**Plan de cours  
Linux Sécurité**

**Mise en commun**Révision de base TCP/IP  
Triade de la sécurité  
Installation des environnements de travail  
 Installation de Debian 11  
 Utilisation judicieuse de root et sudo  
 ss et netstat

**Chiffrement et certificats**Clés symétriques et asymétriques  
Algorithmes de chiffrement  
Algorithmes de hachage (intégrité et /etc/shadow)

Certificats X.509 pour le chiffrement, la signature et l’authentification  
Autorité de certification (openSSL)

Chiffrement d'un disque dur  
Systèmes de fichiers chiffrés (btrfs)

SSH (ssh\_conf et sshd\_conf)

nginx (HTTPS et restrictions par adresses et utilisateurs)  
vsftpd (HTTPS et restrictions par adresses et utilisateurs)  
bind et chiffrement

Chiffrement de fichiers avec GPG

**Gestion de base d’un serveur  
Gestion des accès aux fichiers**Permissions spéciales  
Droits et ACL  
rsync

**Gestion des utilisateurs et groupes**Mots de passe

**Durcissement d’une station Linux**Mises à jour système  
yum|dnf, apt et zypper  
Importation de clef

PAM  
Modes d'exécution  
chroot  
Sécuriser GRUB

Surveillance des journaux  
journalctl, logwatch et logcheck

Quotas de disques

**Sécuriser un serveur visible depuis Internet**

**Outils d’attaques**Anatomie d'une attaque  
Balayages de ports avec nmap  
Wireshark

**Outils de défense**fail2ban et sshguard  
knockd  
portsentry  
rkhunter et checkstart  
chkrootkit  
lynis  
tripwire  
AIDE  
autitd  
PSAD  
tiger  
vlock

**Restriction des accès**hosts.allow et hosts.deny  
Proxy Web (squid)  
Proxy web inversé (nginx et Hproxy)

**Pare-feu et N/ID/PS**iptables, ufw et nftables  
Suricata  
pfsense (base)  
Examen de journaux