Projet 1 : Surveillance réseau

Objectifs du projet

Dans ce projet de groupe (2 étudiants par groupe), vous allez concevoir une infrastructure de surveillance de laboratoire utilisable dans tous les cours du DIC-2-SSI. Ce faisant, vous acquerrez de l'expérience dans les domaines suivants :

- La capture de paquets complets (Full Packet Capture) ;
- Capture NetFlow ;
- Outils de journalisation ;
- Outils d'indexation, de recherche et d'analyse des données.

Ce projet est inspiré du livre blanc du SANS « Building a Home Network Configured to Collect Artifacts for Supporting Network Forensic Incident Response ».

Exigences – Collecte de données

Dans la première partie de ce projet, vous allez collecter des données sur le trafic réseau et archiver les données pour une analyse future. Les données à collecter comprennent la capture de paquets complets (PCAP), les données de résumé de flux (NetFlow), les fichiers journaux des principaux services réseau et les données spécifiques aux protocoles.

Dans le domaine de la surveillance des réseaux, il faut faire des compromis importants au niveau de la conception :

- Quelle quantité de données dois-je capturer ?
- Est-ce que je capture toutes les données des paquets ? (Contient toutes les informations possibles, mais s'accompagne de considérations de confidentialité, d'exigences de stockage massives pour les réseaux occupés, et de temps d'analyse et de traitement lents).
- Est-ce que je capture uniquement les données de résumé de flux ? (Les ensembles de données plus petits sont plus faciles à traiter, mais vous ne serez pas en mesure de reconstituer tous les détails des événements du réseau).
- Pendant combien de temps dois-je conserver les données ? Cette réponse varie-t-elle en fonction du type de données ?
- Quels sont les ports et les liens exacts que je surveille ? (Sur le routeur public ? Quel port ? Sur les principaux commutateurs internes ? Quels ports ?) En fonction des choix effectués, les événements clés du réseau peuvent être visibles ou invisibles.
- Où sont stockées les données capturées ? Comment ce stockage est-il sécurisé ?

Avant toute mise en œuvre, vous devez avoir une discussion technique avec votre groupe pour répondre à ces questions de conception.

Capture de paquets complets (Full Packet Capture)

Votre projet doit capturer des traces complètes de paquets (les formats de fichiers traditionnels sont « PCAP » ou « PCAPNG ») et les sauvegarder de manière bien organisée dans un dépôt de stockage à long terme. Utilisez un outil comme tcpdump ou un autre outil de votre choix.

Capture NetFlow

Votre projet doit capturer des données sommaires de flux de paquets (« NetFlow ») et les sauvegarder de manière bien organisée dans un dépôt de stockage à long terme. Utilisez un outil comme `nfpcapd` (qui fait partie de la suite nfdump) ou un autre outil de votre choix.

Capture d'autres données

Bien que les fichiers PCAP et NetFlow soient les principales sources de collecte de données, d'autres sources de données précieuses sont également disponibles et doivent être enregistrées pour analyse.

Surveillance DNS – L'outil PassiveDNS rend compte des requêtes DNS du réseau. Cet outil peut être configuré soit pour traiter un flux réseau brut en temps réel, soit pour post-traiter les fichiers PCAP après leur sauvegarde.

Surveillance ARP – L'outil ARPWatch rend compte des paires d'adresses IP<->MAC. Cet outil peut traiter un flux réseau brut en temps réel. Lorsque vous configurez cet outil, vous devez répondre à la question de conception : sur quelles interfaces cet outil serait-il plus ou moins utile ? Remarque : renseignez-vous sur l'option `-u` de cet outil.

Fichiers journaux – Les fichiers journaux peuvent être produits par un certain nombre de périphériques, notamment le pare-feu, le serveur DHCP et le proxy HTTP.

Pare-feu – Le projet pfSense est une distribution de pare-feu réseau libre, basée sur le système d'exploitation FreeBSD avec un noyau personnalisé et incluant des paquets de logiciels libres tiers pour des fonctionnalités supplémentaires. Le logiciel pfSense, avec l'aide du système de paquets, est capable de fournir les mêmes fonctionnalités, voire plus, que les pares-feux commerciaux courants, sans aucune de leurs limitations artificielles. Il a remplacé avec succès tous les pares-feux commerciaux de grande marque que vous pouvez imaginer dans de

nombreuses installations à travers le monde, y compris Check Point, Cisco PIX, Cisco ASA, Juniper, Sonicwall, Netgear, Watchguard, Astaro, et bien d'autres encore.

Exigences – Analyse des données

Dans la deuxième partie de ce projet, vous allez charger les données collectées dans des outils d'analyse pour qu'elles soient examinées.

Outils	Description	Source des données
Moloch	Système complet de capture, d'indexation et de base de données des paquets.	PCAP
SOF-ELK	Système polyvalent d'analyse des flux et des journaux	NetFlow, données du journal (passivedns, iptables, dhcpd, etc.)
Snort	Système de détection d'intrusion	Données en temps réel
Zeek	Surveillance de la sécurité du réseau	Données en temps réel

Exigences – Autres

Vous devez concevoir des enseignes d'avertissement « attrayants » à afficher dans tout le laboratoire, avec un contenu similaire à celui-ci :

Laboratoire de cybersécurité - Tous les accès Internet sont surveillés et enregistrés
AVERTISSEMENT ! Vous ne devez avoir aucune attente en matière de confidentialité dans votre utilisation de ce réseau. L'utilisation de ce réseau constitue un consentement à la surveillance, la récupération et la divulgation de toute information stockée sur le réseau, à quelque fin que ce soit.

Exigences – Documentation et tests

Documentation

La documentation suivante est requise pour ce projet. Une documentation complète garantira que le réseau peut être mis à jour et entretenu selon les besoins.

Document de conception publique : préparez un document, adapté à l'affichage public sur un site Web, qui communique votre conception globale de capture de données aux futurs étudiants qui utiliseront le laboratoire. Ce document devrait inclure une description narrative globale de la conception, plus le(s) diagramme(s) de réseau, les diagrammes de flux de données, et d'autres détails importants.

Instructions d'installation privées : fournissez des instructions d'installation étape par étape pour votre système. Si je commence avec une installation Ubuntu Linux générique et un routeur Mikrotik générique, que dois-je faire pour mettre en place votre système final ?

Cette documentation doit être soumise au format Markdown, adapté à une publication directe sur un site Web. Il existe un certain nombre d'éditeurs Markdown que vous pouvez installer sur votre ordinateur (MacDown ou MarkdownPad) ou que vous pouvez utiliser en ligne.

Tests

Vous devez effectuer des tests ponctuels dans le cadre de ce projet pour vous assurer que les systèmes que vous mettez en place sont fonctionnels.

Evaluation

Il s'agit d'un projet de groupe. La répartition des notes est la suivante :

- Contrôle du fonctionnement du laboratoire - 60
- Document public - 20
- Document sur l'installation privée - 20

Délai

Votre objectif est de terminer la collecte des données la première semaine et les outils d'analyse la deuxième semaine.

