Besoins LOT 1

Fourniture de prestations de transfert de compétences de haut niveau d'expertise dans le domaine de la sécurité informatique offensive - technologies variées

Description du profil attendu pour les formateurs

1. Expérience professionnelle requise

- **Plusieurs années d'expérience** en sécurité offensive ou développement système.
- Pratique démontrable du **développement bas-niveau**.
- Pratique régulière des **tests d'intrusion**.
- Expérience en **sécurité du système concerné**.

2. Compétences techniques indispensables

- Maîtrise des **fondamentaux du système d'exploitation concerné**.
- Connaissance approfondie des techniques abordées en formation.
- Maîtrise des TP réalisés en formation.
- Très bonne compréhension des **mécanismes de sécurité** abordés en formation.
- Usage confirmé des mécanismes de sécurité abordés en formation.

3. Savoirs et savoir-faire attendus

- Capacité à **implémenter des mécanismes de sécurité offensifs** dans le système d'exploitation concerné.
- Capacité à enseigner la manipulation des techniques lors des TP.
- Capacité à guider les apprenants dans l'**implémentation complète d'un scénario offensif**.

4. Éléments différenciants (facultatif)

- Diplômes ou certifications spécialisés dans le domaine.
- Formations récentes reçues en cybersécurité.
- Pratique confirmée du débogage et de l'analyse système.
- Expérience dans des scénarios réels proches de ceux enseignés.
- Contributions open-source liées au développement ou à la cybersécurité.
- Participation à des conférences, CTF ou publications techniques avancées.

Description détaillée des prestations attendues

Ref	Libellé	Description	Travaux pratiques	Durée envisagée
TC01/01	Développement d'outils d'intrusion ciblant Linux	**Objectif pédagogique** : Appréhendez les fondements de Linux afin de savoir implémenter, via les API C bas-niveau, des mécanismes de sécurité offensifs. Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Modèle de sécurité du système d'exploitation Linux. - Format ELF. - Processus, threads et injection. - Inter-Process Communication. - Mécanismes de sécurité et isolation.	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée de 3 à 5 jours

Ref	Libellé	Description	Travaux pratiques	Durée envisagée
TC01/02	Développement d'outils d'intrusion ciblant Windows	**Objectif pédagogique** : Appréhendez les fondements de Windows afin de savoir implémenter, via les API C bas-niveau, des mécanismes de sécurité offensifs. Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Format PE et aux moyens de diagnostics sous Windows, utilisation basique d'un debugger. - Développement natif Windows (win32), injection de code, persistance et hooking. - Implémentation des techniques d'injection et de persistance. - Modèle de sécurité de Windows.	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée de 3 à 5 jours

Ref	Libellé	Description	Travaux pratiques	Durée envisagée
TC01/03	Exploitation Android	**Objectif pédagogique** : Appréhendez la recherche et l'exploitation de vulnérabilités sous Android. Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Architecture du système, Interactions entre les processus - Android userspace LPE, Reverse engineering de Java et de code natif - Android kernelspace LPE, Analyse de la surface d'attaque, Allocateur SLUB - Recherche de vulnérabilités, exploitation - Exploitation de use-after-free et de double free	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée de 3 à 5 jours

Ref	Libellé	Description	Travaux pratiques	Durée envisagée
TC01/04	Exploitation Android avancé	**Objectif pédagogique** : Maitriser la recherche et l'exploitation avancée de vulnérabilités sous Android. Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - layout d'une application - Scripting jadx, frida, jvmti - Vulnérabilités classiques SSL, deeplink, webview - Fonctionnement de ART : JVM, JIT, garbage collector	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée de 3 à 5 jours

Ref	Libellé	Description	Travaux pratiques	Durée envisagée
TC01/05	Intrusion sur les systèmes Linux	**Objectif pédagogique** : Maitriser les intrusions discrètes dans des environnements d'entreprise sous Linux, à travers l'exploitation de systèmes et l'élévation de privilèges. Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Fonctionnement d'un environnement Linux - Intrusion en mode anonyme, Intrusion en mode authentifié, reconnaissance, déplacements latéraux - Exploitation de droits administrateur local. - Compromission en profondeur, persistence, rootkit, antiforensic, Docker, LXC, SELinux.	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée de 3 à 5 jours

Ref	Libellé	Description	Travaux pratiques	Durée envisagée
TC01/06	Pentest Active Directory	**Objectif pédagogique** : Appréhendez la réalisation d'un test d'intrusion approfondi sur Microsoft Active Directory. Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - gestion des identités et des accès, stockage des secrets - extraction des objets, BloodHound, contournement de l'UAC. - élévation de privilèges au sein d'un domaine, LSASS, contournement des restrictions logicielles - forge de tickets, manipulation ACL, abus de délégation Kerberos, introduction Azure.	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée de 3 à 5 jours

Ref	Libellé	Description	Travaux pratiques	Durée envisagée
TC01/07	Pentest Active Directory avancé	**Objectif pédagogique** : Maitriser les techniques avancées de reconnaissance, mouvements latéraux, élévation de privilèges, extraction de secrets et persistance sur Microsoft Active Directory. Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - méthodes de récupération d'information, ADIDNS, détection de services via analyses LDAP et GPO, utilisation avancée de BloodHound - empoisonnement ADIDNS, WinRM et JEA, extraction de secrets LAPS. - Élévation de privilèges locale et sur domaine, - extraction de secrets, persistance, ADCS (certificats), tickets Kerberos, DSRM, golden gMSA, abus AdminSDHolder, création de skeleton key, délégation Kerberos, empoisonnement de GPO.	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée de 3 à 5 jours

Ref	Libellé	Description	Travaux pratiques	Durée envisagée
TC01/08	Cloud intrusion tactics	**Objectif pédagogique** : Maitriser les techniques d'intrusion cloud sur Google GCP, Amazon AWS et Microsoft Azure. Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - services d'infrastructure, topologie réseau, gestion des identités et des accès, mécanismes d'authentification (OAuth), Kubernetes. - GCP, Azure, AWS : architecture, IAM (permissions, rôles, principaux et politiques), authentification, utilisation de la CLI, méthodes de reconnaissance des services, abus de droits, élévation de privilèges IAM, reconnaissance réseau (VPC, firewall, VPN, peerings), post-exploitation.	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée de 3 à 5 jours

Ref	Libellé	Description	Travaux pratiques	Durée envisagée
TC01/09	Azure intrusion tactics	**Objectif pédagogique** : Maitriser les techniques d'intrusion cloud sur Microsoft Azure. Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Entra ID : identités et rôles, framework OAuth. - accès initial et discovery (AzureHound, ROADTools, Microsoft Graph CLI), Microsoft 365, API, Teams, Exchange, SharePoint, BloodHound. - mouvements latéraux et post-exploitation, étude de la journalisation. Azure DevOps : architecture, concepts CI/CD, gestion des accès. - méthodes de synchronisation (PHS, PTA, fédération), rebonds on-premise vers Intune et vice-versa, AZURESSO, ADFS, implémentation des agents Entra Connect/Cloud Sync, vol de cookies.	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée de 3 à 5 jours

Ref	Libellé	Description	Travaux pratiques	Durée envisagée
TC01/10	iOS exploitation	**Objectif pédagogique** : Maitriser la recherche et l'exploitation avancée de vulnérabilités sous Apple iOS Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Userland : NSInvocation, NSPredicate. - points d'entrées majeurs 0-click et 1-click : iMessage, WebKit, hardening, IPC - architecture système, processus critiques, permissions - coprocesseurs SEP - analyse d'un 1day : exploitation d'une corruption mémoire userland classique, étude d'une 1day Kernel - processus sandboxés (webkit)	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée de 3 à 5 jours

Ref	Libellé	Description	Travaux pratiques	Durée envisagée
TC01/11	Exploitation kernel Linux	**Objectif pédagogique** : Maitriser la recherche et l'exploitation avancée de vulnérabilités dans le noyau Linux Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Kernel internals : gestion de la mémoire, interruptions, worker/kthread - Sécurité SMAP, SMEP, KPTI, CFI - Fonctionnement et exploitation en heap - Exploitation en local	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée de 3 à 5 jours

Ref	Libellé	Description	Travaux pratiques	Durée envisagée
TC01/12	Exploitation baseband Shannon	**Objectif pédagogique** : Maitriser la recherche et l'exploitation de vulnérabilités dans les couches bas niveaux des télécommunications. Le transfert de compétences avancées traitera *a minima* les thèmes suivants : - Théorie des réseaux cellulaires 2G à 5G - Shannon Reverse - Recherche de vulnérabilité manuelle - Emulateur simpliste - Exploitation OTA, rebond vers l'AP	Travaux pratiques sur l'ensemble des méthodes et outils présentés.	Durée de 3 à 5 jours