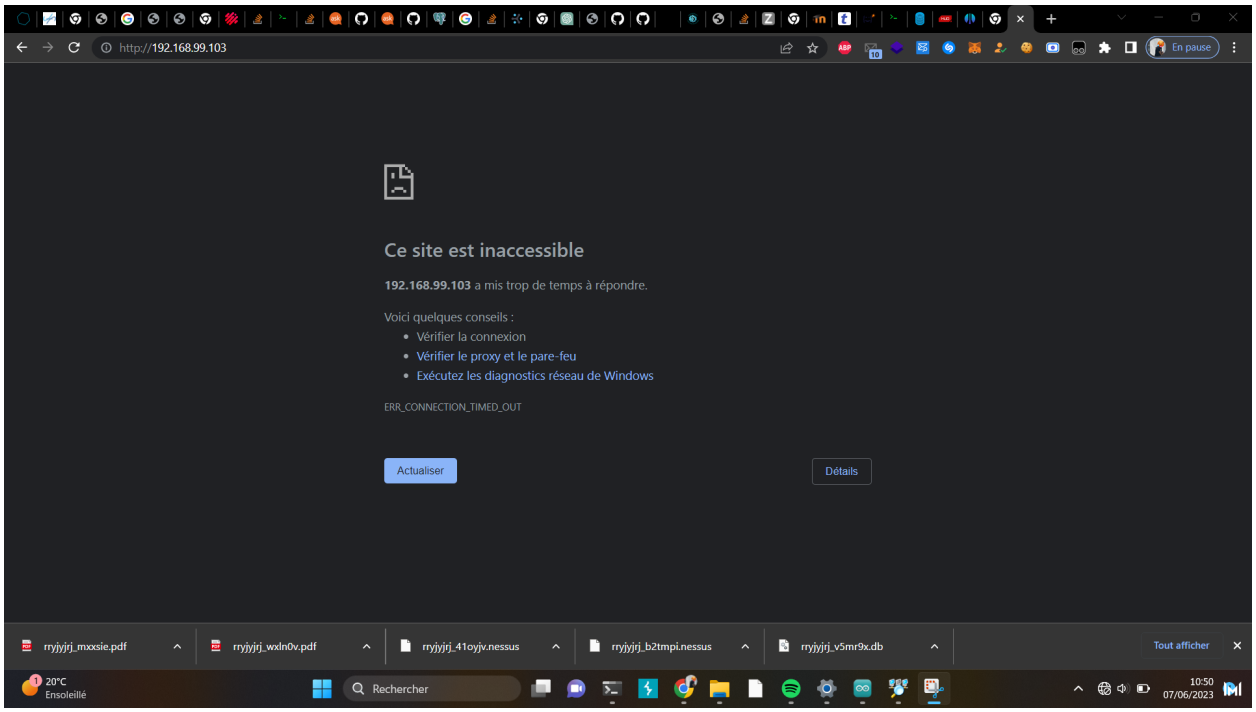
HAMDI REDOUTE AMGHAR GR:9

LOCQMEN MAXIME MOURAD

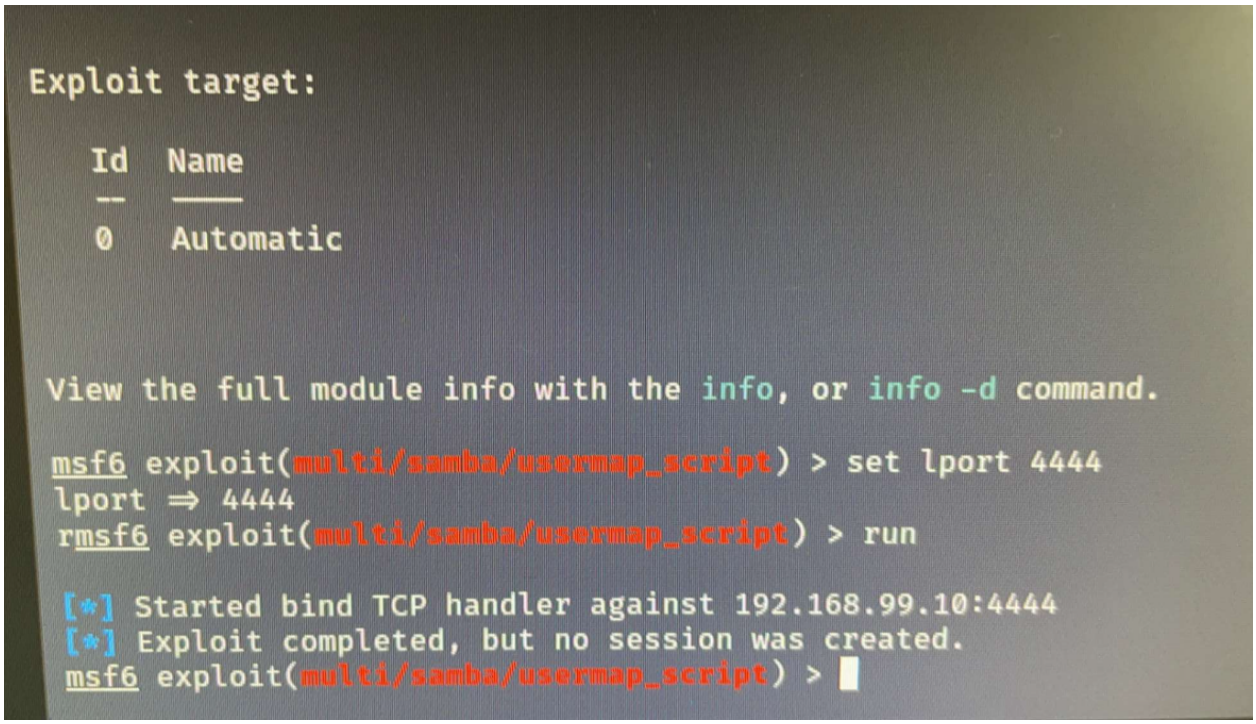
JALON 4

06 Juin 2023

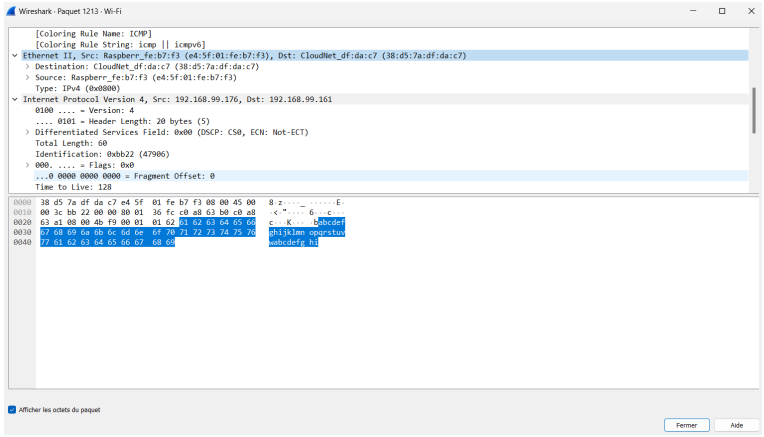
Copie d’écran de la page d’accueil du µc en mode ddos.



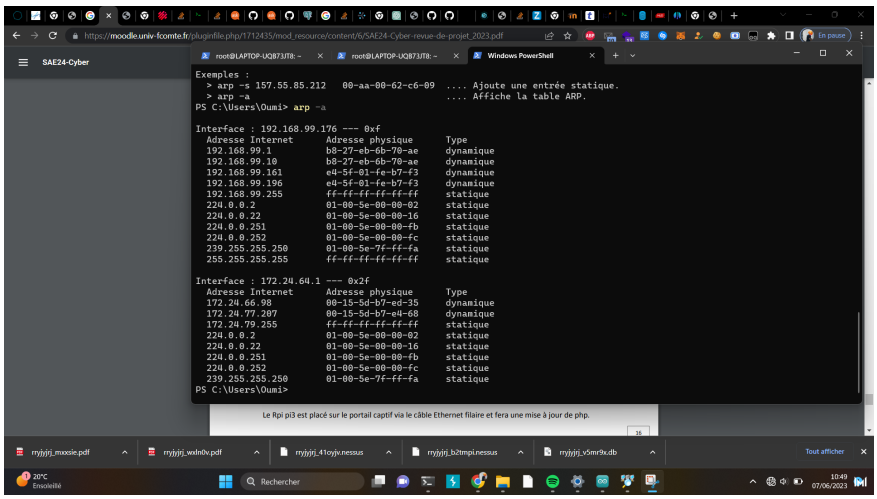
Copie d’écran de la fenêtre terminal « metasploit » lors de la tentative d’intrusion



Copie de l'acquisition wireshark montrant que l'adresse IP de la machine 1 est associée à l'adresse mac de rpi sous kali



Copie de la nouvelle table ARP commentée d'une des 2 cibles



En quoi consiste une attaque MITM ?

Une attaque MITM (Man-in-the-Middle) est une attaque informatique dans laquelle un attaquant s'insère de manière invisible entre deux parties communicantes, interceptant et potentiellement modifiant les communications entre elles. L'attaquant se positionne ainsi comme un intermédiaire entre l'émetteur légitime et le destinataire légitime, ce qui lui permet d'espionner, de modifier ou de bloquer les données échangées.

Quel est le protocole des trames envoyées et qui les envoie ?

L'attaquant peut utiliser divers outils et techniques pour mener une attaque MITM. Certains exemples courants comprennent l'empoisonnement d'ARP (Address Resolution Protocol) pour rediriger le trafic réseau, l'utilisation de logiciels malveillants pour intercepter les données, l'exploitation de failles de sécurité dans les protocoles de communication, la falsification de certificats SSL/TLS pour déchiffrer les communications chiffrées, etc.