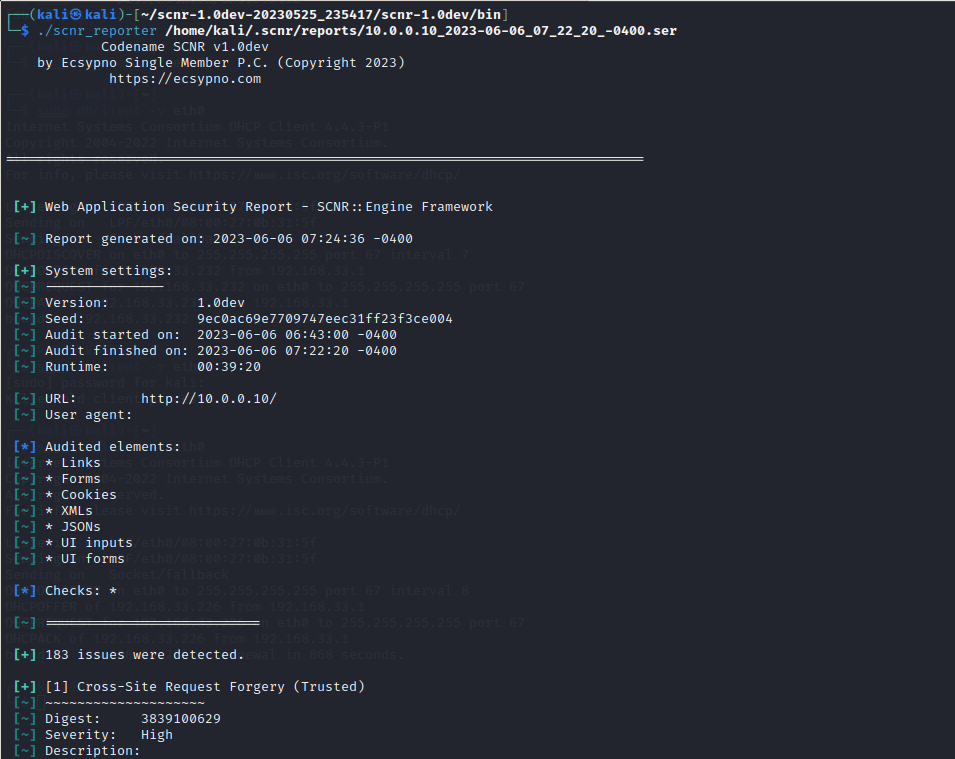
Rapport Scan

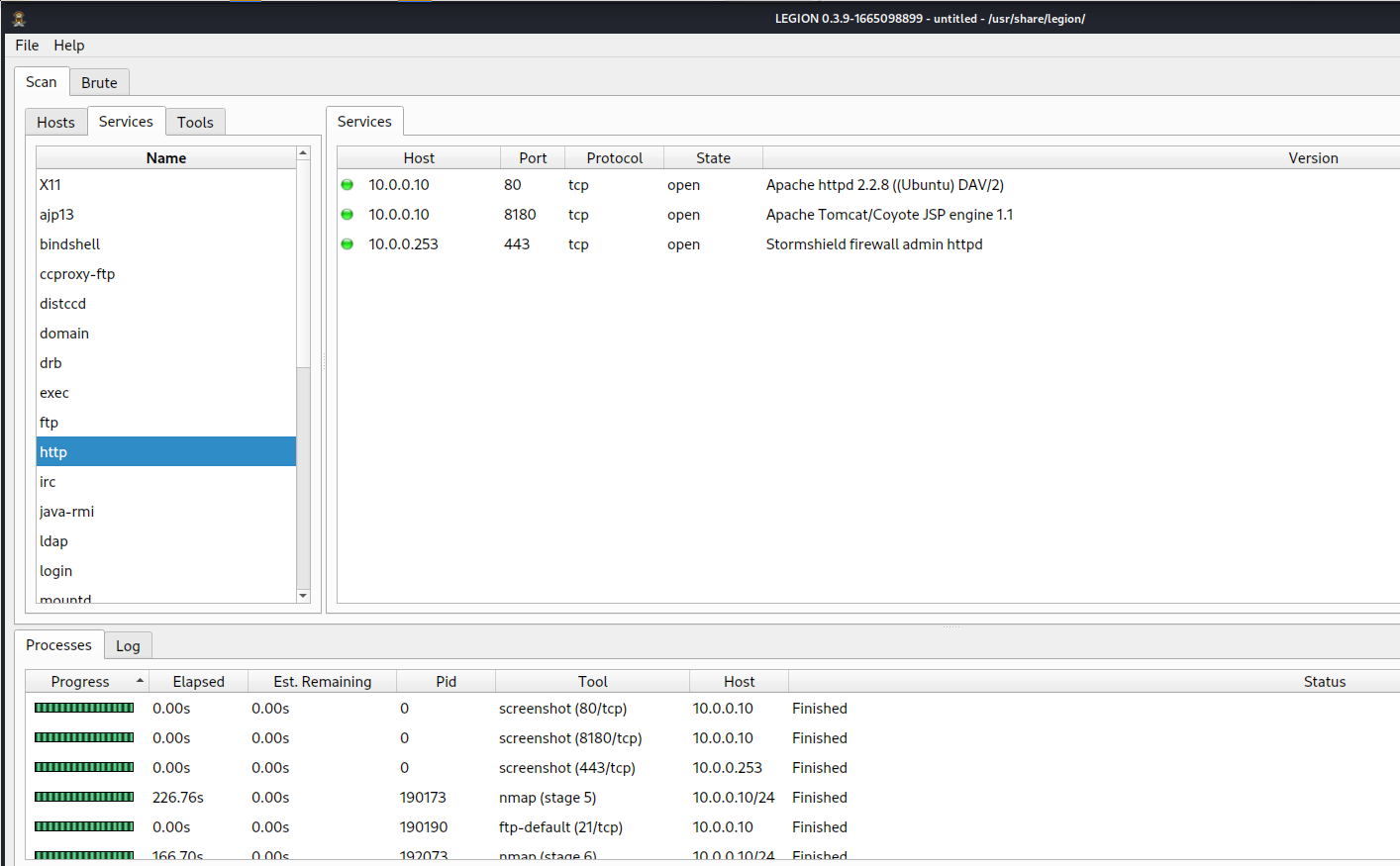
Pour cette partie, nous allons donc mettre en avant les scans de vulnérabilité sur le réseau. Cette mission consistait à effectuer des scans à la fois sur le réseau interne et le réseau externe de notre infrastructure. Pour ce faire, nous avons installé une machine virtuelle Metasploitable sur le port DMZ et utilisé un ensemble d'outils de numérisation, notamment Scnr escypno, Legion, Nuclei et Nikto. Ce rapport fournira une explication détaillée de notre méthodologie et des résultats obtenus sur la sécurité de la machine virtuelle qui est scanné.

Dans un premier temps, nous avons installé une machine virtuelle Metasploitable sur le port DMZ de notre pare feu. Cette machine virtuelle est conçue pour simuler un environnement vulnérable, offrant ainsi un scénario réaliste pour tester les capacités de notre scanner. Ensuite, nous avons branché notre scanner sur le réseau intérieur et lancé les scans à l'aide des logiciels Scnr escypno, Legion, Nuclei et Nikto.

- Scan SCNR intérieur :



Nous voyons que à la suite du scan, 183 issues ont été détecté par le scanner.

- Legion intérieur :

Une image contenant texte, logiciel, Icône d’ordinateur, affichage

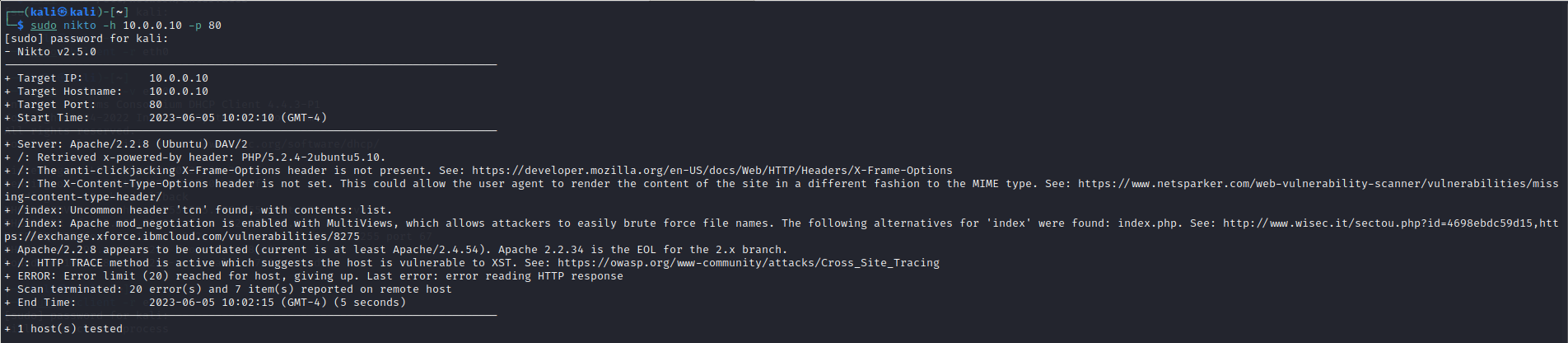
Description générée automatiquement

Nous voyons avec le scan Legion de nombreux ports scannés et ouverts, avec cela nous pouvons trouver par exemple des logins et des mots de passe comme sur la deuxième capture d’écran du scan Legion.

- Scan nuclei Une image contenant texte, capture d’écran, logiciel

Description générée automatiquement

Pour le scan Nuclei, nous pouvons apercevoir les différents ports scannés ainsi que quatre vulnérabilités qui sont « critical » avec un « medium ».

- Scan Nikto :

Nous pouvons voir à la ligne « Scan terminated » qu’il a trouvé 20 erreurs et 7 éléments

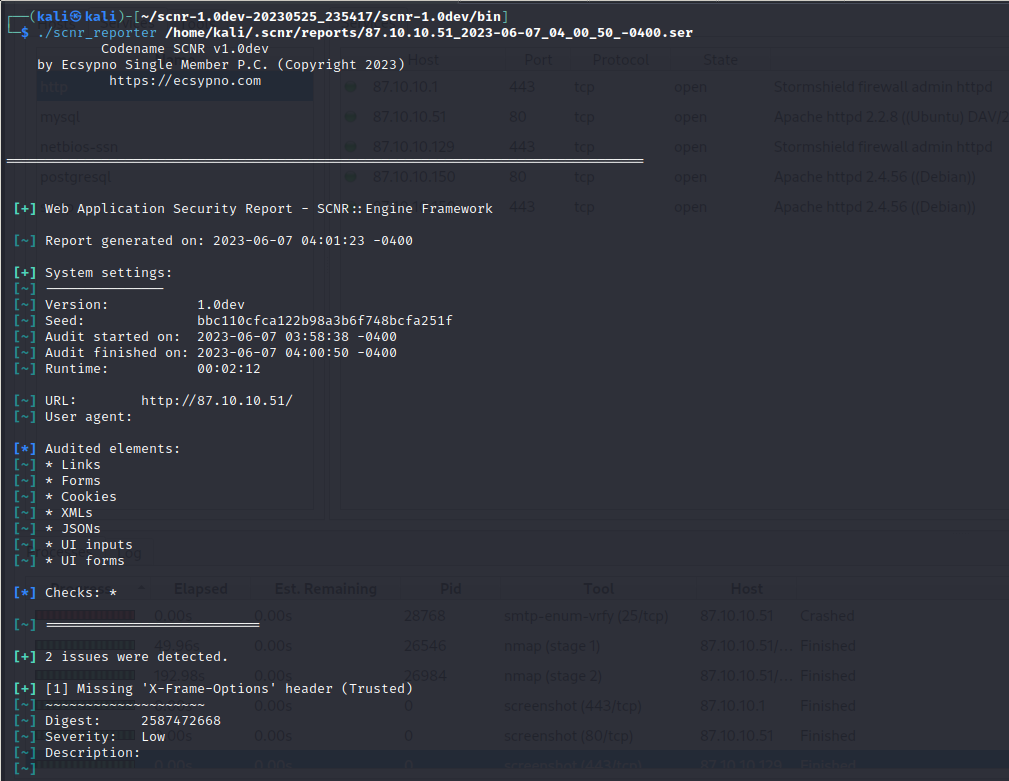
En analysant les résultats obtenus lors de ces scans internes, nous avons pu identifier les failles de sécurité spécifiques qui nécessitaient une attention immédiate.

Ensuite, nous avons branché notre scanner à l'extérieur du réseau pour effectuer à nouveau des scans mais à partir d'une perspective externe. Cela nous a permis de simuler une attaque provenant de l'extérieur et d'évaluer les changements observés en raison des filtres du pare-feu et des paramètres de sécurité supplémentaires.

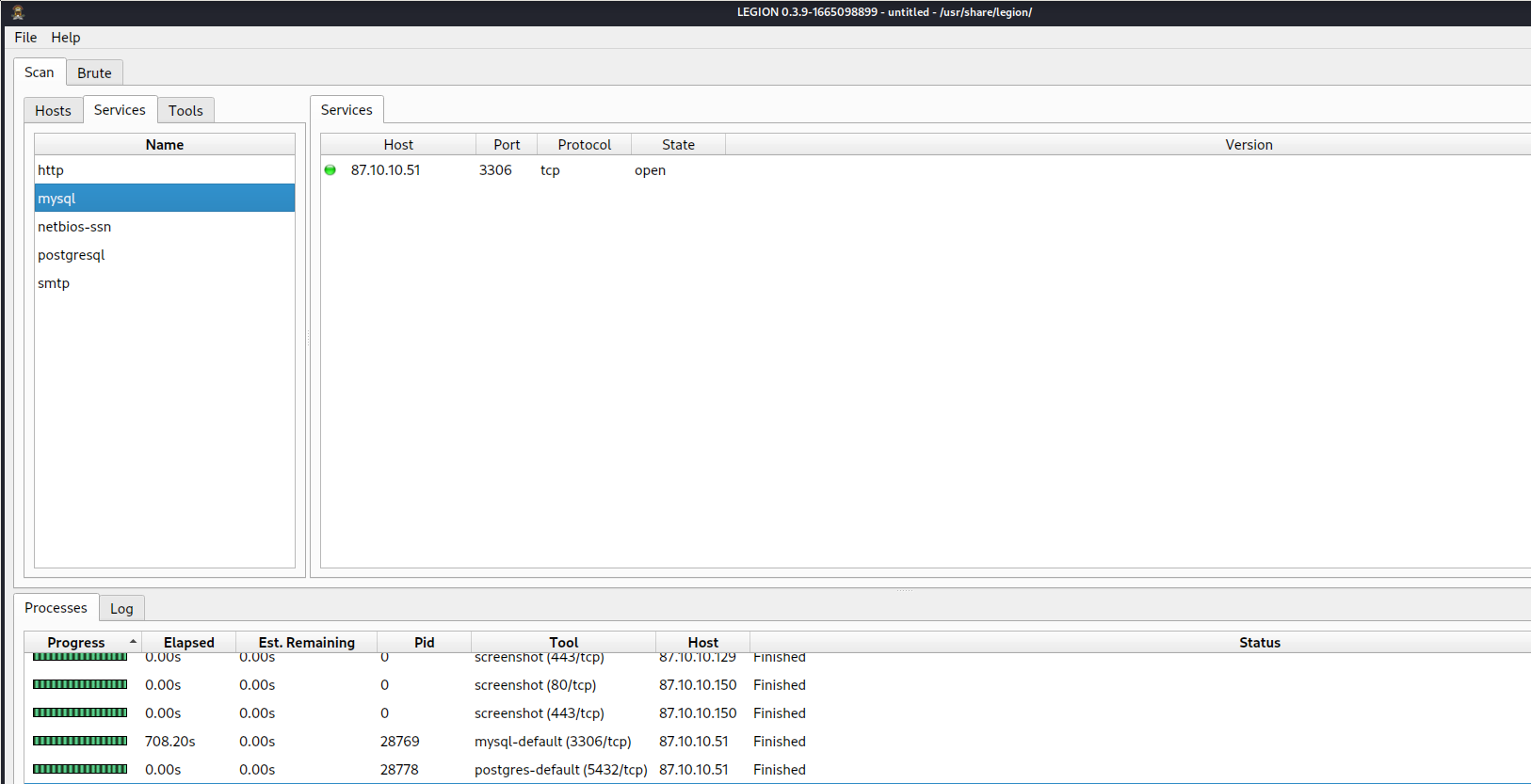
Voici la règle pour crée une NAT :

On indique en source l’ip privée du metasploitable auxquelles le réseau externe n’a pas accès et on met toutes les destinations sur l’interface out. Puis On ajoute une source dans les translations en mettant une IP publique.

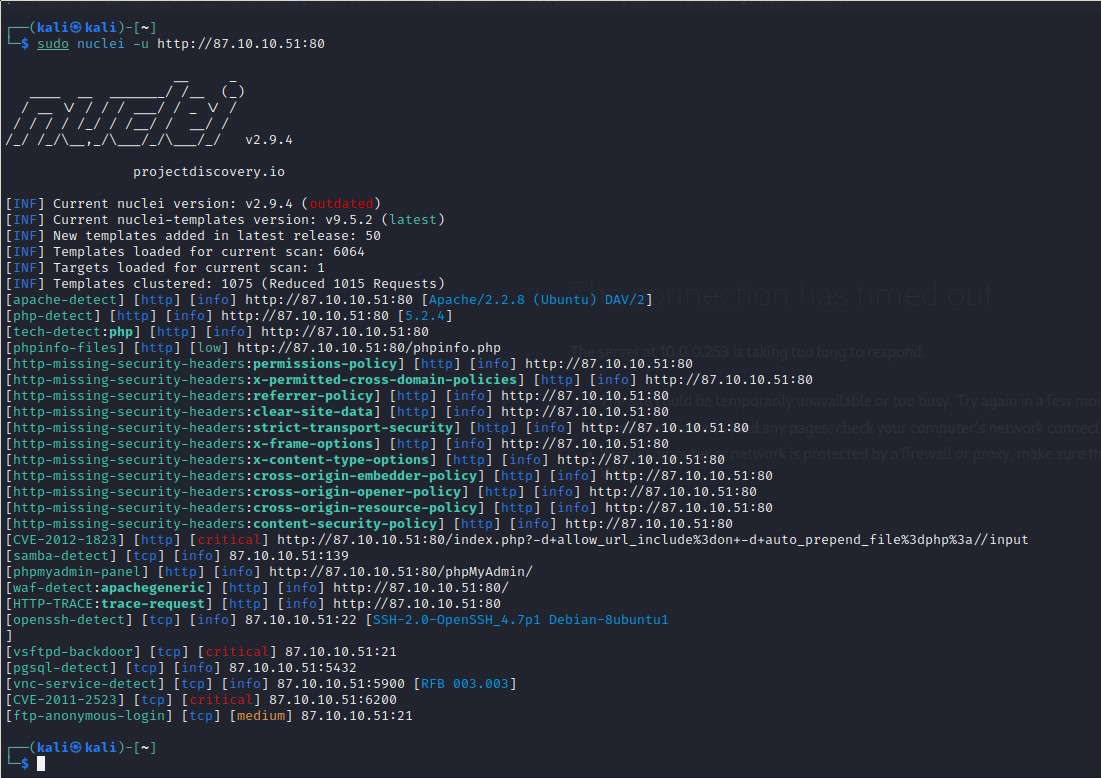
Ensuite on crée une règle qui permet au réseau externe d’accéder à la NAT.

- Scan Scnr extérieur :

On aperçoit qu’il y a toujours des vulnérabilités de scanné mais moins que à l’intérieur. Ici, nous avons 2 issues détectés.

- Scan Legion extérieur :

Pour le scan sur Legion nous tombons sur les mêmes résultats mais comme nous le voyons ci-dessus, moins de ports sont scannés et moins de ports sont donc ouverts.

- Scan Nuclei extérieur :

Avec le scan Nuclei à l’extérieur, nous voyons toujours des vulnérabilités mais cette fois ci on aperçoit trois vulnérabilités « critical » et un « medium ».

- Scan Nikto extérieur

Une image contenant texte, capture d’écran

Description générée automatiquement

Le scan Nikto n’a pas changer, il obtient le même résultat que le scan depuis l’intérieur.

Finalement, nous pouvons donc apercevoir lors du branchement du scanner à l’extérieur du réseau, avec les filtrages et les paramètres de sécurité, nous obtenons moins de résultat contrairement à lorsque nous sommes branchés à l’intérieur. Sauf pour Nikto, ce scan reste le même car c’est un scanner qui scan sur le Web et pas le réseau, vue que le port est ouvert il ne prend pas en compte les paramètres de sécurité donc les vulnérabilités ne change pas.

Ces scans nous ont permis d'obtenir une vision globale de l'état de sécurité du réseau. Il est essentiel de souligner que la sécurité informatique est un processus continu et évolutif. Il est donc recommandé de régulièrement effectuer des scans de vulnérabilités, d'appliquer les correctifs nécessaires pour le maintien du réseau.