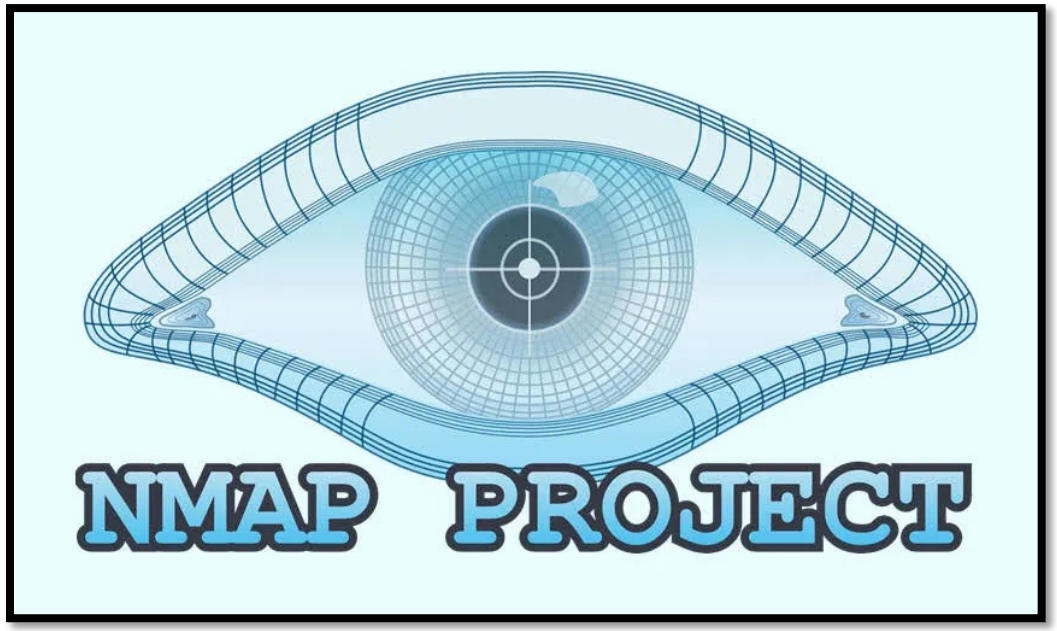
BLOC 1 - CYBERSECURITY ESSENTIALS FINAL PROJECT

Présenté par : Voujemaa HADJAR

ÉTAPE 1

- Scan du réseau de l'entreprise *Evil Corp*.
- Détection de différentes machines et différents ports ouverts



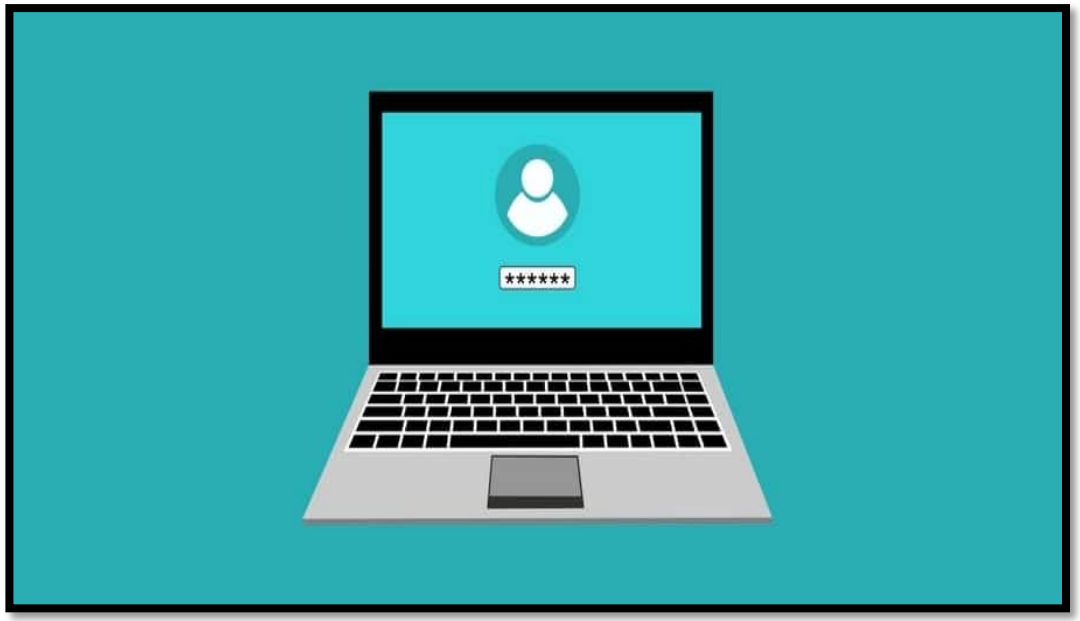
ÉTAPE 2

PORT 21

- Identifier les vulnérabilités avec Metasploit

➡️ Outil de cybersécurité qui teste les systèmes informatiques en simulant des attaques pour trouver et corriger les vulnérabilités avant qu'elles ne soient exploitées par des hackers.

ÉTAPE 3



- Exploitation de la vulnérabilité 🦠

➡️ Connexion au compte par défaut *anonymous*, sans mot de passe donnant accès à une clé privée 🔑

➡️ Connexion possible au compte utilisateur *alice@jedhabootcamp* 👤

CONCLUSION

BILAN

- Clé privée laissée sur un compte ouvert à tous
- Connexion au compte utilisateur Alice
- Exploitation des données

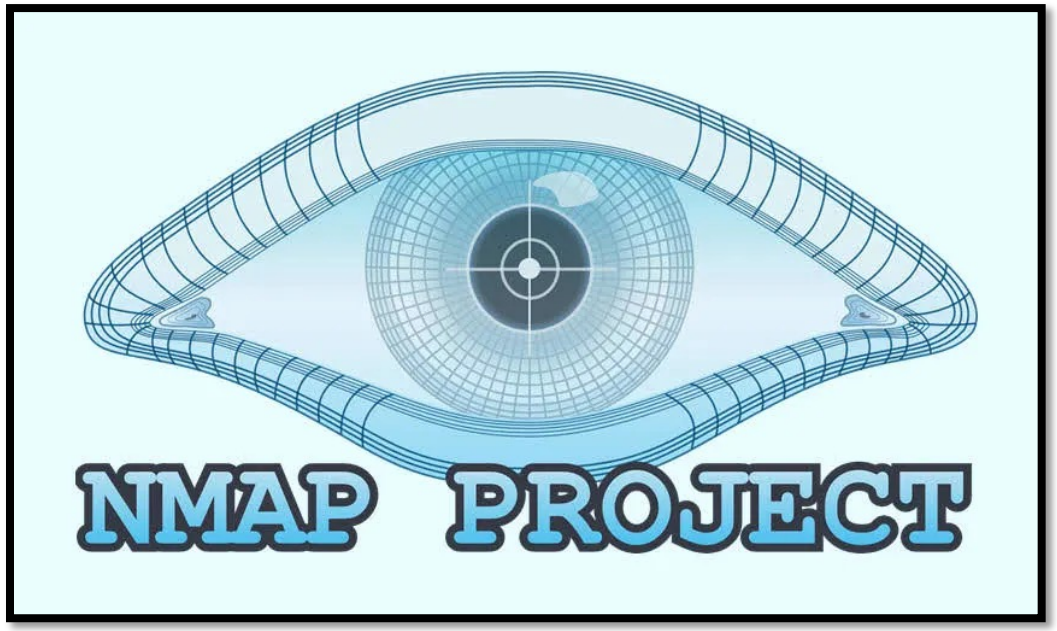
RECOMMANDATIONS

- Administrateur réseau : être davantage vigilant et supprimer le ou les éventuel(s) compte(s) *anonymous*
- *Alice* : ne pas déposer de clé privée sur un compte ouvert à tous

ÉTAPE 1

👁️ Scan plus précis du réseau de l'entreprise

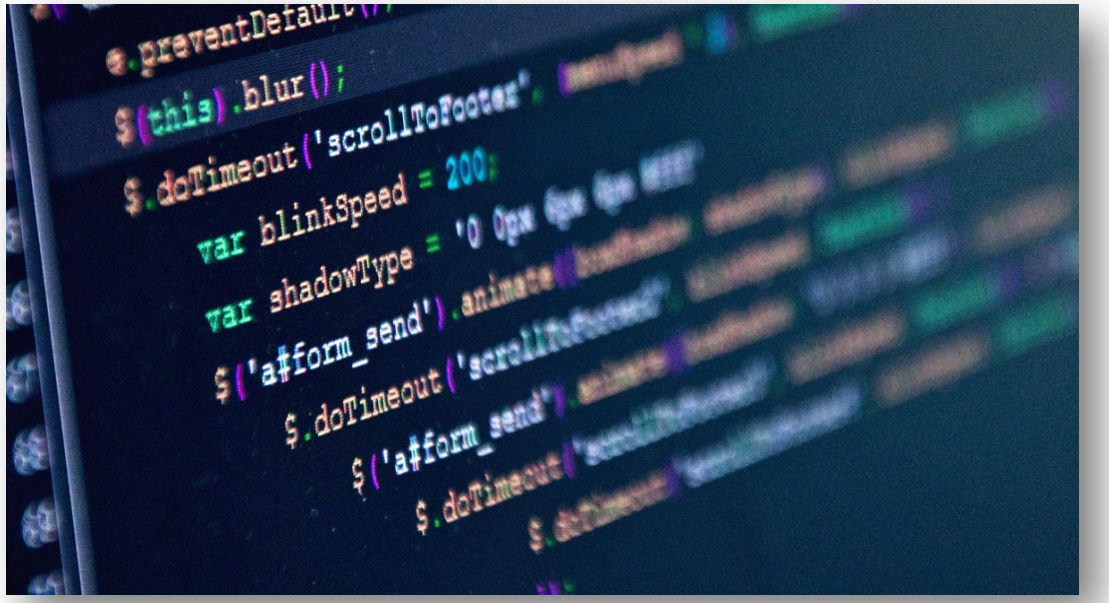
📌 Détection du port 1337 relié à une page internet : http://172.31.35.242:1337



ÉTAPE 2

📩 Page internet donne accès à l'onglet *Contact*

👥 Accès aux noms d'utilisateurs : *devil, john et user* en cliquant sur *Send*



ÉTAPE 3

🔐 Utilisation de la méthode *BruteForce* pour essayer de deviner le mot de passe

⚠️ Mot de passe de John récupéré : *peterpan*

👤 Connexion au compte *john@jedhabootcamp*

CONCLUSION

BILAN

- Site web pas assez protégé
- Mot de passe simple récupéré
- Connexion au compte utilisateur John
- Exploitation des données

RECOMMANDATIONS

- Administrateur réseau : utiliser des équipements pour se protéger contre les attaques (double authentification, captcha…)
- *John* : changer son mot de passe et créer un beaucoup plus complexe
- Bloquer les tentatives infructueuses de mot de passe (max. 3 etc.)