Intrusions réseau

ISI

2 - Intrusions

Résumé du document

Cette note parle de la sécurité réseau, abordant la gestion des ports TCP/UDP, les phases de collecte et de scanning, ainsi que les techniques de protection et de détection des intrusions. Elle détaille les processus de découverte d'hôtes, de scanning de ports (TCP et UDP), d'identification de services et de systèmes d'exploitation, tout en fournissant des commandes Nmap spécifiques pour chaque type de scan. De plus, elle traite des techniques d'intrusion telles que le sniffing, le spoofing, et l'empoisonnement du cache ARP, et évoque les attaques par déni de service (DoS et DDoS) avec des exemples concrets.

Table des matières

1. Sécurité réseau

1.1. Liste des ports TCP/UDP

- Ports TCP sur 16 bits (65 536)
- « Well-known services », ports 0 à 1023

1.2. Collecte vs. « Scanning »

1.2.1. Phase de Collecte d'Informations

- **Examiner les lieux.**

1.2.2. Phase de Scanning

- **Frapper les murs** pour identifier toutes les portes et fenêtres.
- Tester l'ouverture des portes d'un immeuble pour identifier celles qui sont ouvertes.

1.2.3. Objectifs de la Phase de Scanning

1. Déterminer les machines vivantes (alive).
2. Identifier les services actifs.
3. Reconnaître les protocoles réseaux utilisés.

1.3. Objectifs de la phase de «scanning»

Pour une présentation organisée et claire de ces éléments en format typeset, voici une structuration appropriée pour des étapes spécifiques de scans dans un environnement réseau :

1.3.1. Host Scan

- **Déterminer les machines vivantes ("alive").**

1.3.2. Port Scan

- **Déterminer quels ports sont ouverts.**

1.3.3. Service Scan

- **Déterminer quels services sont actifs ou en écoute.**
- **Identifier les protocoles réseaux utilisés.**
  - **Exemple :** Utilisation de protocoles Wifi sur les bornes (par exemple, Kismet).

1.4. Découverte d'hôtes

1.4.1. Détermination de la Présence de Machines sur un Réseau

- **Utilisation de ping (message ICMP)** pour vérifier si une ou plusieurs machines sont vivantes.

1.4.2. Outils Typiques

- **Sing (outil ping avancé)** :
  - `sing -echo 192.168.0.255` (envoi d'un message broadcast)
  - `sing -mask 192.168.0.255` (masquage de l'adresse)
- **ICMPscan** : Outil spécialisé pour le scanning via ICMP.
- **NMAP** :
  - `nmap -sn -PE 192.168.0.0/24`
    - `-sn` = ping scan (désactive le scan de ports)
    - `-PE` = utilisation de l'écho ICMP

1.4.3. Inconvénients du Ping

- **Filtrage des messages ICMP :** Les messages ICMP, souvent utilisés pour le ping, sont régulièrement filtrés par les firewalls, ce qui peut rendre cette méthode moins efficace pour déterminer si une machine est active.

1.4.4. Techniques Alternatives de Scanning

- **Envoi de paquets TCP/UDP :** Utilisation de paquets TCP ou UDP pour contourner le filtrage des messages ICMP.
- **Scanner de Ports :**

- **Méthode :** Scanner toutes les adresses IP sur tous les ports.
- **Objectif :** Réaliser un scan complet de ports, en considérant toutes les machines identifiées comme vivantes lors d'une étape préliminaire.

1.5. Scan de Ports : UDP

1.5.1. Envoi d'un datagramme UDP à destination du port à scanner

- **Action :** Envoyer un datagramme UDP vers le port ciblé.
- **Si pas de réponse :** Le port est considéré comme ouvert.
- **Si réponse ICMP "destination port unreachable" :** Le port est considéré comme fermé.

1.5.2. Commande Nmap

- **Commande :** `nmap -sU`

1.5.3. Inconvénients du Scanning UDP

- **Fiabilité Limitée**
  - **Problème :** Le scan UDP est moins fiable car il ne requiert pas de confirmation de la part du destinataire.

1.6. Scan de ports : TCP connect

- **Tentative de Connexion TCP à Destination du Port à Scanner**
  - **Si port ouvert :** Le port est accessible et accepte les connexions.
  - **Si port fermé :** Le port n'accepte pas les connexions ou est filtré.
- **Commande Nmap pour Scan TCP**
  - **Commande :** `nmap -sT`
  - **Fonction :** Réaliser un scan de ports TCP complet en établissant des connexions TCP complètes.

1.6.1. États de la Connexion TCP

- **SYN-ACK** : Indique que le port est ouvert et prêt à établir une connexion.
- **SYN** : Paquet envoyé pour initier une connexion TCP.
- **ACK** : Paquet de confirmation dans le processus d'établissement de la connexion.
- **RST-ACK** : Paquet envoyé pour réinitialiser la connexion, souvent utilisé pour indiquer que le port est fermé ou refusant la connexion.
- **SYN** : Réinitiation du processus de connexion.

1.7. Scan de ports : TCP SYN-RST

- **Tentative de Connexion TCP à Destination du Port à Scanner**
  - **Si connexion s'ouvre :** Fermeture brusque à l'aide d'un paquet RST pour terminer la connexion.
  - **Si port ouvert :** Le port est accessible et accepte les connexions.
  - **Si port fermé :** Le port n'accepte pas les connexions ou est filtré.
- **Commande Nmap pour Scan TCP**
  - **Commande :** `nmap -sT`
  - **Fonction :** Réaliser un scan de ports TCP complet en établissant des connexions TCP complètes.

1.7.1. États de la Connexion TCP

- **SYN** : Paquet envoyé pour initier une connexion TCP.
- **SYN-ACK** : Réponse indiquant que le port est ouvert et prêt à établir une connexion.
- **RST** : Paquet envoyé pour réinitialiser la connexion brusquement, utilisé pour fermer la connexion après vérification de l'ouverture du port.
- **RST-ACK** : Réponse indiquant que le port est fermé ou refusant la connexion.

1.8. Scan applicatif

1.8.1. Étape de Scanning Avancée

- **Analyse des Couches Supérieures du Modèle OSI**

  - **Spécificité des ports :** Certains ports sont spécifiques à certains services. L'identification des ports ouverts peut révéler les services en cours d'exécution.
  - **Action sur les ports ouverts :** En cas de port ouvert, envoi de paquets spécifiques à l'application et/ou la version pour obtenir le maximum d'informations sur l'application en cours.

- **Commande Nmap pour Scanning Avancé**
  - **Commande :** `nmap -sV`
  - **Fonction :** Sonde les ports ouverts pour déterminer les informations de service et de version (`-sV`).

1.9. OS Fingerprint

1.9.1. Analyse de la Couche TCP/IP

- **Couches Concernées**
  - **Couche Réseaux (IP) et Transport (TCP)** : Focus sur l'interaction avec les champs spécifiques à ces couches.

- **Caractéristiques Spécifiques**
  - **TTL (Time To Live) :** Utilisé dans la couche réseaux pour déterminer la durée de vie du paquet dans le réseau.
  - **WIN (Taille de la fenêtre d'envoi) :** Pertinent pour la couche de transport, indiquant la quantité de données pouvant être envoyées sans accusé de réception.
  - **DF (Flag Don't Fragment) :** Un drapeau de la couche réseaux qui, lorsqu'il est activé, empêche la fragmentation des paquets.
  - **ToS (Type of Service) :** Utilisé dans la couche réseaux pour spécifier la priorité et la politique de gestion du trafic.

- **Utilisation de Paquets Forgés**
  - **Méthode :** Envoi de paquets forgés qui interagissent avec les champs TTL, WIN, DF, et ToS.
  - **Objectif :** Analyser les réponses pour déterminer les caractéristiques spécifiques du système d'exploitation sur le réseau.

- **Commande Nmap pour la Détection du Système d'Exploitation**
  - **Commande :** `nmap -O`
  - **Fonction :** Active la détection du système d'exploitation (`-O`), en se basant sur les réponses aux paquets forgés qui exploitent les caractéristiques des couches IP et TCP.

1.10. Protections contre le « scanning »

1.10.1. Bonnes Pratiques Générales

- **Toujours utiliser la dernière version, patch, etc.** : Assurez-vous que tous les logiciels et systèmes sont à jour pour corriger les vulnérabilités connues.

1.10.2. Filtrage et Contrôle des Messages ICMP

- **Filtrage des messages ICMP** : Limiter ou interdire certains types de messages ICMP pour des raisons de sécurité.
  - **Non-respect des RFC :** Cela peut aller à l'encontre des recommandations des RFC.
  - **Interdiction des messages ICMP de type 3 (« port unreachable »)** : Bloquer ces messages pour éviter la divulgation d'informations sur les ports fermés.

1.10.3. Utilisation de Pare-feux et IDS

- **Interdiction des balayages rapides des ports (ou alarme)** : Détecter et bloquer les scans de ports rapides pour prévenir les reconnaissances malveillantes.
- **Bannir une adresse IP et ne plus tenir compte des paquets** : Exclure les adresses IP suspectes pour réduire les risques d'attaque continue.

1.10.4. Utilisation de Proxys Inverses

- **Empêche les scans de type « Inverse TCP Flag »** : Protéger le réseau en bloquant les tentatives de scans utilisant des drapeaux TCP inversés.

1.10.5. Gestion des Bannières

- **Bannières minimales** : Réduire les informations divulguées dans les bannières des services pour tromper les attaquants.
  - **Modification des « banners »** : Changer les bannières pour désorienter les attaquants potentiels. La fonctionnalité peut varier.

1.10.6. Port Knocking

- **Principe :** Le port est initialement fermé par le pare-feu.
  - **Ouverture par séquence de connexions** : Utiliser une séquence spécifique de connexions sur des ports distincts pour ouvrir le port désiré.

1.10.7. Évaluation de la Sécurité de Son Propre Système

- **Auto-scan :** Effectuer des scans réguliers de son propre système pour identifier et corriger les vulnérabilités potentielles avant qu'elles ne soient exploitées par des attaquants.

1.11. Énumération

- **Basée sur les informations collectées aux étapes précédentes**
  - Utiliser les données obtenues lors des étapes de scanning et d'analyse pour approfondir la connaissance du réseau cible.
- **Objectifs d'Énumération**
  - **Ressources :**
    - Accès, domaines, noms, partages réseau.
  - **Utilisateurs :**
    - Comptes utilisateurs, groupes.
  - **Applications et Services :**
    - Noms, versions des applications et services en cours d'exécution.
  - **Vulnérabilités :**
    - Identifier les failles de sécurité, par exemple, l'utilisation de WEP au lieu de WPA2 pour la sécurité Wi-Fi.
- **Techniques d'Énumération**
  - Les méthodes varient selon les systèmes, applications et technologies spécifiques, et peuvent inclure des techniques telles que :
    - Scanning de partages réseau pour identifier les ressources accessibles.
    - Interrogation des services réseau pour obtenir des listes d'utilisateurs et de groupes.
    - Inspection des bannières des applications pour déterminer les versions et identifier les vulnérabilités connues.

1.12. Types d'intrusions

1.13. « Sniffing »

1.13.1. Écoute du Trafic Réseau (Sniffing, cf. 3.4 de [SECINF])

- **Objectifs de l'Écoute du Trafic**
  - **Déboguage ?**
  - **Capturer des informations sensibles, confidentielles.**
  - **Capturer des mots de passe**
    - **Transmis en clair :** telnet, rsh, FTP, HTTP, POP, IMAP.
    - **Non transmis en clair :** capture des codes hachés, challenge/réponse.
  - **Scan passif :** scan de ports, scan applicatif, etc.
  - **«Reverse-engineering» de protocole.**
- **Outil de base**
  - **Wireshark :** Outil utilisé pour analyser le trafic réseau et capturer des paquets en temps réel.

1.13.2. Techniques et Outils

- **Techniques de Sniffing**

- **Méthode :** Utilisation de Wireshark pour intercepter et analyser les paquets transitant sur le réseau. Cela permet d'obtenir des détails précis sur les données échangées et de potentiellement identifier des vulnérabilités ou des expositions de données sensibles.

1.13.3. Mode Normal des Cartes Réseau

- **Fonctionnement par défaut :** Les cartes réseau ne transmettent pas au système d'exploitation les informations non destinées à elles-mêmes, pour des raisons de performance et de confidentialité.
- **Filtrage des paquets :** La carte réseau filtre les paquets pour ne passer que ceux qui lui sont adressés directement.

1.13.4. Mode Promiscuous (Promiscuité)

- **Niveau OSI :** Niveau 2.
- **Fonctionnalités :**
  - Permet de capturer tous les paquets reçus par la carte réseau.
  - Captures typiquement à destination de toutes les adresses IP/MAC, sans filtrage.
  - Nécessite d'être connecté à un réseau.
  - Possible sur les réseaux filaire ou sans fil.

1.13.5. Distinction avec le Mode Monitor (RFMON)

- **Niveau OSI :** Niveau 2.
- **Fonctionnalités :**
  - Permet de capturer des paquets sans être associé à un réseau.
  - Utilisé uniquement dans le contexte de réseaux sans fil.

1.14. « Spoofing »

1.14.1. Falsification d'Identité Source (Réseau)

- **Se faire passer pour quelqu'un d'autre**
  - **Exemples :** Falsification de l'adresse IP source ou de l'adresse MAC.

1.14.2. Objectifs de la Falsification d'Identité

- **Contourner un filtrage de paquets**
  - **Par exemple :** Un pare-feu autorise des paquets provenant d'une certaine adresse IP.
- **Contourner un contrôle d'accès par adresse source**
  - **Par exemple :** Une adresse IP spécifique ne requiert pas d'authentification (RSH).
- **Brouiller les traces**

1.14.3. Techniques et Outils

- **Falsification IP/MAC**
  - **Méthode :** Utiliser des outils ou des techniques de programmation pour modifier l'adresse IP ou MAC émise par son dispositif réseau afin de se faire passer pour un autre appareil autorisé ou de confiance.

1.15. Attaques ARP

1.15.1. Empoisonnement du Cache ARP

- **Objectif :** Faire en sorte que les messages parviennent au pirate en modifiant le cache ARP des victimes.
- **Méthode :**
  - Envoi de messages ARP à la victime.
  - Modifier le cache ARP de la victime pour faire correspondre une adresse IP (IPx) à l'adresse MAC du pirate (MACpirate).

1.15.2. Idée de l'Attaque

- **Stratégie :** Prendre l'identité de la passerelle et/ou de la victime (par exemple : IPgateway = MACpirate).
- **Conséquence :** Tous les messages transiteront par le pirate, souvent dans le cadre d'une attaque « Man-in-the-middle » (MITM).
- **Transparence :** Le pirate capte puis transmet les messages plus loin, qu'ils soient modifiés ou non.

1.15.3. Types d'Attaques ARP

1. **« Gratuitous ARP »** : Envoi d'une réponse ARP volontaire sans demande préalable.
2. **Réponse ARP non sollicitée :** Envoi d'une réponse ARP en l'absence de requête spécifique.
3. **Réponse ARP forgée :** Envoi d'une réponse à une requête légitime avec des informations falsifiées.
4. **Requête ARP forgée (et non sollicitée) :** Envoi d'une requête ARP falsifiée sans qu'elle ait été demandée.

1.16. DNS cache poisoning

1.16.1. DNS

- **Fonction :** Conversion de nom de domaine en adresse IP.
- **Attaque :** Faire correspondre l'adresse IP du pirate à un nom de domaine et rediriger les utilisateurs vers un autre serveur contrôlé par l'attaquant.
- **Similitude :** Le site Web sur le serveur pirate doit ressembler très fortement à l'original pour tromper les utilisateurs.

1.16.2. Objectifs des Attaques

- **Usurpation d'identité :** Faire croire aux utilisateurs qu'ils interagissent avec le site ou service légitime.
- **Phishing :** Recueillir des informations sensibles telles que les identifiants de connexion.
- **Propagation de maliciels :** Diffuser des logiciels malveillants sous couvert d'un site ou service légitime.

1.16.3. Moyens d'Attaque

- **Vulnérabilité DNS :** Exploiter les failles dans le système DNS pour rediriger les utilisateurs.
- **Maliciel :** Utiliser des logiciels malveillants pour compromettre les systèmes et modifier les configurations DNS.
- **Man-in-the-Middle (MITM) :** Intercepter et modifier les communications entre l'utilisateur et les services légitimes pour rediriger ou altérer les données.

1.17. Session hijacking

1.17.1. Vol de Session (cf. 3.5 de [SECINF])

- **Objectifs**
  - **S'introduire dans un système sans devoir s'authentifier** : Utiliser une session existante pour accéder à un système normalement protégé par une authentification.
- **Méthodes de Vol de Session selon les Protocoles**
  - **TCP**
    - **Difficulté :** Le vol de session est difficile et nécessite de trouver les numéros de séquence des paquets pour usurper la session.
  - **HTTP**
    - **Fréquence :** Très courant, en raison de la simplicité relative de capturer des cookies ou de manipuler des URLs.
    - **Techniques :**
      - Vol de cookie : Intercepter les cookies de session transmis sur des connexions non sécurisées.
      - Vol de l'URL : Capturer ou manipuler l'URL qui peut contenir des paramètres de session.
      - Construction de l'URL : Créer des URLs qui exploitent les paramètres de session pour accéder illégalement aux comptes utilisateurs.

1.18. Denial of Service (DoS)

1.18.1. Déni de Service (Denial of Service - DoS)

- **Référence :** Voir chapitre 3.2 de [SECINF].
- **Objectif :** Nuire à la disponibilité d'un système d'information.
  - **But :** Empêcher les utilisateurs légitimes d'accéder aux services ou aux ressources en saturant le système avec un volume excessif de demandes.
- **Exemples de Techniques Connues**
  - **SYN Flooding**

    - **Description :** Utiliser des paquets SYN excessifs pour épuiser les ressources serveur, empêchant de nouvelles connexions légitimes.
  - **Smurf**
    - **Description :** Exploiter les requêtes ICMP pour amplifier le trafic réseau et submerger une cible avec des réponses inutiles.
  - **Déni de Service Distribué (DDoS)**
    - **Description :** Coordonner une attaque de déni de service à partir de multiples sources pour augmenter l'efficacité et la difficulté de mitigation.
- **Autres Vecteurs de DoS**
  - **Réseau électrique d'une entreprise :** Saboter l'alimentation électrique pour causer un arrêt des opérations.
  - **Réseau téléphonique :** Inonder le réseau téléphonique avec des appels pour empêcher son utilisation normale.

1.19. Distributed DoS (DDoS)

1.19.1. Utilisation de Machines "Esclaves"

- **Définition :** Machines compromises utilisées pour mener des attaques coordonnées.
  - **Installation de maliciel :** Un grand nombre de machines sont infectées avec un maliciel pour les transformer en agents contrôlables à distance.
  - **Contrôle à distance :** Ces machines, appelées bots ou zombies, sont commandées à distance.
  - **Méthodes de communication :** Les commandes peuvent être transmises via des canaux comme le chat, P2P, Twitter, etc.
- **Organisation en Botnet**
  - **Définition :** Les machines esclaves sont commandées par un ou plusieurs maîtres, formant un réseau appelé botnet.
  - **Exemples historiques :**
    - **Mafiaboy en 2000 :** Attaques notoires contre des sites tels qu'Amazon et eBay.
    - **Outils de Anonymous :** Utilisation de LOIC (Low Orbit Ion Cannon) pour mener des attaques par déni de service.