3.06 - KaliLinux : introduction à Kali et metasploit

Durée approximative : ***8h***

Éléments du référentiel adressé :

U7 - Cybersécurité des services informatiques

- **B3.5 : Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service**

I. Installation de kali

Faire installer kali sur WSL ou une VM au choix.

Présenter Kali et ses différents outils.

II. TP1 - Intrusion système

Déroulé du TP :

red vs Blue : Fiche TP - Kali 01 - intrusion système

Remédiation :

- Faire changer les mots de passe systèmes (passwd)
- Faire sortir admin des sudoers (usermod -rG sudo admin)
- Activer le firewall : Ubuntu Server - Paramétrer UFW

- Sécuriser SSH : Ubuntu Server - Paramétrer SSH

- Sécuriser la base de donnée :
  - Appliquer :
  - Changer les mots de passes :

```
ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql_native_password BY
'YourRootPassword'; FLUSH PRIVILEGES;
```

- Sécuriser le site web :
  - chown admin:www-data des fichiers de conf
  - chmod 660 des fichiers de conf
  - empêcher le parsing du fichier en web

```
<Directory "/var/www/mysite">
   Require all denied
</Directory>
```

  - Passage en HTTPS : Apache2 - Configuration HTTPS

III. TP2 - Intrusion réseau

<todo>

IV. introduction a metasploit et armitage

utilisation de metasploit et armitage pour compromettre des infrastructures.

utiliser par exemple 'Damn Vulnerable Linux' et 'Damn Vulnerable WebApp'

Ressources associées :

GRP_SEC_GG_Gitlab-Bash / lab-VulnerableLinux · GitLab

Revision #1
Created 2026-07-17 13:33:59 UTC by Olivier
Updated 2026-07-17 13:34:01 UTC by Olivier