CM3 - Sécurité Réseau - Attaques et Défenses

Introduction à la sécurité informatique

Mohamed Said M'Bareck

SUPNUM
ms.mbareck@supnum.mr

2025-2026

Plan du cours

1. Introduction et Fondations
   - Contexte et Principes Stratégiques de la Sécurité
2. Techniques d'Attaque – Phase 1 : Reconnaissance et Accès
   - Footprinting, Balayage et Énumération
   - Compromission de la Couche Liaison (L2)
3. Techniques d'Attaque – Phase 2 : Exploitation et Impact
   - Déni de Service (DoS) et Exploitation
   - Malware et Notions de Forensique
4. Stratégies de Défense – Mise en Œuvre
   - Défense en Profondeur (DiD) et Monitoring
   - Protection des Protocoles et des Hôtes
5. Conclusion
   - Synthèse et Responsabilités Éthiques

- **Les Trois Piliers Fondamentaux (CIA Triad) :**
  - **Confidentialité** : Maintenir l'information secrète ou privée de tout accès non autorisé.
  - **Intégrité** : Assurer que l'information n'est pas altérée ou modifiée par des entités non autorisées.
  - **Disponibilité** : Garantir que les ressources sont accessibles à un individu autorisé sans interruption.
- **Principes Stratégiques :**
  - La sécurité réseau est une **guerre asymétrique** ; l'attaquant n'a besoin que d'une seule faille, tandis que le défenseur doit toutes les couvrir.
  - La défense doit être pensée en couches successives. C'est le principe de la **Défense en Profondeur**.

Phase 1 : Comprendre la Cible

L'attaquant collecte passivement et activement des informations.

- **Reconnaissance (Footprinting) :**
  - **OSINT** (Open Source Intelligence) : Utilisation de sources ouvertes (sites web, réseaux sociaux, archives publiques) pour trouver des informations sur les cibles (employés, technologies, adresses IP).
  - Outils : **Maltego**, **theHarvester**.
- **Balayage (Scanning) :**
  - **Balayage de ports** : Utilisé pour identifier les ports ouverts et les services actifs sur un hôte.
  - **Nmap** est l'outil de référence. Commandes clés :
    - `-sS` (Scan SYN "furtif") : N'achève pas la poignée de main TCP pour être moins "bruyant".
    - `-Pn` : Ne pas faire de ping avant de scanner (utile si le ping est bloqué par un pare-feu).
    - `-sV` : Tenter de déterminer la version des services.
    - `-sU` : Scanner les ports UDP.

Techniques d'Attaque – Phase 1 : Reconnaissance et Accès

Compromission de la Couche Liaison (L2)

Attaques L2

- **Empoisonnement du Cache ARP :**
  - Attaque Man-in-the-Middle (MiM) qui exploite le protocole ARP non sécurisé.
  - L'attaquant envoie de faux paquets ARP pour associer l'IP d'une victime à sa propre adresse MAC, interceptant ainsi tout son trafic.
- **MAC Flooding :**
  - Sature la table CAM d'un switch avec de fausses adresses MAC.
  - Le switch panique et se comporte comme un hub, envoyant tout le trafic à tous les ports.

Défenses L2

- **Dynamic ARP Inspection (DAI) :**
  - Fonctionnalité de switch qui vérifie la validité des paquets ARP et bloque les paquets suspects.
  - Contrecarre l'empoisonnement ARP.
- **Port Security :**
  - Limite le nombre d'adresses MAC autorisées sur un port de switch.
  - Contrecarre le MAC Flooding.
- **BPDU Guard :**
  - Protège contre les attaques sur le protocole Spanning Tree.

Techniques d'Attaque – Phase 2 : Exploitation et Impact

Déni de Service (DoS) et Exploitation

- **Déni de Service Distribué (DDoS) :**
  - Le but est de rendre un système inutilisable en **surchargeant ses ressources** (CPU, bande passante, connexions).
  - Peut cibler la couche **Réseau** (ex : SYN Flood), ou la couche **Application** (ex : requêtes HTTP complexes).
  - **Land Attack** : Une attaque historique où un paquet SYN est envoyé avec la même IP source et destination, provoquant une boucle sur d'anciens systèmes.
- **Exploitation et Post-Exploitation :**
  - **Exploitation** : Utilisation d'une vulnérabilité pour obtenir un accès. Des outils comme **Metasploit** automatisent ce processus.
  - **Post-Exploitation** : Ce que l'attaquant fait *après* avoir obtenu l'accès.
    - **Escalade de privilèges** : Devenir administrateur/root.
    - **Mouvement latéral (Lateral Movement)** : Pivoter pour attaquer d'autres machines sur le réseau interne.
    - **Persistance** : Installer des backdoors pour garder l'accès.
    - **Collecte de credentials** (ex : Pass the Hash).

- **Malware (Logiciel malveillant) :** Code conçu pour nuire.
  - **Virus/Ver (Worm) :** Se propage en s'attachant à des programmes ou de manière autonome sur le réseau.
  - **Ransomware :** Chiffre les fichiers de la victime et demande une rançon.
  - **Spyware/Keylogger :** Vole des informations (mots de passe, habitudes de navigation).
  - **Rootkit :** Se cache profondément dans le système d'exploitation pour maintenir un accès persistant et invisible.
- **Notions de Forensique Numérique (Digital Forensics) :**
  - L'art et la science de l'investigation après un incident de sécurité.
  - **Objectif :** Comprendre ce qui s'est passé, préserver les preuves et identifier l'attaquant si possible.
  - **Principes clés :** Ne jamais travailler sur l'original (travailler sur une copie bit-à-bit), maintenir une chaîne de possession (Chain of Custody) pour garantir l'intégrité des preuves.

Stratégies de Défense – Mise en Œuvre

Défense en Profondeur (DiD) et Monitoring

- **Défense en Profondeur (Defense-in-Depth) :**
  - Ne pas compter sur une seule ligne de défense. Mettre en place des contrôles de sécurité multiples et redondants.
  - **Segmentation réseau** : Isoler les parties critiques du réseau. Une **DMZ** (Zone Démilitarisée) est utilisée pour héberger les serveurs publics (web, mail) et les séparer du réseau interne.
  - **Filtrage Egress (sortant)** : Contrôler le trafic qui *sort* de votre réseau pour bloquer l'exfiltration de données et les communications de malwares.
  - **Inspection Profonde de Paquets (DPI)** : Les pare-feux modernes ne regardent pas seulement les adresses et les ports, mais aussi le contenu des paquets.
- **Network Security Monitoring (NSM) :**
  - **"La prévention est idéale, mais la détection est une obligation."** On part du principe que des attaques réussiront.
  - Le cycle NSM : **Collection** (des logs, du trafic), **Analyse**, **Escalade** (alerter les bonnes personnes) et **Résolution**.
  - La **synchronisation temporelle (NTP)** de tous les systèmes est essentielle pour pouvoir corréler les événements entre différentes sources de logs.

Stratégies de Défense – Mise en Œuvre

Protection des Protocoles et des Hôtes

- **Sources de Données pour le NSM :**
  - **Full Content Data** : Captures complètes du trafic (fichiers pcap). Très riche mais lourd à stocker.
  - **Metadata** (ex : NetFlow) : Informations sur les communications (qui a parlé à qui, quand, combien de temps). Moins de détails mais plus léger.
  - **Alert Data** : Alertes générées par des systèmes de détection d'intrusion (**NIDS/NIPS**) comme Snort ou Suricata.
- **Hardening des Systèmes et Protocoles :**
  - **Utiliser des protocoles sécurisés :** Remplacer systématiquement les protocoles en clair (Telnet, FTP, HTTP) par leurs équivalents chiffrés (**SSH, SFTP, HTTPS**).
  - **Principe du moindre service :** Désactiver tous les services et ports qui ne sont pas absolument nécessaires.
  - **Gestion des patchs :** Appliquer les mises à jour de sécurité de manière rigoureuse et régulière.

Conclusion

Synthèse et Responsabilités Éthiques

- **Perspective de l'attaquant :** Les attaquants cherchent un accès, puis la persistance, l'expansion (mouvement latéral) et l'exfiltration de données.
- **Perspective du défenseur :** Mettre en place une défense en profondeur, surveiller activement le réseau (NSM), et durcir les systèmes pour réduire la surface d'attaque.
- **Rapport et Éthique Professionnelle :**
  - Un test de pénétration est toujours encadré par un contrat et un accord de non-divulgation (**NDA**).
  - Les livrables incluent un **Résumé Exécutif** (pour la direction, sans jargon technique) et un **Rapport Technique** détaillé (pour les ingénieurs).
  - Le rôle de l'**Ethical Hacker** est d'identifier les faiblesses pour permettre de renforcer la défense, pas de causer des dommages.