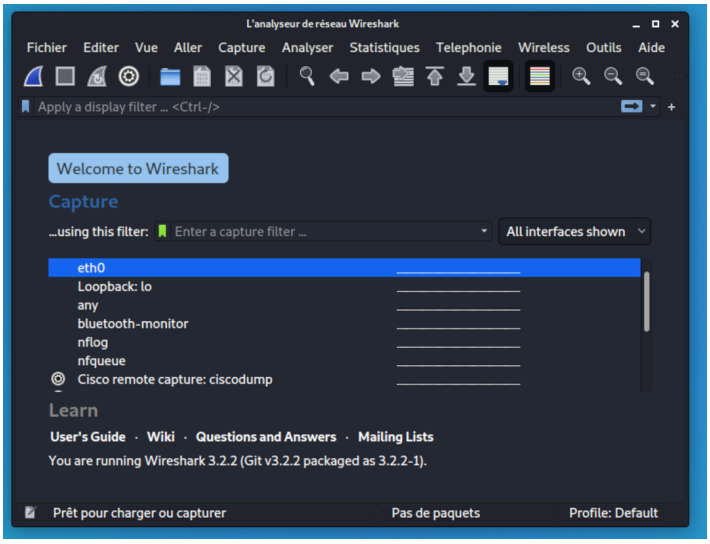
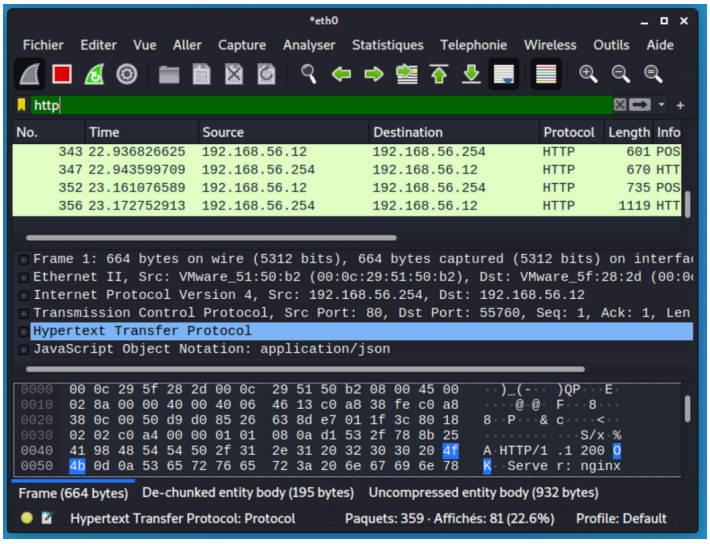
Capturer et analyser le trafic

DOCUMENT CREATED
BY ERICSSON

CYBERSÉCURITÉ

Étape 1 : Lancer Wireshark sur KaliAttaquant





Ouvrez Wireshark :

- Dans le terminal de Kali, tapez :

wireshark &

Sélectionnez l'interface réseau active :

- Dans Wireshark, choisissez l'interface correspondant à **eth0** (ou celle utilisée pour l'attaque).
- Cliquez sur **Start** pour démarrer la capture.

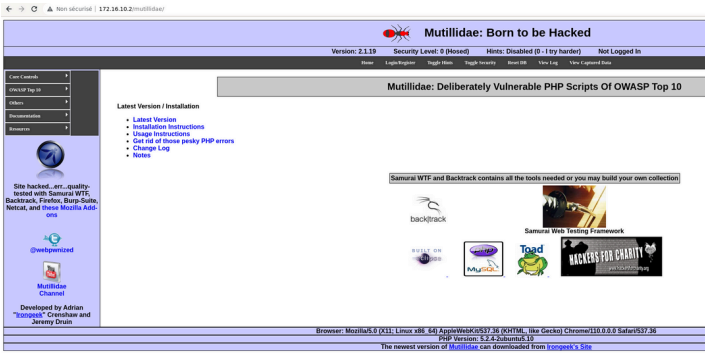
Sélectionnez l'interface réseau active :

- Dans Wireshark, choisissez l'interface correspondant à **eth0** (ou celle utilisée pour l'attaque).
- Cliquez sur **Start** pour démarrer la capture.

Configurer un filtre de capture HTTP :

- Dans le champ de filtre en haut, tapez : **http**

Étape 2 : Générer du trafic HTTP depuis la victime



Depuis DebSSHCli :

- Ouvrez un navigateur sur la machine victime.

Accédez à l'application web vulnérable Mutillidae sur Metasploitable :

http://172.16.10.2/mutillidae

Connectez-vous ou effectuez une action :

- Essayez de vous connecter à l'application avec un utilisateur fictif, ou naviguez dans l'interface.
- Si possible, créez un compte ou saisissez des données dans un formulaire.