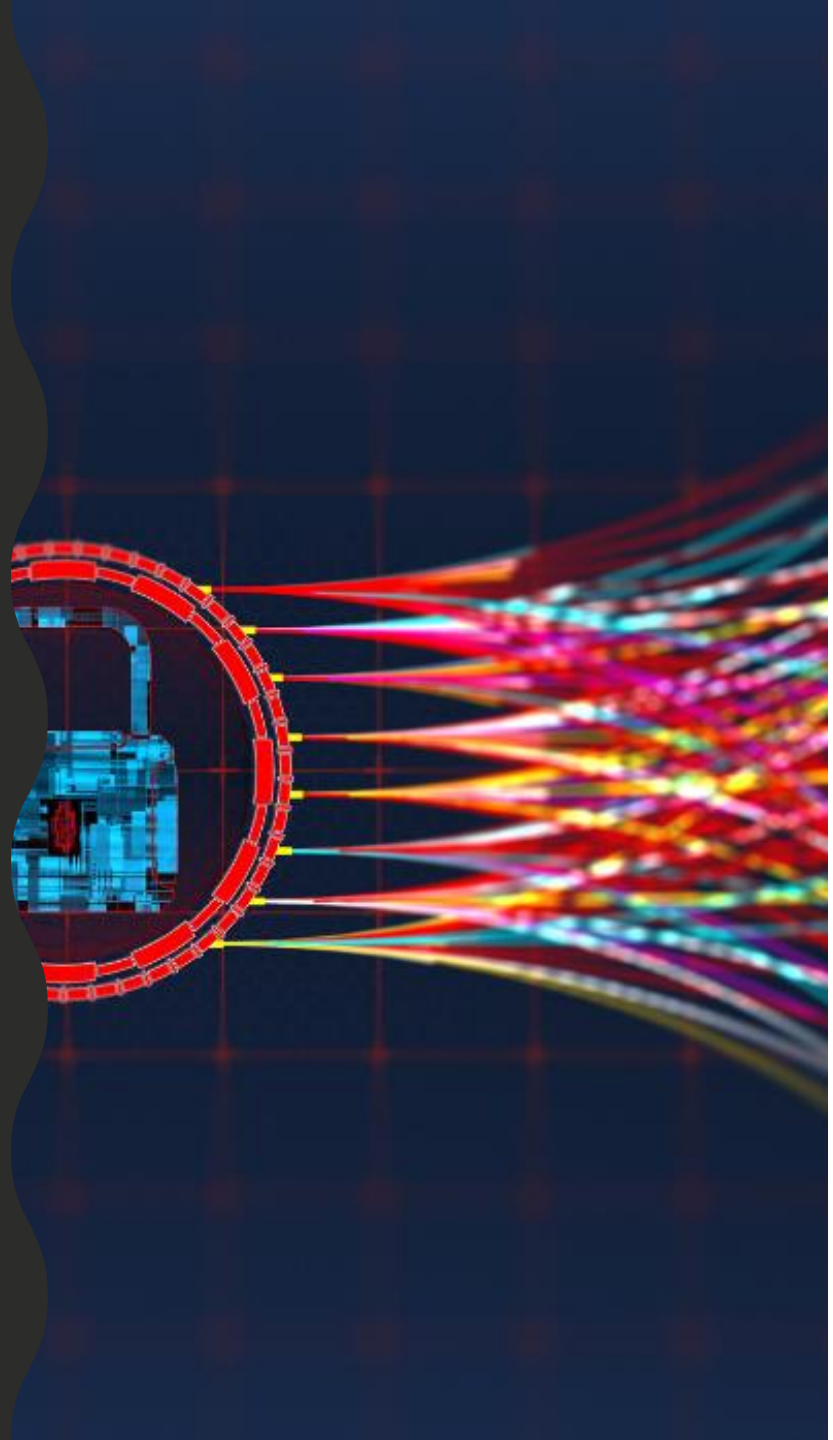
LA LIVRAISON

PYTHON POUR LA CYBERSÉCURITÉ



OBJECTIFS

- A la fin de cette partie, vous devriez être en mesure de :
  - Décrire le concept générale de la livraison
  - Décrire le concept
    - du piratage et de l'exploitation des vulnérabilités
    - de livraison par code malveillant en PJ
    - de page phishing
  - Ecrire un code qui permet
    - de créer des pages de phishing
    - d'automatiser l'exploitation d'une vulnérabilité et de la livraison de code malveillant

C'EST QUOI?

- Infiltration du réseau d'une cible et atteindre les utilisateurs
- Utilisation des cyber-armes à cette fin
- Peut prendre la forme d'un piratage du réseau cible et de l'exploitation d'une vulnérabilité matérielle ou logicielle.
- Peut aussi impliquer l'utilisation du phishing
  - Liens vers des pages de phishing (récolte d'information, téléchargement de logiciels malveillants, etc.)
  - Logiciels malveillants en pièces jointes

PIRATAGE & EXPLOITATION DE VULNÉRABILITÉS

- Basée sur les vulnérabilités identifiées lors de la reconnaissance et des exploits disponibles
- Livre une charge primaire qui servira par la suite à
  - Contourner les limitations imposées par les mesures de sécurité
  - Téléchager les autres charges plus importantes
  - Maintenir l'accès

LE PHISHING

- Envoie de courrier automatisé aux cibles potentielles
- Le Spear Phishing est du Phishing adapté à la cible (e.g administration, dirigeants, etc.)
- A pour but de s'approprier des identifiants ou autre information qui facilitent l'attaque
- Le courrier contient souvent de faux-liens vers des pages de phishing
  - La page est identique à la page originale
  - Le formulaire de collecte d'identifiant est envoyé aux serveur de l'attaquant
  - Une page d'erreur (faux utilisateur ou mot de passe) redirigeant vers la page originale

PAGE DE PHISHING

- Ecrire une fonction pour télécharger une page légitime et la sauvegarder dans un fichier
- Ecrire une fonction qui lit le contenu du fichier et remplace les liens “absolus” pertinents par des liens malicieux relatifs à une page php locale
- La page php malicieuse lira les champs du formulaire et les stockera dans un fichier et redirigera la victime vers la page légitime
- Tester la page
- Ecrire une fonction qui lit un fichier CSV et en extrait la colonne Nom/Prénom ainsi que la colonne adresse mail et les stocke dans une liste
- Ecrire une fonction qui lit la liste et envoie des mails aux victimes contenant le lien de la page malicieuse

METASPLOIT FRAMEWORK

- Outil open source, qui fait partie du projet Metasploit (un projet de cybersécurité)
- Développement et exécution d'exploits contre une machine distante,
- Utilise les informations du catalogue d'exploit-db pour fournir des informations sur les vulnérabilités du système.
- Interface graphique implémentée et développée pour le framework Metasploit
- Ligne de commande activée par la commande msfconsole
- Librairie Python