev" argument is required.
bash: 26/24: No such file or directory
root@metasploitable:/etc# ip addr add 10.0.0.26/24 dev eth0
root@metasploitable:/etc# ip addr del 192.168.2.254/24 dev eth0
root@metasploitable:/etc# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:ae:f9:31 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.26/24 scope global eth0
    inet6 fe80::a00:27ff:feae:f931/64 scope link
       valid_lft forever preferred_lft forever
root@metasploitable:/etc# ping 10.0.0.25
PING 10.0.0.25 (10.0.0.25) 56(84) bytes of data.
64 bytes from 10.0.0.25: icmp_seq=1 ttl=64 time=2.91 ms
64 bytes from 10.0.0.25: icmp_seq=2 ttl=64 time=2.62 ms
64 bytes from 10.0.0.25: icmp_seq=3 ttl=64 time=3.35 ms

--- 10.0.0.25 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 2.622/2.960/3.350/0.305 ms
root@metasploitable:/etc#
```



Après avoir installé Métasploit sur les machines virtuelles, j'ai procédé à la configuration des connexions réseau. Tout d'abord, j'ai connecté un câble Ethernet à notre réseau situé dans la DMZ. Ensuite, j'ai mis en place deux interfaces réseau. Pour la première, appelée "adapter 1", j'ai sélectionné le mode NAT afin de garantir un accès à Internet, ce qui sera utile pour télécharger des paquets supplémentaires à l'avenir. Pour la seconde interface, "adapter 2", j'ai choisi une configuration en mode accès par pont (en mode bridge) permettant ainsi d'attribuer une adresse IP directement depuis le réseau externe. Cette configuration assure non seulement une connexion à Internet, mais aussi la communication entre les deux machines virtuelles.



Suite à cela j'ai effectué une update suivi d'une upgrade pour mettre mes paquets du système à jour. Après avoir finalisé les mises à jour, j'ai procédé à un test de connectivité en exécutant des pings entre les deux machines virtuelles afin de confirmer leur capacité à communiquer sans aucun obstacle. (résultat des pings foncctionnels entre les 2 vms sur les 2 premiers screens du rapport)

Installez et utilisez SCNR :

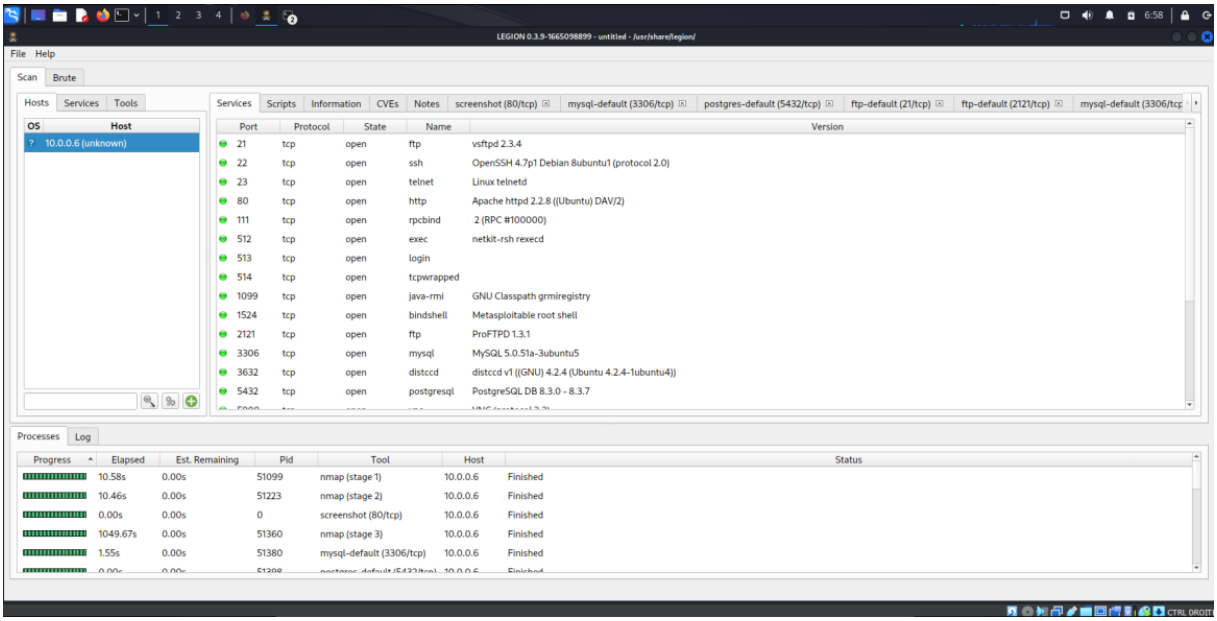
Pour installer SCNR, nous avons consulté le dépôt GitHub contenant le script d'installation. Une fois le script récupéré, nous avons ajusté les permissions nécessaires pour permettre son exécution. Après cela, une série de tests a été lancée sur notre installation préexistante de Metasploit. Bien que le processus de scan devait initialement durer 22 heures selon les informations fournies, il a été interrompu après seulement une heure, cette période étant jugée suffisante pour recueillir les données nécessaires à une analyse préliminaire des résultats.

Installez et utilisez Legion :

Legion est un outil d'automatisation de réseaux et de tests de pénétration qui simplifie le processus de découverte et d'exploitation des réseaux. Il s'agit d'un framework qui intègre plusieurs outils de scan tels que nmap, screenshot etc.. , et de bruteforce. Voici comment l'utiliser typiquement :
Sur Kali Linux, Legion est préinstallé, ce qui facilite son utilisation. Il vous suffit de saisir la commande **legion** dans le terminal pour le lancer. L'interface graphique s'ouvre, présentant divers onglets tels que "Hosts", "Services", "Tools", et plus encore. Pour débuter un scan, vous pouvez cliquer sur le bouton **+** afin d'ajouter l'adresse IP de la cible, dans ce cas celle associée à une instance Metasploit. En lançant le scan, Legion procède à une série de tests visant à identifier les services en cours d'exécution, les ports ouverts, les vulnérabilités potentielles, etc.

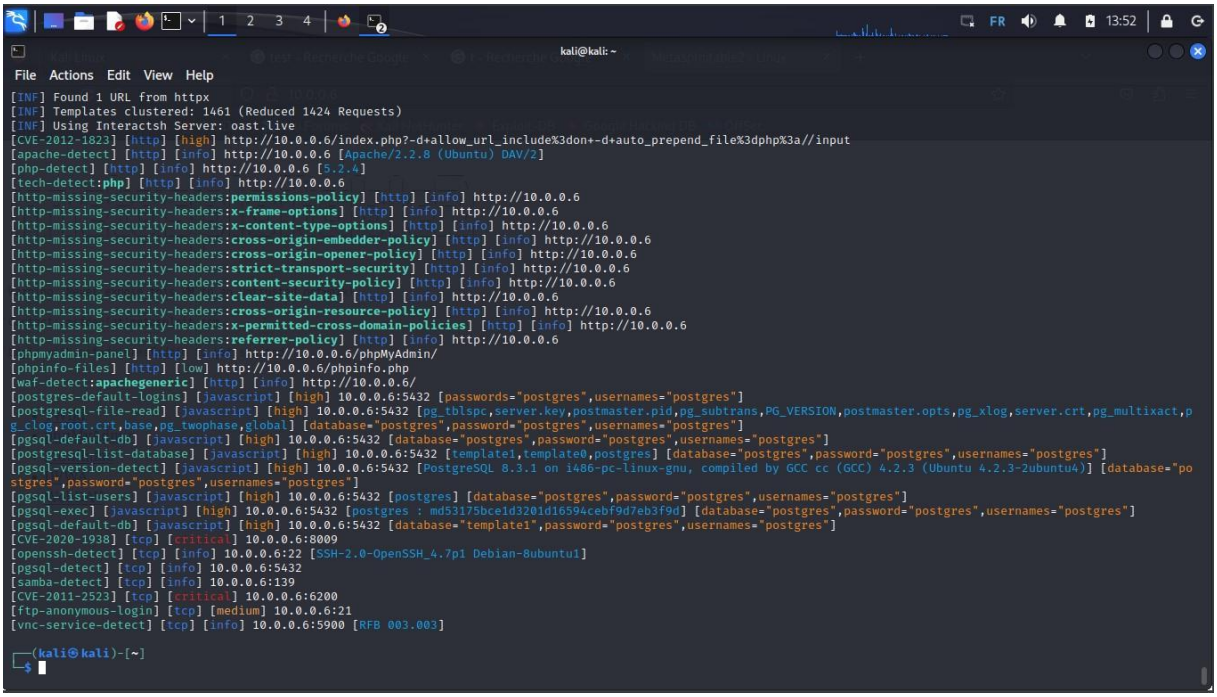
Les résultats du scan sont ensuite enregistrés dans notre vm (dossier root). Ces résultats peuvent contenir des informations précieuses telles que des configurations de service mal sécurisées, des vulnérabilités spécifiques à certaines versions de logiciels, et des vecteurs potentiels d'attaque. En pratique, Legion facilite l'organisation et l'automatisation des phases

initiales d'un pentest, ce qui réduit le temps nécessaire pour collecter des données et permet à l'utilisateur de se concentrer sur l'interprétation des résultats et les étapes suivantes du processus de test.



Installez et utilisez Nuclei :

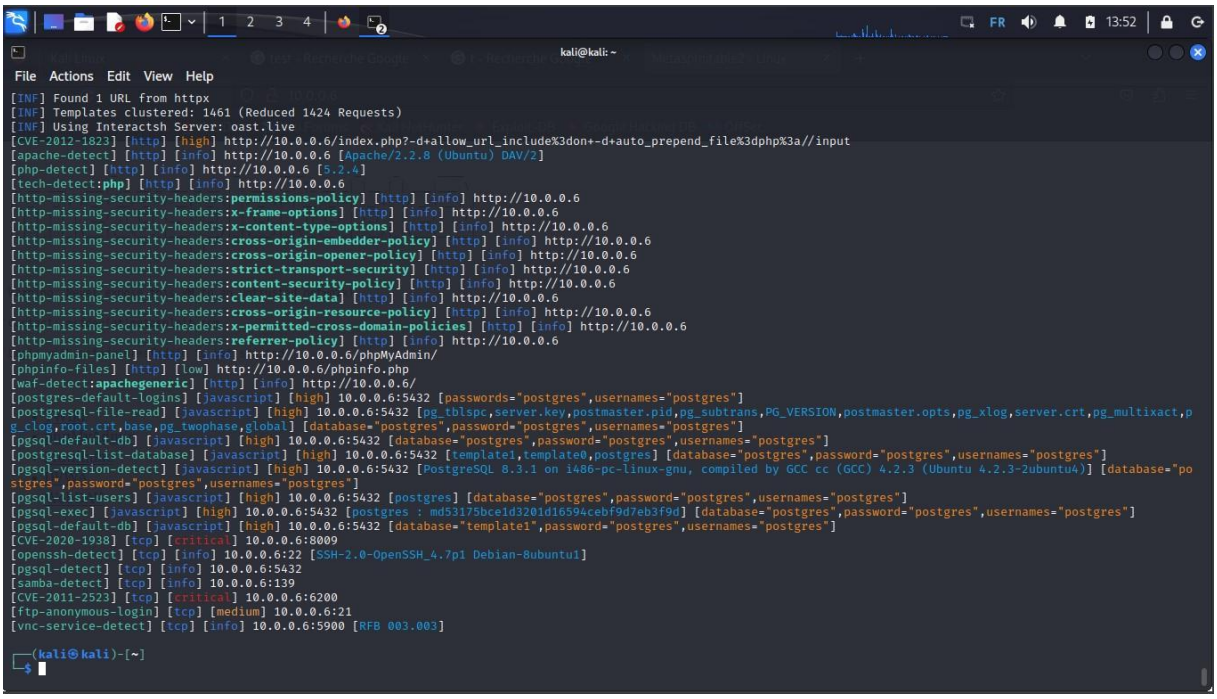
À l'origine, Nuclei n'était pas inclus dans Kali Linux. Cependant, après avoir saisi "nuclei" dans le terminal, il a été recommandé de l'installer, ce que nous avons donc fait.



Après son installation, Nuclei a été utilisé pour effectuer un scan sur une adresse IP. Ce scan a mis en lumière plusieurs problèmes potentiels, tels que des en-têtes de sécurité HTTP manquants, des versions obsolètes de serveur Web, ainsi que des lacunes dans la politique de sécurité du contenu. Ces résultats se révèlent précieux pour identifier les vulnérabilités d'un système et déterminer les mesures de sécurité à mettre en place afin de renforcer le serveur contre d'éventuelles attaques. Ils permettent également de prioriser les correctifs et les mises à jour de sécurité nécessaires.

Installez et utilisez Nikto :

Nikto est également inclus d'origine dans Kali Linux. J'ai exécuté la commande "nikto -h 10.0.0.6".

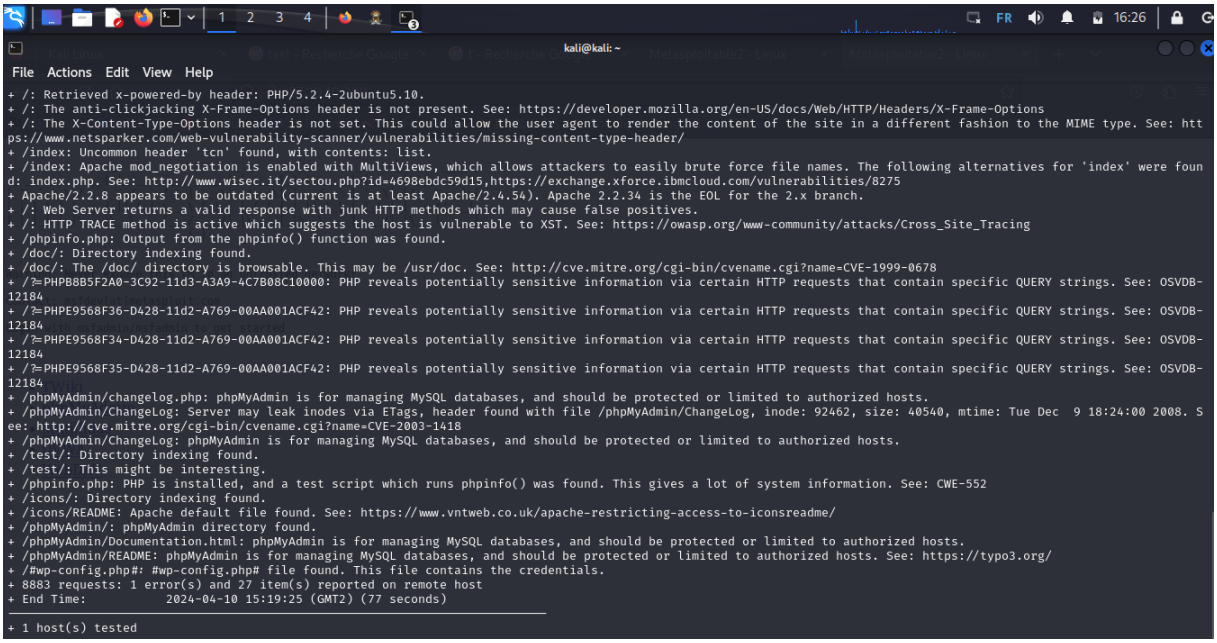


Placez les scanners dans la DMZ, puis à l'extérieur :

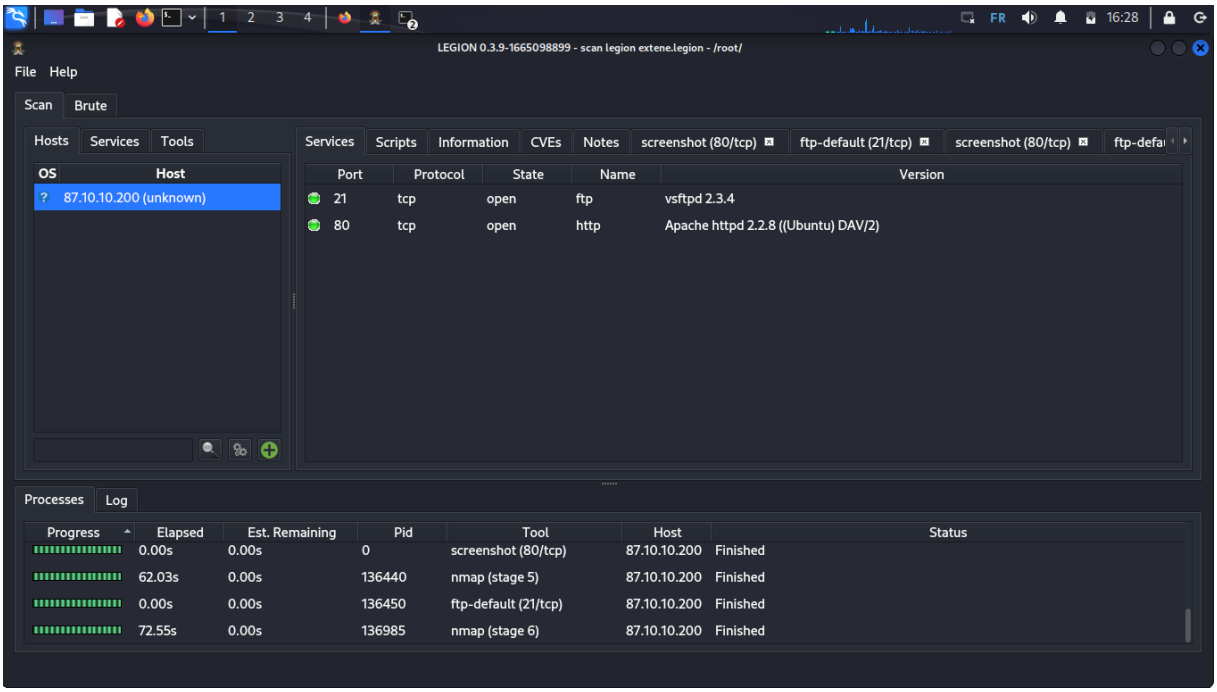
Scan Nikto :

Nikto a identifié plusieurs problèmes critiques, dont l'utilisation d'une version obsolète du serveur Apache (2.2.8), qui présente un risque accru en raison de l'absence de correctifs de sécurité. En outre, divers en-têtes HTTP manquants ont été détectés, laissant la porte ouverte à des attaques telles que le clickjacking et le cross-site scripting (XSS). Le scan a également signalé l'activation de la méthode TRACE HTTP, une configuration déconseillée en raison de son potentiel d'exposition d'informations sensibles.
Des problèmes de configuration, tels que l'indexation des répertoires et l'exposition de fichiers et de panneaux d'administration sensibles, ont été relevés, soulignant le risque d'accès non autorisé à des données confidentielles ou de compromission du système si ces éléments ne

sont pas correctement sécurisés.
En conclusion, le rapport de Nikto souligne l'urgence d'une révision approfondie de la configuration du serveur pour remédier à ces vulnérabilités. Cela inclut la désactivation des méthodes obsolètes ou dangereuses ainsi que la mise en œuvre des mesures de sécurité recommandées pour prévenir l'exploitation des faiblesses détectées.

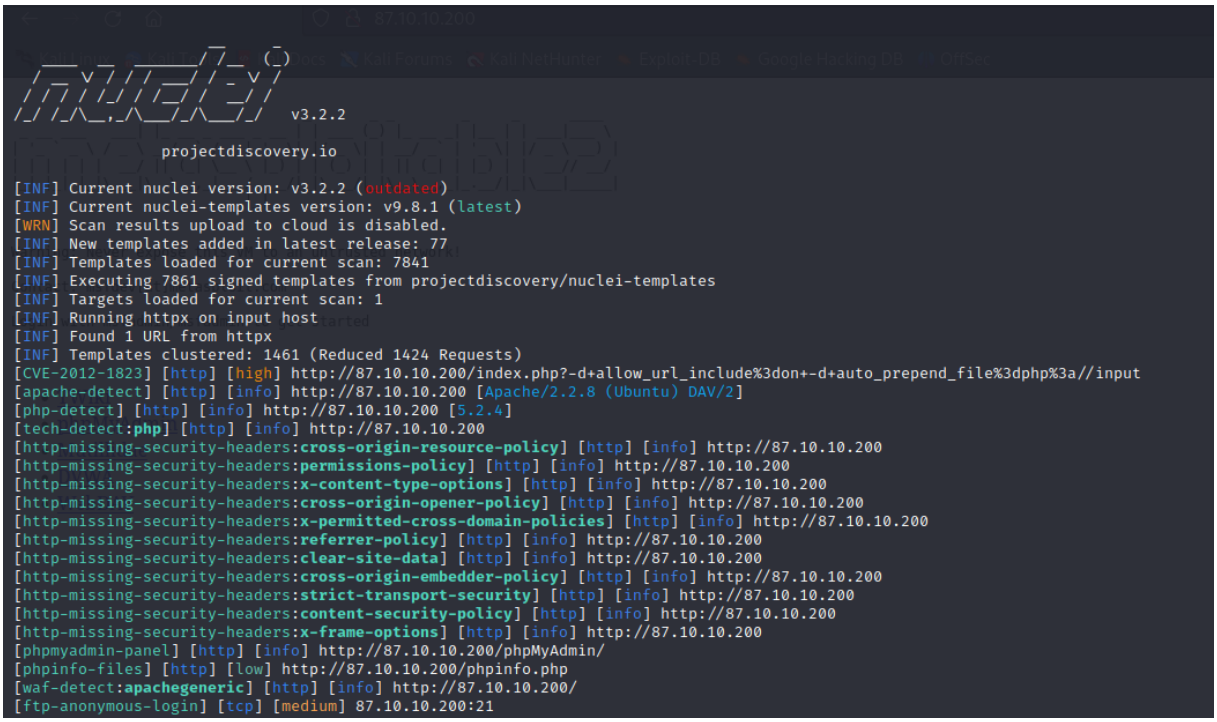


Pour ce faire, nous avons lancé Legion sur un système Kali Linux, déjà préinstallé, ne nécessitant aucune installation supplémentaire. Une fois l'outil démarré, nous avons pu facilement ajouter l'adresse IP de notre cible, 87.10.10.200, en utilisant le bouton ‘+’ disponible dans l'interface. Le scan s'est exécuté sans problème, passant méthodiquement en revue chaque service et port ouvert afin d'identifier toute vulnérabilité potentielle. Les ports suivants ont été détectés comme ouverts et fonctionnels : FTP (21/tcp), SSH (22/tcp), Telnet (23/tcp), SMTP (25/tcp), HTTP (80/tcp), et bien d'autres.
Les résultats obtenus avec Legion ont été soigneusement archivés en vue d'une analyse ultérieure, offrant ainsi une vue d'ensemble des configurations de services potentiellement non sécurisées, des vulnérabilités spécifiques à certaines versions de logiciel, et d'autres vecteurs d'attaque possibles. L'utilisation de Legion a grandement optimisé les premières étapes de notre test de pénétration, réduisant ainsi le temps nécessaire pour recueillir des données et permettant une concentration plus poussée sur l'interprétation des résultats ainsi que sur la planification des actions de sécurisati



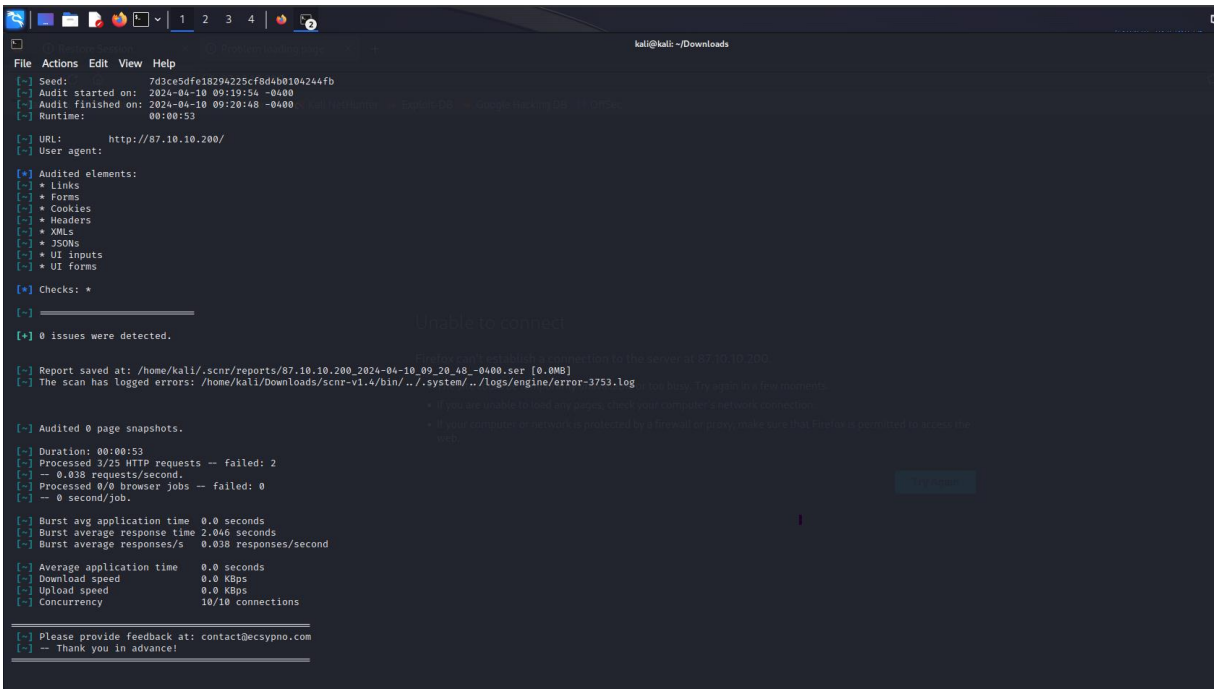
Scan Nuclei :

Le scan effectué avec Nuclei a révélé des lacunes dans les en-têtes de sécurité HTTP, incluant des en-têtes tels que X-Frame-Options, X-Content-Type-Options, et X-XSS-Protection, qui jouent un rôle critique dans la prévention de diverses attaques web telles que le clickjacking et le cross-site scripting. De plus, des failles ont été repérées dans les configurations des politiques de sécurité de contenu, ce qui accroît la surface d'attaque pour d'éventuels exploits.
Des informations concernant des versions obsolètes du serveur web Apache, ainsi que des services tels que SSH et Samba, ont été signalées, laissant entrevoir des potentiels vecteurs d'attaque. Nuclei a également mis en évidence la présence de panneaux d'administration phpMyAdmin accessibles, ce qui pourrait présenter un risque significatif si ces interfaces ne sont pas correctement sécurisées.



Scan SCNR :

Pour achever la dernière étape de cette sous-tâche, j'ai décidé d'utiliser deux ordinateurs distincts. Le premier a lancé un scan en ciblant l'adresse IP externe liée à notre environnement Metasploitable. Tout au long du processus, SCNR a exploré les URLs pertinentes, identifiant les éventuelles failles et vulnérabilités. Bien que cette tâche soit normalement conçue pour durer plusieurs heures afin de couvrir de manière exhaustive, j'ai préféré l'interrompre après une demi-heure. Ce laps de temps était suffisant pour obtenir un échantillon initial de données nécessaire à une évaluation préliminaire.
En comparant les résultats avec ceux du premier test, nous constatons des écarts significatifs en ce qui concerne les vulnérabilités détectées et la surface d'attaque potentielle. La capacité de SCNR à repérer des faiblesses dans des contextes réseau variés, qu'ils soient internes ou externes, a été mise en évidence, soulignant ainsi l'importance d'une approche stratifiée et multicouche en matière de sécurité informatique.


kali@kali: ~/Downloads
File Actions Edit View Help
[~] Seed: 7d3ce5dfe10294225cf8d4b0104244fb
[~] Audit started on: 2024-04-10 09:19:54 -0400
[~] Audit finished on: 2024-04-10 09:20:48 -0400
[~] Runtime: 00:00:53
[~] URL: http://87.10.10.200/
[~] User agent:
[*] Audited elements:
[~] * Links
[~] * Forms
[~] * Cookies
[~] * Headers
[~] * XMLs
[~] * JSONs
[~] * UI inputs
[~] * UI forms
[*] Checks: *
[~] ==========
[+] 0 issues were detected.
[~] Report saved at: /home/kali/.scnr/reports/87.10.10.200_2024-04-10_09_20_48_-0400.ser [0.0MB]
[~] The scan has logged errors: /home/kali/Downloads/scnr-v1.4/bin/../.system/../logs/engine/error-3753.log
[~] Audited 0 page snapshots.
[~] Duration: 00:00:53
[~] Processed 3/25 HTTP requests -- failed: 2
[~] -- 0.038 requests/second.
[~] Processed 0/0 browser jobs -- failed: 0
[~] -- 0 second/job.
[~] Burst avg application time 0.0 seconds
[~] Burst average response time 2.046 seconds
[~] Burst average responses/s 0.038 responses/second
[~] Average application time 0.0 seconds
[~] Download speed 0.0 KBps
[~] Upload speed 0.0 KBps
[~] Concurrency 10/10 connections
[~] Please provide feedback at: contact@ecsypno.com
[~] -- Thank you in advance!