EPSI – B3

# Sécurité - Chapitre 03 – Cryptographie symétrique & asymétrique

# TP

## Préparation

1. Connectez-vous sur un linux en ligne de commande

## Openssl - Chiffrement

1. Créer un fichier secret.txt contenant un cours texte (ex : Hello World !!!)
2. Chiffrer ce fichier avec la commande openssl en AES-256-CBC

Quelles options pour la commande openssl avez-vous utilisé ?

## Openssl - Déchiffrement

1. Déchiffrer le fichier secret.aes en un fichier decrypt.txt

## Openssl - STDIN

1. Chiffrer STDIN en aes-256-cbc bits grâce à la commande openssl

## Openssl - STDOUT

1. Déchiffrer le fichier secret.aes vers STDOUT (sans passer par un fichier en clair)
2. Quel est l'intérêt de la 2nd méthode, celle ou on ne passe pas un fichier en clair, ni pour chiffrer ni pour déchiffrer ?

## Openssl - Sécurisation

1. Quel est le protocole le moins sécurisé ?

   AES-256-ECB AES-256-CFB AES-256-OFB AES-256-CBC

2. Pourquoi ?
3. Quel est la différence entre ECB et CBC ?

## RSA – Mode Manuel

1. Chiffrez le mot SOS avec du RSA, vous présenterez chaque étapes de la création des clés aux chiffrement

## RSA – Openssl

1. Générez une pair de clé RSA avec la commande openssl
2. Chiffrez le message du fichier secret.txt
3. Signer le message du fichier secret.txt
4. Vérifiez la signature et déchiffrez le message

## RSA – GPG

1. Reprenez les 5 questions précédente mais cette fois ci avec GPG

## SSH

1. Comment ssh assure-t-il sa sécurité sans autorité de certification ?

# CHAPITRE 5 - PENTEST

## Metasploit

# PTES

## Penetration Testing Execution Standard

# PTES

1. Renseignement - Collecte d'informations
2. Analyse de Vulnérabilités
3. Exploitation
4. Post Exploitation
5. Rapport

# RENSEIGNEMENT

- whois
- wifi
  - airmon-ng
  - airodump-ng
  - kismet
- port scanning
  - nmap
- smtp
- Web
  - http://www.google.com
  - http://www.facebook.com
  - etc..
- **Metasploit**

# ANALYSE DE VULNÉRABILITÉS

- Scanners de Vulnérabilité
  - OpenVAS
  - Nessus
  - NeXpose
- Analyse passive
  - wireshark
- **Metasploit**

# EXPLOITATION

- Fuzzing
- Sniffing
  - Wireshark
- aireplay-ng
- SQL injection
- **Metasploit**

# POST EXPLOITATION

- Installation d'une backdoor
- dump de la base des mots de passe
- Désactivation de l'anti-virus
- Désactivation du système de mise à jour
- **Metasploit**

# RAPPORT

| | Coeur de métier | Service de support | Service non-urgent |
|---|---|---|---|
| Département ou groupe de VIP | Critical | High | High |
| Petit groupe ou VIP | Critical | High | Medium |
| Utilisateur simple | High | Medium | Low |

# METASPLOIT

## Les bases

# METASPLOIT

## Qu'est-ce que c'est ?

- C'est un framework permettant de réaliser des tests de pénétration.
- On peut l'utiliser dans toutes les phases du PTES

# METASPLOIT - DÉFINITIONS

- **Exploit** : Moyen non prévu par le développeur qu'a un attaquant d'utiliser un logiciel afin de pénétrer un système.

- **Payload** (Charge) : Code que l'on veut faire exécuter par le système, afin de pouvoir accéder au système (ex : reverse-shell)

- **Shellcode** : Suite d'instructions utilisées comme payload. Souvent écrit en assembleur

# MESTASPLOIT - INTERFACES

- **MSFConsole** : L'interface d'interaction principale avec le framework

- **MSFCli** : S'utilise depuis la ligne de commande, idéale pour scripter les exploits.

- **Armitage** : L'interface graphique