1. Types d’attaques

5P :

* Probe (sonde)

Ping, traceroute, nslookup

Scanner de port

* Penetrate (Intrusion)

Brute force, dictionnaire

Failles des logiciels

* Persist (Persistant)

Créer un accès administrateur en fraude

Outil de contrôle à distance (cheval de Troie)

* Propagate (Propager)

Sonder les failles du réseau local

Propager l’intrusion

* Paralyze (Paralyser)

Endommager des systèmes ou des données

Utiliser les machines attaquer d’autres systèmes

1. Scan

* Simple

Tentative de connexion aux services

Facilement détectable

* Furtif

Tentative d’échange des données sans connexion

* Détournement des normes RFC
* Aveugle

Utiliser des machines intermédiaires

Spoofing, usurper identité d’une machine ou d’un équipement

* Passif

Spifing, enregistrer et analyser les communications réseaux

1. Attaques réseaux

* IP Spoofing

Usurper IP

* ARP Spoofing

Usurper MAC

* DNS Spooging

Usurper DNS

* Attaque par fragment

Fragments overlopping, substitution de fragments

Tiny fragments

* Détournement de session TCP

Ecouter le réseau et attendre l’authentification

Désynchroniser le client et le serveur en créant une latence

Usurper client (ou serveur)

1. Attaque sur les logiciels

* Configuration par défaut
* Bugs
* Dépassement de pile
* Script
* Injection SQL
* Homme du milieu
* DOS / DDOS

Déni de service distribué

* Inonder le service de demandes
* Demandes de connexion
* Surcharger le service en demande UDP
* Smurfling, inonder de requête ICMP(ping) en broadcast en usurpant l’identité de machines
* DDOS

1. Types de détection

IDS Système de détection d’intrusions

* Surveiller la mémoire et le processus
* Trier les connexions
* Filtrer les communications sur la passerelle/routeur

1. Méthodes de détection

* Recherche de motif
* Analyse de protocoles à la recherche d’abus connu
* Analyse heuristique à la recherche comportement inconnu
* Approche probabiliste / statistique