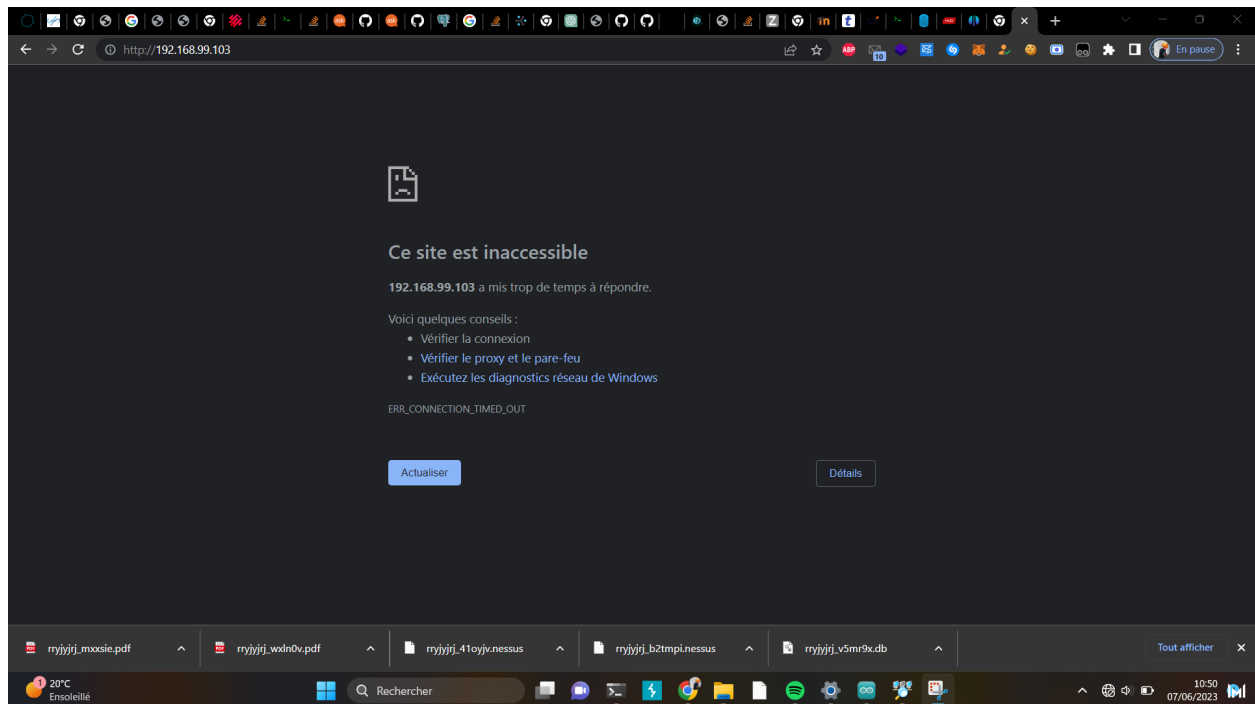


JALON 4

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

```
Exploit target:

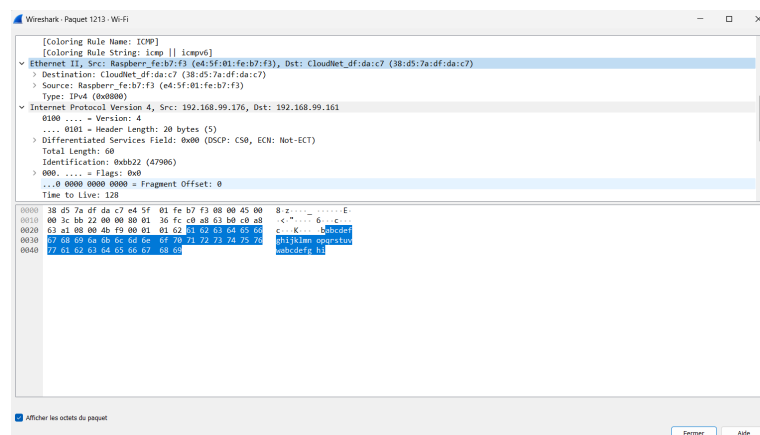
Id  Name
--  ---
0   Automatic

View the full module info with the info, or info -d command.

msf6 exploit(multi/samba/usermap_script) > set lport 4444
lport => 4444
rmsf6 exploit(multi/samba/usermap_script) > run

[*] Started bind TCP handler against 192.168.99.10:4444
[*] Exploit completed, but no session was created.
msf6 exploit(multi/samba/usermap_script) > █
```

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

```
Exemples :
> arp -s 157.55.85.212 08-aa-00-62-c6-09 .... Ajoute une entrée statique.
> arp -a ..... Affiche la table ARP.
PS C:\Users\Oumi> arp -a

Interface : 192.168.99.176 --- 0xf
Adresse Internet Adresse physique Type
192.168.99.1 b8-27-eb-6b-79-ae dynamique
192.168.99.10 b8-27-eb-6b-79-ae dynamique
192.168.99.161 e4-5f-01-fe-b7-f3 dynamique
192.168.99.196 e4-5f-01-fe-b7-f3 dynamique
192.168.99.255 ff-ff-ff-ff-ff-ff statique
224.0.0.2 01-00-5e-00-00-02 statique
224.0.0.22 01-00-5e-00-00-16 statique
224.0.0.251 01-00-5e-00-00-fb statique
224.0.0.252 01-00-5e-00-00-fc statique
239.255.255.250 01-00-5e-7f-ff-fa statique
255.255.255.255 ff-ff-ff-ff-ff-ff statique

Interface : 172.24.64.1 --- 0x2f
Adresse Internet Adresse physique Type
172.24.66.98 08-15-5d-b7-ed-3b dynamique
172.24.77.287 08-15-5d-b7-ed-00 dynamique
172.24.79.255 ff-ff-ff-ff-ff-ff statique
224.0.0.2 01-00-5e-00-00-02 statique
224.0.0.22 01-00-5e-00-00-16 statique
224.0.0.251 01-00-5e-00-00-fb statique
224.0.0.252 01-00-5e-00-00-fc statique
239.255.255.250 01-00-5e-7f-ff-fa statique
255.255.255.255 ff-ff-ff-ff-ff-ff statique

Le Rpi p3 est placé sur le portail captif via le câble Ethernet filaire et fera une mise à jour de php.
```

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.