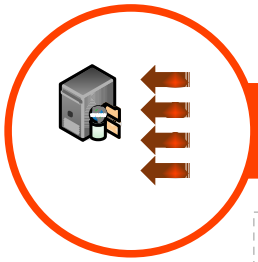
INFOGRAPHIE CYBERSECURITÉ



DENI DE SERVICE (DOS)

TCP SYN FLOOD
À chaque connexion, le serveur créé une session TCP et conserve la connexion en mémoire. L'attaque consiste à saturer la mémoire de connexions non terminées

BOTNETS
En utilisant un réseau de machines zombies, l'attaquant conduit une attaque de masse vers un réseau ou un serveur.

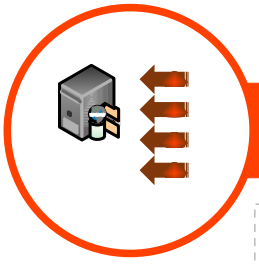
SMURF ATTACK
L'attaquant effectue des requêtes nécessitant de gros calculs sur le serveur. Il utilise pour cela de multiples adresses IP (même s'il ne reçoit jamais les résultats).

L'HOMME DU MILIEU (MITM)

SESSION HIJACKING
L'attaquant se fait passer pour un site de confiance et trompe le destinataire pour obtenir des informations importantes.

IP SPOOFING
L'attaquant envoi des packets IP usurpés pour obtenir la confiance du réseau destinataire.
Localement, un ARP poisoning permet de passer la sécurité des commutateurs.

REPLAY
L'attaquant enregistre des trames IP pour pouvoir les envoyer plus tard et ainsi obtenir les mêmes accès que l'émetteur original.



PHISHING

EMAIL PHISHING
L'attaquant envoi un courriel ressemblant à une source fiable, mais place des liens qui renvoient vers des sites piégés.

ATTAQUE SUR MOT DE PASSE

DICTIONARY ATTACK
L'attaquant utilise un programme qui automatise le remplissage d'identifiants, en testant des mots de passe tirés de dictionnaires

BRUTE FORCE ATTACK
L'attaquant utilise un programme qui automatise le remplissage d'identifiants, en testant des mots de passe de manière itérative, caractère par caractère. Attaque très longue.

RAINBOW TABLE ATTACK
Similaire à l'attaque par dictionnaire, les tests sont effectués en se basant sur le mot de passe chiffré, dont on essaye de reconnaître les failles (voir RC4).

BTS SIO – D. ROUMANET

INFOGRAPHIE CYBERSECURITÉ

ATTAQUES PAR MALWARES

VIRUS
Un virus s'exécute au lancement d'une application infectée. Il va alors chercher d'autres exécutables à infecter . Plus tard, il peut lancer des actions destructrices

VERS
Principalement utilisé par courriel, en pièces jointes, ces programmes malicieux tentent de ce propager aux autres contacts de la messagerie.

RANSONWARE
Ce type de virus chiffre ou verrouille des fichiers et les rend indisponibles sans une clé de déchiffrement. En général, l'attaquant fournit cette clé en échange d'une rançon (argent).

ÉCOUTES CLANDESTINES (EAVESDROPPING)

ÉCOUTE PASSIVE
En obtenant des informations privés lors d'une écoute sur un réseau corrompu, l'attaquant peut planifier une attaque, en déterminant les faiblesses de la société écoutée.

ÉCOUTE ACTIVE
L'attaquant peut se faire passer pour une personne de confiance et obtenir des actions des destinataires favorables à ses attaques.

INJECTIONS SQL

PERSISTENT XSS
Un utilisateur sur un serveur de confiance trouve un lien hors du domaine, qui permet d'exécuter un code malicieux.

```
<img src="http://target.site.com/add-user?user=name&grant=admin">
```

REFLECTED XSS
.

DOM-BASED XSS
.