Université Cheikh Anta Diop (UCAD)

Ecole Supérieure Polytechnique
Département Génie Informatique
Année Universitaire 2023-2024

Veille Technologique

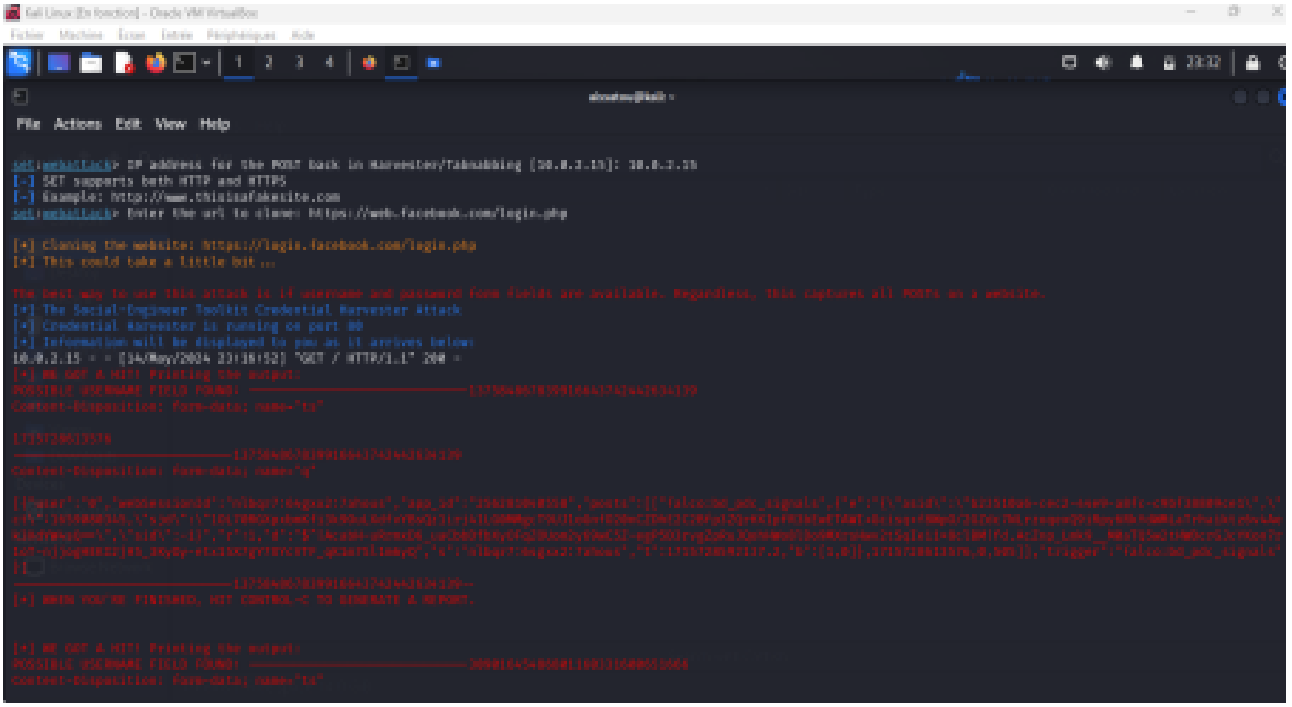
Prenom et nom:
Assane Gueye (GLSIB)

Professeur :
Mr Doudou Fall

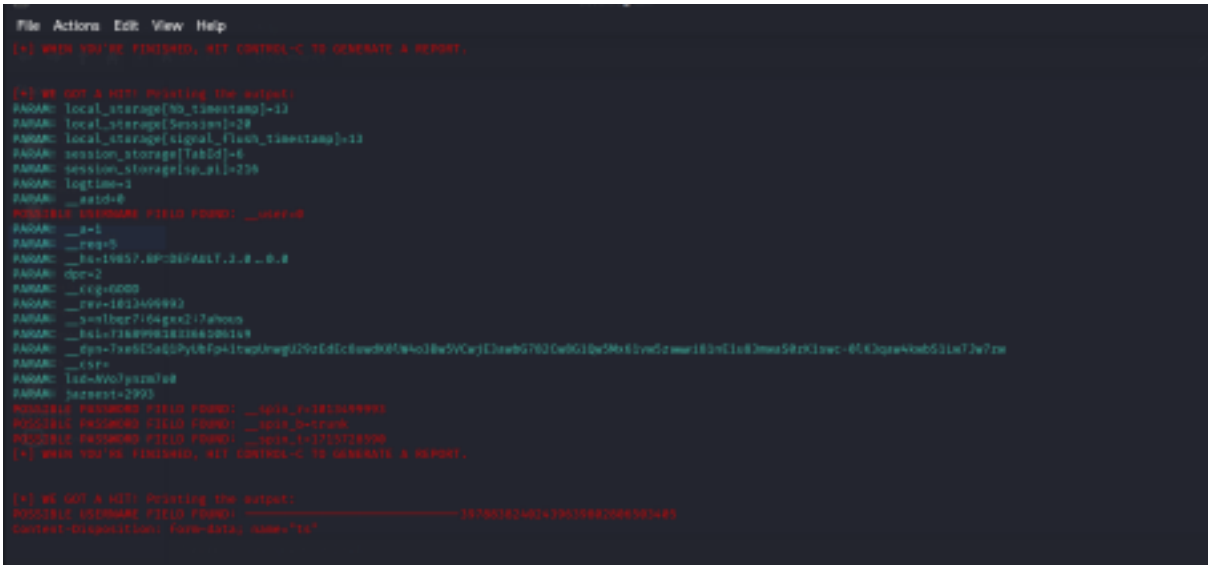
ATELIER 7:

Partie 1 : Récolte d'informations d'identification via Site Cloner

Importez le rapport XML que SET produit avec toutes les informations d'identification volées. Voici ce qu'on a : un long tapis rouge contenant les informations sur les comptes volés. Je n'arrive pas a trouver l'emplacement du rapport XML de ce fait j'ai fait une capture à la place.


File Actions Edit View Help
[-] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND:
Content-Disposition: form-data; name="lsd"
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND:
Content-Disposition: form-data; name="lsd"


Content-Disposition: form-data; name="lsd"
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND:
Content-Disposition: form-data; name="lsd"
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


File Actions Edit View Help
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND:
POSSIBLE PASSWORD FIELD FOUND:
POSSIBLE PASSWORD FIELD FOUND:
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND:
Content-Disposition: form-data; name="lsd"

Question 1 : regardez l'URL de votre site cloné : http://aaa.bbb.ccc.ddd. Cette adresse IP convient-elle à une véritable attaque d'ingénierie sociale sur Internet ? Pourquoi cela ne fonctionne -t-il pas ?

Sur l'URL du site cloné il est écrit "https://web.facebook.com/login.php '' alors que cela devrait etre « https://www.facebook.com/login.php »

Cette adresse IP ne convient pas à une attaque d'ingénierie sociale car elle est une adresse locale dons non accessible depuis l'internet. Cela ne fonctionne pas car les utilisateurs n'ont pas accès à cette adresse depuis leurs appareils.

Question 1 (suite) : comment pouvez-vous résoudre le problème de l'adresse IP dans la question précédente ?

Pour résoudre ce problème, nous devons utiliser une adresse IP publique ou un nom de domaine accessible depuis Internet. Nous pouvons soit héberger le site cloné sur un serveur public avec une adresse IP publique, soit utiliser un service de redirection de domaine pour rediriger vers votre adresse IP locale.

Question 2 : regardez à nouveau l'URL de votre site cloné : http://aaa.bbb.ccc.ddd. Une adresse IP ! Comment pourriez-vous remédier à ce problème ?

Pour remédier au problème de l'adresse IP dans l'URL, nous devons utiliser un nom de domaine plutôt qu'une adresse IP. Enregistrer un nom de domaine approprié et le configurer pour pointer vers notre adresse ou notre serveur où le site cloné est hébergé.

Question 3 : regardez à nouveau l'URL de votre site cloné : http://aaa.bbb.ccc.ddd. Ce n'est pas crypté. Les navigateurs Web signalent de plus en plus clairement que ces pages ne sont pas sécurisées au moyen de divers avertissements ou icônes. Comment pourriez-vous résoudre ce problème gratuitement ?

Pour sécuriser le site gratuitement, utilisons Let's Encrypt pour obtenir un certificat SSL/TLS, puis configurons notre serveur web pour utiliser HTTPS et rediriger automatiquement le trafic HTTP vers HTTPS. Cela garantira que les données échangées sont sécurisées et évitera les avertissements de navigateur concernant la sécurité de votre site.

Partie 2: Envoi d'e-mails

Décrire SPF, avec vos propres mots. (1 paragraphe) SPF, ou Sender Policy Framework, est un système de validation de courrier électronique conçu pour empêcher le spam et le phishing en vérifiant les expéditeurs de courriels. Il fonctionne en permettant aux propriétaires de domaines de publier une liste d'adresses IP autorisées à envoyer des courriels en leur nom à travers un enregistrement DNS spécifique. Lorsqu'un courriel est reçu, le serveur de messagerie du destinataire vérifie cet enregistrement SPF pour s'assurer que le courriel provient d'une source légitime mentionnée dans la liste. Si le courriel est envoyé à partir d'une adresse IP qui n'est pas dans cette liste, il peut être marqué comme suspect ou rejeté, réduisant ainsi les risques d'usurpation d'identité (spoofing) où les expéditeurs malveillants tentent de se faire passer pour quelqu'un d'autre.

En utilisant un des nombreux sites web pour créer des politique de SPF, générez une règle SPF pour le domaine societe.sn, en spécifiant que l'adresse IP 123.45.67.89 est autorisée à envoyer des courriels pour ce domaine, et que l'hôte gmail.com est également autorisé à envoyer des courriels pour ce domaine.

Décrire DKIM : Il aide aussi à protéger ses utilisateurs contre les emails frauduleux et les tentatives de phishing.

Décrire DMARK : DMARC utilise SPF et DKIM pour vérifier

l'authenticité des emails.