SYNACKTIV

FORMATIONS

2023.08

Présentation

Synacktiv prend à cœur le partage de son expérience en cybersécurité, acquise au fil des années, en dispensant des formations inter-entreprises. Alliant enseignement théorique et travaux pratiques, nos formations ont été conçues pour offrir une expérience d'apprentissage unique et enrichissante, et s'adressent principalement à des professionnels de la sécurité des systèmes d'information : pentesteurs, experts en retro-ingénierie, analystes SOC, analystes CSIRT, administrateurs systèmes, architectes sécurité, développeurs, etc.

Chaque session est animée par deux formateurs expérimentés qui assureront une compréhension optimale tout en apportant des retours d'expérience concrets. Tout le matériel nécessaire à la réalisation des travaux pratiques sera fourni aux étudiants et chacun disposera d'un environnement individuel afin d'assurer une expérience d'apprentissage immersive. Les supports de cours seront transmis au format PDF, permettant aux participants de les consulter à tout moment et de les utiliser comme référence.

Les formations se déroulent dans nos locaux parisiens, dans un environnement professionnel et confortable qui favorisera la concentration des apprenants. Les déjeuners et boissons sont inclus, ainsi qu'un repas au restaurant le dernier jour de formation.

- 2 formateurs expérimentés
- 7 à 12 participants
- Minimum 50 % de pratique
- Travaux pratiques au sein de labs individuels
- Matériel fourni (ordinateurs portables)
- Supports de cours fournis
- Dans nos locaux 5 bd Montmartre, Paris 75002
- Repas et boissons inclus

Pentest

Pentest Découverte

Obtenez les compétences nécessaires à la compréhension des principales étapes d'une intrusion. Reconnaissance, applications web, systèmes Linux et Windows, étapes de post-exploitation, cette formation fournit un socle essentiel à tout professionnel de sécurité.

5 jours | Junior

Pentest Active Directory 1

Découvrez les fondamentaux de la sécurité des environnements Active Directory au travers de cette formation offensive. D'un accès anonyme et jusqu'à la compromission complète des infrastructures, devenez autonome en intrusion de réseaux d'entreprises.

5 jours | Intermédiaire

Pentest Linux

Maîtrisez les techniques d'intrusion sur des infrastructures Linux au travers de cette formation offensive. D'un accès anonyme et jusqu'à la compromission complète de l'environnement, devenez autonome en intrusion de réseaux d'entreprises.

5 jours | Intermédiaire

Pentest Active Directory 2

Approfondissez vos compétences d'intrusion en environnements Active Directory avec cette formation de niveau confirmé. Découvrez les techniques d'exploitation avancées et maîtrisez la compromission de réseaux d'entreprises complexes.

5 jours | Avancé

Pentest Cloud

Initiez-vous à la compromission de réseaux modernes avec cette formation sur les infrastructures cloud. GCP, AWS, Azure et Kubernetes, découvrez les mécanismes caractéristiques de ces technologies récentes, avec la posture d'un attaquant.

5 jours | Intermédiaire

Pentest Web Black Box

Étudiez les mécanismes de sécurité des applications web modernes et les méthodes d'exploitation avancées permettant de les contourner. PHP, Java, Python et Perl, maîtrisez la compromission d'applications web complexes.

5 jours | Intermédiaire

Pentest

Pentest Web White Box

Obtenez les compétences nécessaires à la recherche de vulnérabilités web Java et PHP. Étude de frameworks et outils d'analyse statique et dynamique, cette formation permet aux pentesteurs et développeurs d'optimiser leur recherche de vulnérabilité en boîte blanche.

5 jours | Intermédiaire

Pentest d'applications Android

Découvrez les méthodologies et techniques d'analyse des applications Android. Architecture des applications, points d'entrée, analyses statique et dynamique, maîtriser le pentest en environnement Android.

2 jours | Junior

Anti-Forensic

Maîtrisez les techniques de furtivité permettant de dissimuler vos actions sur les environnements Linux et Active Directory. Altération et suppression de journaux, ne laissez aucune trace de votre intrusion.

3 jours | Intermédiaire

Password Cracking

Étudiez les méthodes d'optimisation du cassage de mots de passe avec les outils John et Hashcat. Règles de mutation, masques, attaques prince et siga, devenez un véritable expert des mots de passe.

1 jour | Junior

Reverse

Développement Offensif Windows

Appréhendez les fondements du système d'exploitation Windows afin de savoir implémenter, via les API C bas-niveau, des mécanismes de sécurité offensifs.

5 jours | Intermédiaire

Développement Offensif Linux

Appréhendez les fondements du système d'exploitation Linux afin de savoir implémenter, via les API C bas-niveau, des mécanismes de sécurité offensifs.

5 jours | Intermédiaire

Android for Security Engineers

Découvrez de façon approfondie et à l'aide d'exercices pratiques, le fonctionnement d'Android et de ses mécanismes de sécurité.

5 jours | Intermédiaire

iOS for Security Engineers

Découvrez de façon approfondie et à l'aide d'exercices pratiques, le fonctionnement d'iOS et de ses mécanismes de sécurité.

5 jours | Intermédiaire

IDA Avancé

Familiarisez-vous avec les fonctionnalités avancées d'IDA, son API et son écosystème. Apprenez comment développer des scripts et plugins pour étendre ses fonctionnalités.

5 jours | Intermédiaire

Intrusion Hardware

Apprenez à apprivoiser un PCB : reconnaître des composants, identifier des testpads et inférer puis interagir avec des protocoles (UART, JTAG/SWD, SDIO, SPI). Utiliser les outils et matériels actifs/passifs (analyseur logique, FT2232H, JTAGulator, OpenOCD).

5 jours | Intermédiaire

Forensic

Forensic Windows

Maîtrisez l'investigation numérique des systèmes Windows 10 et 11 en apprenant à identifier et caractériser les malveillances associées, autant dans le cadre d'un incident de sécurité que d'une recherche de compromission (levée de doute, hunting).

5 jours | Junior

Forensic Linux

Maîtrisez l'investigation numérique des systèmes Linux en apprenant à identifier et caractériser les malveillances associées, autant dans le cadre d'un incident de sécurité que d'une recherche de compromission (levée de doute, hunting).

5 jours | Junior

Forensic Mobile

Découvrez l'investigation numérique de système d'exploitation mobile Android et iOS en étudiant les techniques d'acquisition de données, la découverte d'applications malveillantes ou encore les artefacts de fonctionnement du téléphone.

5 jours | Junior

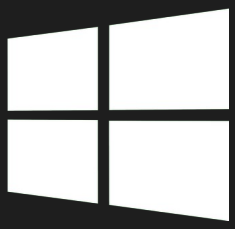
Analyse de Malwares Windows

Découvrez l'analyse de code malveillant dans le cadre d'un incident de sécurité au travers de situations diverses et de cas réels de modes opératoires d'attaquants.

5 jours | Intermédiaire

Pentest Découverte

5 jours | Niveau junior



Description

La réalisation de tests d'intrusion permet une mise en situation réaliste des mécanismes de défense et représente par conséquent une étape clé dans la sécurisation des systèmes d'information. Cette formation d'introduction au pentest vise à fournir une compréhension approfondie de l'audit de sécurité en abordant les différentes étapes d'une intrusion.

Au cours de ces cinq jours de formation, les participants seront exposés à quatre modules de cours couvrant la reconnaissance, les applications web, les systèmes Linux et Windows, et les techniques de post-exploitation. Chaque module sera illustré par des travaux pratiques guidés permettant d'appliquer les notions théoriques enseignées. Enfin, la formation se conclura par une mise en situation réaliste sur un réseau d'entreprise.

- 5 jours (35 heures)
- 4 modules de cours couvrant les étapes principales d'un test d'intrusion
- Reconnaissance, applications web, Linux, Windows, post-exploitation
- 20 exercices d'application
- 1 intrusion guidée sur environnement d'entreprise complet (10 machines)

Public et prérequis

Cette formation a été conçue pour des personnes n'ayant aucune expérience préalable sur les tests d'intrusion. Elle s'adresse principalement aux pentesteurs débutants, administrateurs systèmes, architectes sécurité et développeurs, mais également à tout profil technique souhaitant enrichir son parcours professionnel avec une composante sécurité.

- Pentesteurs débutants
- Administrateurs systèmes
- Architectes sécurité
- Développeurs

Des connaissances basiques de l'environnement Unix et des langages web sont recommandées.

Contenu

Jour 1

Introduction aux méthodes de reconnaissance : énumération DNS et HTTP, scans de services. Présentation des principaux outils d'intrusion : Metasploit, Burp Suite. Vulnérabilités sur les applications web : injections SQL, XSS (Cross-Site Scripting), XXE (XML eXternal Entities), SSRF (Service-Side Request Forgery), upload de fichiers, désérialisation, avec différents exercices de mise en pratique.

Jour 2

Mise en pratique sur des applications web complexes : reconnaissance, exploitation et élévations de privilèges jusqu'à l'obtention d'un accès aux serveurs. Élévation de privilèges sur les systèmes Linux : fondamentaux (gestion des identités et des accès), reconnaissance et exploitation (permissions, configurations sudo, tâches planifiées, unités systemd, kernel) et technologies de conteneurisation (Docker, LXC/LXD).

Jour 3

Élévation de privilèges sur les systèmes Windows : fondamentaux (gestion des identités et des accès, gestion des secrets), reconnaissance et exploitation (permissions, configurations de services, tâches planifiées, vulnérabilités publiques). Mise en pratique sur des serveurs depuis un accès non privilégié.

Jours 4 et 5

Étapes de post-exploitation : extraction de secrets (disque, mémoire), installation de portes dérobées et déplacements latéraux (rebond réseau, proxy SOCKS, forward de ports). Mise en situation sur un réseau d'entreprise.

Pentest Active Directory 1

5 jours | Niveau intermédiaire

Description

Pour de nombreuses entreprises, l'Active Directory constitue le cœur de la gestion des identités et des accès. Son omniprésence au sein des systèmes d'information en fait une cible de choix pour les attaques informatiques et les tests d'intrusion sont un composant clé de sa défense contre les menaces.

Au cours de cette formation de cinq jours, vous acquerrez les compétences nécessaires à la réalisation d'un test d'intrusion Active Directory approfondi. En suivant les cinq modules d'apprentissage, les étudiants apprendront la méthodologie et les techniques utilisées par nos experts lors d'une intrusion, depuis un accès anonyme jusqu'à la compromission totale de l'environnement et la persistance des accès en son sein. Afin de mettre en pratique les concepts enseignés, les apprenants seront guidés au travers de deux environnements d'entreprise complets.

- 5 jours (35 heures)
- 5 modules de cours couvrant les étapes d'une intrusion réaliste + 1 module Azure
- 2 environnements d'entreprise avec plus de 30 machines

Public et prérequis

Cette formation est adaptée pour des personnes ayant des notions de sécurité offensive mais pas d'expérience préalable sur les environnements Active Directory. Elle s'adresse principalement aux pentesteurs, administrateurs systèmes et architectes sécurité, mais également à tout profil technique souhaitant enrichir son parcours professionnel avec une composante sécurité.

- Pentesteurs
- Administrateurs système
- Architectes sécurité

Des notions de sécurité offensive et de bonnes connaissances réseau et Unix sont recommandées.

Contenu

Jour 1

Bases théoriques des mécanismes de sécurité : fonctionnement des mécanismes d'administration (RPC, SMB, WMI, RDP, WinRM), gestion des identités et des accès, stockage des secrets, protocoles d'authentification réseau (NTLM, Kerberos), hiérarchie et liens de confiance Active Directory. Techniques de reconnaissance et d'exploitation depuis un accès anonyme : énumération, empoisonnement de protocoles réseau, relaying.

Jour 2

Reconnaissance sur le domaine depuis un accès non privilégié : extraction des objets (utilisateurs, groupes, machines, GPO) et cartographie avec BloodHound. Élévation de privilèges locale : énumération et exploitation (services locaux, tâches planifiées, ACLs, vulnérabilités publiques), techniques de contournement de l'UAC.

Jour 3

Élévation de privilèges au sein d'un domaine : extraction de secrets (registres, LSASS, DPAPI), rejeu d'authentification, kerberoasting, abus de chemins de contrôle. Contournement de restrictions logicielles : AppLocker, évasion de bureaux restreints (Citrix, Kiosque RDP).

Jour 4

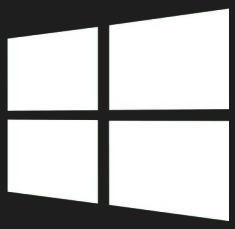
Étapes de post-exploitation depuis un accès privilégié sur le domaine : extraction de secrets (NTDS, DPAPI), forge de tickets (silver et golden tickets), manipulation d'ACL, persistance au sein de l'environnement et effacement des traces. Extension de la compromission : études des relations de confiance inter-domaines et inter-forêts, abus de délégation Kerberos.

Jour 5

Introduction à Azure : concepts fondamentaux (terminologie, gestion des identités et des accès), intégration avec l'Active Directory (synchronisation des identités, mécanisme Single Sign-On), étapes de reconnaissance et compromission depuis l'environnement on-premise.

Pentest Active Directory 2

5 jours | Niveau avancé



Description

Pour de nombreuses entreprises, l'Active Directory constitue le cœur de la gestion des identités et des accès. Son omniprésence au sein des systèmes d'information en fait une cible de choix pour les attaques informatiques et les tests d'intrusion sont un composant clé de sa défense contre les menaces.

Au cours de cette formation de cinq jours, vous approfondirez vos compétences d'intrusion en environnement Active Directory, ainsi que sur des environnements hybrides Azure. Guidé par nos experts, étudiez des techniques avancées de reconnaissance, mouvements latéraux, élévation de privilèges, extraction de secrets et persistance. Afin de mettre en pratique les concepts enseignés, les apprenants seront mis en situation sur deux environnements d'entreprise complets.

- 5 jours (35 heures)
- 5 modules de cours couvrant les étapes d'une intrusion réaliste
- 2 environnements d'entreprise avec plus de 40 machines et un environnement Azure

Public et prérequis

Cette formation est destinée aux personnes ayant déjà de bonnes connaissances sur les environnements Active Directory. Elle s'adresse principalement aux pentesteurs, administrateurs systèmes et architectes sécurité.

- Pentesteurs
- Administrateurs système
- Architectes sécurité

De bonnes connaissances réseau et Unix sont également recommandées.

Contenu

Jour 1

Rappel des fondamentaux : mécanismes Active Directory, principes d'intrusion généraux et spécifiques à ces environnements. Reconnaissance et premières actions depuis un accès authentifié : méthodes de récupération d'information (ADIDNS, détection de services via analyses LDAP et GPO) utilisation avancée de BloodHound (Cypher queries).

Jour 2

Mouvements latéraux : empoisonnement ADIDNS, WinRM et JEA, extraction de secrets LAPS, gMSA/sMSA, abus de liens de confiance MS-SQL, relaying NTLM (dissection, relai cross-protocoles, WebDAV), coercing d'authentification, relai Kerberos, pivots inter-forêts, pivots vers Azure (PHS, PTA, ADFS), pivots depuis Azure (Intune).

Jour 3

Élévation de privilèges locale : access token et impersonation, étude des vulnérabilités potatoes. Élévation de privilèges sur le domaine : étude et abus des ACL, exploitation avancée de délégation Kerberos, ADCS ESC1 à 11, abus de groupes privilégiés, analyse de vulnérabilités publiques.

Jour 4

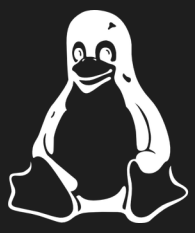
Extraction de secrets : méthodes et outils d'extraction LSASS, usurpation de tokens, analyse des secrets de bases de registres, implémentation DPAPI, extraction de bases KeePass.

Jour 5

Persistance : ADCS (certificats), tickets Kerberos (golden, diamond, sapphire), DSRM, golden gMSA, abus AdminSDHolder, création de skeleton key, délégation Kerberos, empoisonnement de GPO.

Pentest Linux

5 jours | Niveau intermédiaire



Description

Linux est un système d'exploitation très largement utilisé, notamment pour les serveurs mais également pour les postes de bureautique et les systèmes embarqués, tels que les équipements réseau. La gestion d'une infrastructure Linux repose sur des mécanismes et des méthodes d'administration dont la compréhension est essentielle pour les attaquants.

Au travers de ces cinq jours de formation, les participants seront exposés à quatre modules de théorie détaillant la méthodologie d'une intrusion depuis un accès anonyme jusqu'à la compromission de l'infrastructure, avec un intérêt particulier pour la limitation de l'empreinte. Un module complémentaire sera également dédié aux systèmes durcis (AppArmor, SELinux). Ces notions seront appliquées tout au long de la semaine sur deux réseaux d'entreprise complexes, issus d'intrusions réellement menées par nos experts.

- 5 jours (35 heures)
- 4 modules de cours sur les étapes d'une intrusion réaliste + 1 module sur les systèmes durcis
- 2 environnements d'entreprise avec plus de 30 machines

Public et prérequis

Cette formation est adaptée pour des personnes ayant des notions de sécurité offensive mais pas d'expérience préalable sur l'intrusion d'environnements Linux d'entreprise. Elle s'adresse principalement aux pentesteurs, administrateurs systèmes et architectes sécurité, mais également à tout profil technique souhaitant enrichir son parcours professionnel avec une composante sécurité.

- Pentesteurs
- Administrateurs système
- Architectes sécurité

Des notions de sécurité offensive et de bonnes connaissances réseau et Unix sont recommandées.

Contenu

Jour 1

Concepts fondamentaux : gestion des identités et des accès, mécanismes de sécurité (ACL étendues, attributs standards et étendus, capabilities), conteneurisation (namespaces, cgroups, seccomp, implémentations Docker et LXC / LXD), méthodes d'administration.
Techniques de reconnaissance et d'exploitation depuis un accès anonyme : cartographie réseau, protocoles de résolution de noms (mDNS / DNS), interceptions (ARP spoofing).

Jour 2

Reconnaissance depuis un accès non privilégié : énumération système et réseau (services, sessions, configurations, LDAP, partages NFS / Samba), détection de conteneurisation.
Élévation de privilèges locale : configurations sudo avancées, tâches planifiées, capabilities, exploitation kernel (analyse de vulnérabilités publiques, adaptation de code d'exploitation, implémentation de protections).

Jour 3

Étapes de post-exploitation : extraction de secrets sur le disque, dissection de la mémoire et abus de composants de mise en cache (agents SSH / GPG, DBUS Secret Service API), empoisonnement des authentifications (OpenSSH, PAM, sudo), déplacements latéraux (rebond réseau, proxy SOCKS, forward de ports).

Jour 4

Compromission en profondeur : installation de mécanismes de persistance avancés (rootkits userland et kernel), gestion de l'empreinte sur le système (introduction anti-forensic).

Jour 5

Compromission de systèmes durcis : implémentation et configuration des LSM AppArmor et SELinux, analyse et contournement du durcissement.

Pentest Cloud

5 jours | Niveau intermédiaire

Description

Les technologies cloud sont progressivement intégrées dans le système d'information des entreprises. Elles apportent de nombreux mécanismes de sécurité parfois difficile à appréhender et forçant les attaquants à repenser leurs méthodes d'intrusion.

Au cours de cette formation de cinq jours, les participants seront exposés aux concepts des trois fournisseurs cloud principaux : GCP (Google), AWS (Amazon) et Azure (Microsoft). Après avoir étudié les fondamentaux qui leur sont communs, les spécificités d'implémentation seront détaillées et illustrées au travers d'environnements complets permettant de s'initier aux techniques d'intrusion cloud. Un module complémentaire sera également dédié aux infrastructures Kubernetes.

- 5 jours (35 heures) modulaires (découpage possible)
- 3 modules de cours sur GCP, AWS et Azure + 1 module dédié à Kubernetes
- 4 environnements complets et individualisés

Public et prérequis

Cette formation est adaptée pour des personnes ayant des notions de sécurité offensive mais pas d'expérience préalable sur les environnements cloud. Elle s'adresse principalement aux pentesteurs, administrateurs systèmes, architectes sécurité et développeurs, mais également à tout profil technique souhaitant enrichir son parcours professionnel avec une composante sécurité.

- Pentesteurs
- Administrateurs système
- Architectes sécurité
- Développeurs

De bonnes connaissances réseau et Unix et des notions d'intrusion web sont recommandées.

Contenu

Jour 1

Fondamentaux : terminologie cloud, services d'infrastructure, topologie réseau, gestion des identités et des accès, mécanismes d'authentification (OAuth), rappels des mécanismes de sécurité Linux (namespaces, cgroups, seccomp, LSM), recherche d'accès en source ouverte.

Jour 2

Google Cloud Plateform : architecture (organisation, dossier, projets, ressources, régions et zones), IAM (permissions, rôles, principaux et politiques), authentification (OAuth 2.0, JWT), utilisation de la CLI gcloud, méthodes de reconnaissance des services, abus de droits sur les buckets, implémentations App Engine et Instance (abus des metadata), élévation de privilèges IAM, reconnaissance réseau (VPC, firewall, VPN, peerings), post-exploitation (délégation sur le domaine, rebond sur Workspace), analyse des évènements.

Jour 3

Amazon Web Services : architecture (organisation, comptes), IAM (types d'identité, assumation de rôle, politiques), utilisation de la CLI aws, méthodes de reconnaissance des services, énumération non-authentifiée des identités, abus de droits sur les buckets S3, EC2 (metadata, mouvements latéraux et empoisonnement des agents SSM), Lambdas (runtime API, persistance, exfiltration de données), Cognito (user et identity pools) élévation de privilèges IAM, reconnaissance réseau (VPC, network ACL, security groups), persistance (modification de politiques IAM, role chain juggling).

Jour 4

Azure : architecture (tenants, management groups, subscriptions), Azure AD (types d'identité, gestion des accès, rôles Azure AD et RBAC), synchronisation en environnement hybride (PHS, PTA, ADFS), reconnaissance non-authentifiée, utilisation de la CLI azure et module Az, reconnaissance authentifiée (ROADrecon, AzureHound), implémentation blob storage, key vault, machines virtuelles, mouvements latéraux (Vnet, bastions).

Jour 5

Kubernetes : architecture (conteneurs, pods, nodes, services internes), reconnaissance, authentification (mot de passe, certificats, tokens) et autorisations (node, ABAC, RBAC, WebHook), utilisation de la CLI kubectl, pod templates et contrôleurs, escapes (namespaces, PSP, PSA), concepts réseau (ingress, pod to pod, CNI, politiques).

Pentest Web Black Box

5 jours | Niveau intermédiaire

Description

Les applications web représentent une grande partie de la surface d'attaque exposée sur Internet. Au fil de l'évolution des technologies, de nouvelles vulnérabilités et méthodes d'exploitation continuent d'apparaître, complexifiant par conséquent les étapes d'intrusion.

Lors de cette formation de cinq jours, les participants seront amenés à étudier le fonctionnement des mécanismes de sécurité implémentés dans les applications web récentes. Les différents exercices issus du retour d'expérience de nos experts leur permettront d'affiner leurs méthodes d'intrusion pour l'exploitation de vulnérabilités complexes. Enfin, les apprenants pourront appréhender les spécificités des langages et frameworks Java, PHP, Python et Perl, à l'aide de modules dédiés.

- 5 jours (35 heures) modulaires (découpage possible)
- 9 modules de cours dont Java, PHP, Python et Perl
- Plus de 30 exercices pratiques

Public et prérequis

Cette formation est adaptée pour des personnes ayant une expérience préalable en techniques intrusion web. Elle s'adresse principalement aux pentesteurs et développeurs.

- Pentesteurs
- Développeurs

De bonnes connaissances réseau et Unix sont également recommandées.

Contenu

Jour 1

BurpSuite : utilisation avancée, limitations, raccourcis et mécanismes d'automatisation, extensions (AuthMatrix, Hackvertor, ActiveScan++). Reconnaissance : énumération DNS, vhosts, fuzzing, identification des composants web.

Jour 2

Mécanismes de sécurité fondamentaux : authentification (OAuth, JWT, SAML), gestion des sessions (cookies, tokens, viewstates), réinitialisation de mot de passe, contrôle d'accès, gestion des entrées utilisateur. Exploitation avancée : XXE, SSRF, injections, SSTI, prototype pollution, attaques cryptographiques, GraphQL, spécificités des environnements cloud.

Jour 3

Java : reconnaissance et identification de frameworks (extensions, endpoints, en-têtes, interfaces d'administration), exploitation de vulnérabilités spécifiques (XXE, injections HQL, désérialisation, expression languages, JNDI, path traversals).

Jour 4

PHP : reconnaissance et identification de frameworks (endpoints, erreurs, en-têtes), fonctions de sécurité (gestion des sessions, sanitization), exploitation de vulnérabilités spécifiques (type juggling, stream wrappers et filtres, désérialisation et conception de POP chains complexes, XXE), post-exploitation (exécution fileless, contournements de disable_functions).

Jour 5

Python Django : exposition de la surface d'attaque (mode debug, signature des cookies, injection de templates DTL et Jinja2). Perl : rappels fondamentaux, reconnaissance, exploitation de comportements spécifiques (fonctions natives, types de données, NULL bytes), analyses de vulnérabilités dans Twiki et Bugzilla.

Pentest Web White Box

5 jours | Niveau intermédiaire

Description

La complexité des applications web modernes nécessite une forte compréhension des mécanismes natifs des langages utilisés. Les méthodes d'analyse de code source permettent d'optimiser la recherche de vulnérabilités lors d'une intrusion.

Au cours de cette formation de cinq jours, vous acquerrez les compétences nécessaires à l'identification de vulnérabilités complexes au sein du code source d'applications Java et PHP. En s'appuyant sur de nombreux cas pratiques sur des frameworks répandus tels que Spring ou Symfony, les participants apprendront à optimiser leur recherche à l'aide d'outils d'analyse statique et dynamique.

- 5 jours (35 heures) modulaires (découpage possible)
- 7 modules couvrant les spécificités des langages Java et PHP
- Cas pratiques sur les frameworks Spring, Struts, Hibernate, Zend, Symfony et Laravel

Public et prérequis

Cette formation est adaptée pour des personnes ayant de bonnes connaissances des technologies web et des vulnérabilités associées. Elle s'adresse principalement aux pentesteurs et développeurs souhaitant améliorer leur méthode de recherche.

- Pentesteurs
- Développeurs

De bonnes connaissances réseau et Unix sont recommandées.

Contenu

Jour 1

Méthodologie : approches top-down, bottom-up et hybrides, analyses statique et dynamique, outillage. Applications Java classiques : structure d'une application (composants Class, JAR, JSP, configurations), formats (WAR, EAR), configuration web.xml (mapping URI, filtres, hooks, contraintes de sécurité), application des approches top-down et bottom-up, outillage.

Jour 2

Applications Java basées sur des frameworks : identification, analyse des architectures et implémentations Spring (JavaBean, modèle MVC, SpEL, AOP, Security), Struts2 (actions, intercepteurs, vues, OGNL, configuration, SMI / DMI, devMode) et Hibernate (définition des modèles, configuration des connecteurs, ORM, HQL et transformation SQL), aperçu d'autres frameworks communs (JavaServer Faces, VAADIN, SEAM, Play).

Jour 3

Instrumentation Java : Byteman, AspectJ et JDWP. Applications Java closed-source : méthodes et outillage pour décompilation.

Jour 4

Applications PHP basées sur des frameworks : mise en place de l'environnement d'analyse (IDE, Xdebug, configuration PHP), analyse des architectures et implémentations Symfony (ORM, routing, contraintes, authentification et contrôle d'accès), Zend (routing, authentification et contrôle d'accès), Laravel (structure, configuration). POP chains : concepts, recherche et développement

Jour 5

Applications PHP closed-source : mécanismes (scrambling, chiffrement), analyse des implémentations Blenc et IonCube, utilisation d'outils d'extraction et d'analyse de code protégé (VLD, Xdebug, Dtrace, AOP, APD, RunKit).

Pentest d'applications Android

2 jours | Niveau junior

Description

Android est l'un des systèmes d'exploitation pour mobile les plus répandus sur le marché et sur lequel de nombreuses applications sont développées. Cet écosystème définit des normes d'implémentation, de communication, de stockage et des mécanismes de sécurité qui lui sont propre et que les développeurs doivent respecter.

Au cours de cette formation de deux jours, les participants découvriront les spécificités d'implémentation des applications Android et étudieront les méthodologies et techniques employées pour les analyser.

- 2 jours (14 heures)
- 5 modules de cours
- 9 applications Android

Public et prérequis

Cette formation est adaptée pour des personnes ayant des notions de sécurité offensive mais pas d'expérience préalable sur l'audit d'applications Android. Elle s'adresse principalement aux pentesteurs et développeurs Android.

- Pentesteurs
- Développeurs Android

Des notions de sécurité offensive et des connaissances réseau et Unix sont recommandées.

Contenu

Jour 1

Fondamentaux : fonctionnement d'une application et de l'écosystème Android (services, intents, keystore, format des APK, fichier de cache, shared prefs, mécanisme de backup). Analyse statique : analyse des permissions et des interactions avec le système et les autres applications, présentation des outils d'analyse et explication des artefacts courant donnant de l'information sur les activités d'une application.

Jour 2

Analyse dynamique : architecture d'une application au runtime, mécanisme d'interception et d'instrumentation de code Java, présentation de Frida et d'Objection pour automatiser des contournements classiques ou obtenir de l'information. Cas pratiques : mise en applications sur des applications Android.

Anti-Forensic

3 jours | Niveau intermédiaire

Description

Les systèmes d'information modernes collectent en permanence un large volume d'évènements pouvant être générés au cours d'une intrusion. Afin de préserver la discrétion lors d'une compromission, il est nécessaire de comprendre les différents artefacts impliqués afin de les manipuler ou les effacer.

Au cours de cette formation de trois jours, les participants étudieront les différents mécanismes de journalisation présents sur les systèmes Linux et Windows, notamment au sein d'une infrastructure Active Directory. Des méthodes de contournement, de dissimulation et de suppression seront ensuite enseignées afin de maîtriser l'art de la discrétion. Ces notions seront illustrées à l'aide de travaux pratiques.

- 3 jours (21 heures)
- 2 modules de cours sur l'effacement des traces en environnements Active Directory et Linux
- Nombreux exercices d'application

Public et prérequis

Cette formation est adaptée pour des personnes ayant de bonnes notions d'intrusion sur les systèmes Windows et Linux. Elle s'adresse principalement aux pentesteurs, administrateurs systèmes et réseau, et architectes sécurité.

- Pentesteurs
- Administrateurs système et réseau
- Architectes sécurité

Contenu

Jour 1

Fondamentaux Windows : types de journaux (System, Security, Setup), format EVTX, API de journalisation, forward d'évènements (Event Log Collector, MDI), étude des permissions d'accès, analyse du service de journalisation, outils de manipulation des journaux. Journalisation des mouvements latéraux : évènements générés via RDP, WMI, SMB, DCOM. Suppression des traces : modification des journaux nativement et manuellement, timestomping, masquerading, altération des services de journalisation, fichiers prefetch, ShimCache, AmCache, Shadow copies, USN, SRUM, ShellBags.

Jour 2

Persistance discrète : dissimulation de tâches planifiées, fileless WMI, camouflage de services, abus de paramètres de registre. Exfiltration de données : BITS. Active Directory : étude des évènements générés par différentes actions (password spraying, requêtes LDAP, Diamond / Sapphire tickets, extraction du NTDS) et méthodes à privilégier.

Jour 3

Linux et Solaris : types d'évènements (établissement de session, obtention de TTY), historiques, programmes d'administration (su, sudo), auditd et contournements. Persistance : développement de backdoors dans les composants applicatifs ou d'administration (PAM, Apache), injection de librairies, développement de méthodes d'exécution en mémoire.

Password Cracking

1 jour | Niveau junior

Description

Les mots de passe constituent encore aujourd'hui un composant essentiel de la sécurité des systèmes d'informations. Lors des intrusions, différents types d'empreintes de mots de passe sont récupérés et pouvoir les casser dans un temps restreints peut s'avérer décisif.

Cette formation a pour objectif de présenter les techniques et les outils permettant de casser le plus rapidement des empreintes de mots de passe. Un historique des évolutions du stockage des mots de passe sera également présenté, afin de mettre en lumière les mauvais exemples et erreurs commises dans des projets répandus.

- 1 jour (6 heures)
- Techniques d'optimisation du cassage de mots de passe
- Datasets fournis

Public et prérequis

Cette formation est adaptée pour des personnes n'ayant pas de connaissances préalables sur le cassage de mots de passe. Elle s'adresse principalement aux pentesteurs, administrateurs systèmes, et développeurs.

- Pentesteurs
- Administrateurs système
- Développeurs

Contenu

Théorie sur le stockage et la génération de mots de passe : type de stockage, fonctions de hachage, attaques sur les fonctions, génération de candidats, technologies de calcul. Historique des algorithmes. Série d'exercices pratiques : identification des algorithmes dans du code source, prise en main de John the Ripper (modes de génération de candidats, développement de règles de dérivation et de filtres de candidats basés sur une politique de mots de passe, formats dynamiques, implémentation ou modification d'un format natif), prise en main de Hashcat (génération de candidats avancée avec combinaison prince, mutations génétiques siga et génération de règles).

Développement offensif Windows

5 jours | Niveau intermédiaire

Description

De nos jours, les AV et EDR scannent agressivement les processus créés pour y détecter les intrusions, et Windows tente de se protéger via un nombre important de contre-mesures récemment introduites (AppContainer, ProtectedProcess, AMSI). C'est pourquoi il devient de plus en plus nécessaire pour un pentesteur de pouvoir se construire un outillage d'intrusion personnalisé sous Windows afin de passer sous le radar des solutions de sécurité lors de ses missions de Red Team.

Au cours de cette formation les élèves apprendront à utiliser les APIs bas niveau de Windows afin d'effectuer de manière furtive des opérations considérées comme hostiles sur le système ciblé. Ils apprendront aussi à manipuler les outils traditionnels de diagnostic système tel qu'un débuggeur applicatif dans le but de résoudre les problèmes inhérents au développement d'outils d'intrusions. Enfin ils seront exposés au modèle de sécurité de Windows et à la façon dont le système d'exploitation est architecturé du côté espace utilisateur.

- 5 jours (35 heures)
- 8h théorie / 27h pratique

Public et prérequis

L'introduction au développement d'outils d'intrusions personnalisés pour Windows est une formation de niveau intermédiaire conçue pour les pentesteurs, les développeurs sous Windows et les équipes de sécurité.

- Pentesteurs
- Développeurs Windows
- Équipes sécurité

De bonnes connaissances en développement C et une bonne compréhension du modèle de mémoire associé sont recommandés.

Contenu

Jour 1

Présentation de l'environnement de travail. Introduction au format PE et aux moyens de diagnostics sous Windows, utilisation basique d'un debugger (x64dbg et WinDBG).

Jour 2 & 3

Toolchain Visual Studio, développement natif Windows (win32), injection de code, persistance et hooking.

Jour 4

Exercices pratiques à partir d'un prototype de RAT, implémentation des techniques d'injection et de persistance.

Jour 5

Présentation du modèle de sécurité de Windows (niveau d'intégrité, token, security descriptor, SID) et compréhension des limites associées.

Développement offensif Linux

5 jours | Niveau intermédiaire

Description

L'objectif de cette formation est d'appréhender les fondements du système d'exploitation Linux afin d'implémenter, via les API C bas-niveau, des mécanismes de sécurité offensifs.

Après une première journée de rappel sur les bases du système d'exploitation Linux, les participants apprendront à manipuler les APIs bas niveaux liées aux processus (création, communication, injection, débogage). Ils découvriront également le format ELF ainsi que sa représentation en mémoire. Enfin les mécanismes de sécurité (LSM), d'isolation (cgroup, namespaces), et d'audit du système seront également abordés.

Durant cette formation les participants seront amenés à implémenter un scénario dans lequel un attaquant injectera une librairie dans le service sshd afin d'intercepter puis exfiltrer les mots de passe des utilisateurs, tout en assurant la persistance sur le système en installant une porte-dérobée dans une librairie partagée.

- 5 jours (35 heures)
- 13h théorie / 22h pratique

Public et prérequis

L'introduction au développement système orienté sécurité sous Linux est une formation de niveau avancé conçue pour les pentesteurs, les développeurs sous Linux et les équipes de sécurité.

- Pentesteurs
- Développeurs Linux
- Équipes sécurité

De bonnes connaissances en développement C ainsi qu'une bonne culture générale en sécurité sont recommandées.

Contenu

Jour 1

Bases du système d'exploitation Linux : accueil et démarrage des environnements de travail, distributions Linux, shells, système de fichiers, modèle de sécurité, chaîne de compilation, Systemd, D-Bus et PAM.

Jour 2

Format ELF, représentation en mémoire et techniques de hooking.

Jour 3

Processus, threads et injection : création, terminaison, monitoring, API, débogage et injection de processus.

Jour 4

Mécanismes d'IPC, mécanismes de sécurité et d'isolation : communication inter-processus, Linux Security Module (AppArmor et SELinux), cgroup et namespace.

Jour 5

Audit de l'activité système et interface noyau / utilisateur.

Android for Security Engineers

5 jours | Niveau intermédiaire

Description

Android est l'un des systèmes d'exploitation pour mobile les plus répandus sur le marché. Bien qu'il soit basé sur Linux, il se démarque par des composants spécifiques qui l'éloignent de l'OS traditionnel. Au cours de cette formation, les participants découvriront l'architecture d'Android et les interactions entre ses différents composants internes. Le système permet d'exécuter des applications tierces tout en protégeant les données de l'utilisateur final.

Les composants clés du système seront décortiqués, y compris le processus de démarrage et les mécanismes de sécurité. Les formateurs détailleront les évolutions des versions à partir d'Android 10 et évoqueront certaines particularités des constructeurs. Au cours des chapitres, les notions présentées seront mises en pratique au travers d'exercices concrets.

À la fin de cette formation, les participants auront une compréhension approfondie d'Android et seront en mesure d'être autonomes dans tout travail de recherche sur cet écosystème.

- 5 jours (35 heures)
- 15h théorie / 20h pratique

Public et prérequis

Android for Security Engineers est une formation de niveau avancé conçue pour les ingénieurs sécurité souhaitant mener des travaux de recherche sur ce système.

- Pentesteurs
- Développeurs Android
- Ingénieurs sécurité

De bonnes connaissances en développement C ainsi que des connaissances de base sur les systèmes Linux sont recommandées.

Contenu

Jour 1

Architecture globale d'Android, chaîne de démarrage, système de mise-à-jour, modèle de sécurité et root d'un téléphone.

Jour 2

Format des applications (APK) et présentation des outils de compilation et de debug (exercices avec Frida).

Jour 3

Android Runtime, mécanisme d'IPC (Binder) et présentation de la bibliothèque Bionic (libc Android).

Jour 4

Cycle de vie d'une Application : installation, démarrage, exécution et arrêt. Exploration des traces/logs pouvant être présents sur un appareil. Chiffrement des données utilisateurs.

Jour 5

Exercice final : modification d'un environnement Android via les modules Magisk et mise en pratique des notions vues pendant la semaine. Analyse des spécificités du noyau Linux pour Android.

iOS for Security Engineers

5 jours | Niveau intermédiaire

Description

iOS est un des systèmes d'exploitation les plus répandus sur le marché, offrant un modèle de sécurité à l'état de l'art.

Au cours de cette formation, les participants aborderont l'écosystème et les briques fondamentales du système d'exploitation iOS. Ils découvriront l'utilisation de la chaîne de compilation macOS afin de déployer un programme, puis les outils de débogage et de diagnostic.

Les fondamentaux du reverse-engineering d'applications et des services systèmes seront abordés dans un second temps : le fonctionnement d'Objective-C, les mécanismes d'IPC (mach, XPC, NSXPC) et les API du noyau. Des exemples pratiques et des exercices guideront les participants tout au long du training. Enfin, les mesures de sécurités logicielles et matérielles propres à iOS seront couvertes, tant dans l'espace noyau qu'utilisateur.

- 5 jours (35 heures)
- 18h théorie / 17h pratique

Public et prérequis

iOS for Security Engineers est une formation de niveau intermédiaire, conçue pour les ingénieurs sécurité souhaitant mener des travaux de recherche sur ce système.

- Pentesteurs
- Développeurs iOS
- Ingénieurs sécurité

De bonnes connaissances en développement C et des bases en rétro-ingénierie sont recommandées. Une licence IDA Pro avec le décompilateur Hex-Rays pour ARM64 est un plus.

Contenu

Jour 1

Introduction : présentation de l'environnement de travail, développement sur les plateformes Apple (iOS et macOS), utilisation des outils de diagnostic, introduction à l'écosystème Apple.

Jour 2

Introduction au reverse-engineering sur les plateformes Apple : extraction de mise à jour, formats de fichiers importants et outils, découverte et expérimentation du fonctionnement interne d'Objective-C, introduction au kernel XNU.

Jour 3

Mécanismes Mach : explications et exercices autour de l'API IPC de XNU, présentation et exercices sur l'implémentation de l'API Mach pour l'interaction avec les objets noyau, utilisation de Frida pour instrumenter des services.

Jour 4

Reverse-engineering de services Mach : théorie et exercices pratiques autour de XPC et NSXPC, les abstractions utilisées pour les communications inter-processus. Panorama de l'utilisation des pointeurs signés sur les plateformes Apple.

Jour 5

Sécurité de XNU : présentation du framework MACF, explications du fonctionnement d'AMFI et des politiques d'isolation (sandbox), description des mécanismes de défense en profondeur de XNU, contre-mesures matérielles de sécurité dans le noyau, mitigations des vulnérabilités noyau. Cas d'étude sur l'envoi de données de diagnostiques.

IDA Avancé

5 jours | Niveau intermédiaire

Description

Hex-Rays est un des acteurs majeurs dans le développement d'outils pour la rétro-ingénierie. Leur produit IDA s'est imposé au fil des années comme la référence en la matière. Cependant, le manque de documentation et de ressources rendent parfois difficile son maniement.

L'objectif de cette formation est de se familiariser avec IDA (son interface, ses fonctionnalités, son API et son écosystème) au travers de plusieurs modules théoriques et pratiques. Les participants apprendront également comment développer des scripts et plugins pour étendre les fonctionnalités d'IDA et son décompilateur.

- 5 jours (35 heures)
- 8h théorie / 27h pratique

Public et prérequis

Cette formation de niveau avancé est conçue pour les chercheurs en sécurité et experts en rétro-ingénierie souhaitant changer d'environnement ou se perfectionner dans l'utilisation d'IDA.

- Chercheurs en sécurité
- Experts en rétro-ingénierie

De bonnes connaissances en assembleur (x86-x64, ARM) ainsi qu'en programmation Python sont fortement recommandées. Une licence IDA Pro (non fournie) est indispensable.

Contenu

Jour 1

Introduction à IDA :terminologie, architecture et présentation de l'outil
Découverte du SDK et de l'API Python : notions élémentaires

Jour 2

Prise en main des fonctionnalités disponibles via différents exercices. Analyse statique : désassembleur, FLIRT / Lumina, IDS, Type Info Library. Analyse dynamique : débuggeur, traceur et instrumentation binaire

Jour 3

Programmation avancée (partie1) : présentation détaillée du SDK et mise en pratique par du scripting pour automatiser les tâches complexes.

Jour 4

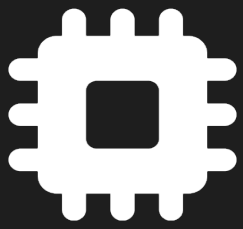
Programmation avancée (partie2) : développement de plugins, loader et extension de processeur pour mettre en pratique les TP précédents.

Jour 5

Extension du décompilateur : présentation de l'API Hex-Rays, manipulation du microcode et de l'AST, Extension et amélioration des outils créés lors de la session.

Intrusion Hardware

5 jours | Niveau intermédiaire



Description

L'objectif de cette formation est de monter en compétences sur l'analyse de sécurité hardware. Elle s'adresse autant aux novices qu'à ceux ayant un niveau intermédiaire.

À l'issue de cette formation les étudiants doivent connaître les principes de base en électronique et soudure. Ils sauront reconnaître les différents composants d'un PCB et rechercher des informations pertinentes dans des datasheets de composants type System on Chip (SoC) ou Flash externe pour en tirer partie (mise en RST, fonctionnalité de debug).

Enfin, ils sauront identifier les éventuels points de tests, inférer puis interagir avec les protocoles les plus courants (UART, JTAG/SWD, SDIO, SPI).

Lors de la formation, les étudiants apprendront également à utiliser des matériels et outils utiles à l'analyse (analyseurs logiques & Logic2, sondes à base de FT2232H & OpenOCD/flashrom)

- 5 jours (35 heures)
- 17h théorie / 18h pratique

Public et prérequis

L'initiation à l'intrusion matérielle est une formation de niveau débutant à intermédiaire conçue pour les pentesteurs, les chercheurs en sécurité et les équipes de sécurité.

- Pentesteurs
- Chercheurs en sécurité
- Équipes sécurité

Des connaissances de base en électricité et électronique (savoir se servir d'un multimètre, connaître la loi d'Ohm) sont recommandées.

Contenu

Jour 1

Notions fondamentales sur les composants : PCB, SoC, Flash, résistances, condensateur, transistor, oscillateur à quartz et PMIC.

Jour 2

Rappels théoriques : électricité, sécurité, électronique analogique et numérique.

Jour 3 à 5

Protocoles courants : théorie (caractéristiques, variation, utilité dans l'analyse de sécurité, forme du signal) et pratique (identifier les ports intéressants, connaître et savoir utiliser le matériel et les outils permettant de s'y connecter). Soudure : principe, matériel et bonnes pratiques.

Forensic Windows

5 jours | Niveau junior

Description

L'investigation numérique permet de reconstruire et comprendre de manière détaillée la chronologie des activités présentes et passées d'un système. Dans le cas de cette formation, nous nous intéressons au système d'exploitation Windows 10 ou 11. Qu'il s'agisse d'un incident de sécurité ou d'une recherche de malveillance informatique, les premières réponses visent à établir le périmètre de compromission et le mode opératoire de l'attaquant. La démarche technique présentée se veut la plus exhaustive possible et reproductible.

Au cours de ces cinq jours de formation, il sera exposé aux différents participants les fondamentaux à connaître afin de mener une investigation numérique pour Windows et ainsi identifier les traces d'une malveillance. Chaque module sera illustré par des travaux pratiques guidés permettant d'appliquer les notions théoriques enseignées préalablement. Enfin, la formation se conclura par une mise en situation sur plusieurs traces (disque, mémoire, pcap).

Cette formation est focalisée sur le poste de travail et n'intègre pas la dimension entreprise comme Azure/ADFS (une autre formation abordera prochainement cet aspect).

- 5 jours (35 heures)
- 11 modules de cours couvrant les fondamentaux de l'investigation Windows
- Approche à froid ou à chaud pour couvrir plusieurs cadres d'intervention
- Travaux dirigés sur des artefacts afin d'illustrer au mieux la théorie

Public et prérequis

Cette formation a été conçue pour des personnes ayant une première expérience sur la compréhension des environnements Windows (administration, troubleshooting, utilisation avancée) et désirant aller plus loin dans le domaine de l'investigation numérique. Elle nécessite une maîtrise basique de l'environnement Linux : ce système étant utilisé pour mener certaines investigations.

- Utilisateurs avancés (développeurs)
- Administrateurs système
- Analystes SOC niveau 2 ou d'une équipe de cybersécurité
- Analystes forensique débutants

Des notions de sécurité offensive et de bonnes connaissances Windows & Unix sont un plus pour la compréhension de cette formation.

Contenu

Jour 1

Prises en main : prise en main de l'environnement de formation (machine virtuelle, système Linux). Rappel de l'utilisation de la ligne de commande Linux. Windows : Description du fonctionnement de Windows (historique de Windows, processus, services, drivers, fichiers, modèle de sécurité, pile réseau, principale attaque). Évènements Windows : description du modèle de journalisation Windows et des évènements à connaître par cas d'usage. Mise en situation sur des fichiers d'évènements.

Jour 2

NTFS : étude du système de fichiers privilégié de l'environnement Windows. MFT, Journal des USN et autres fichiers spéciaux. Décodage des dates et fichiers supprimés. Reconstituer la chronologie des événements et pivoter sur un élément (date, IOC).
Base de registre : contenu des bases de registre. Cas d'usage et configuration du système Windows. Mécanismes de persistance : les moyens de persistance privilégiés par un attaquant sont passés en revue et ainsi identifient les programmes malveillants exécutés par un attaquant.

Jour 3

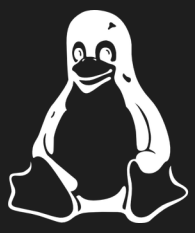
Exécution de commandes : traces liées à l'exécution de commande à distance sur le poste au travers des différents protocoles Windows (WinRM, Psexec, WMI, RPC). Codes et fichiers malveillants : outils et méthodes d'analyse permettant de mener une première étude sur un code malveillant et ainsi extraire les informations d'intérêt (comportement, IOC). Par extension les fichiers pouvant embarquer une charge malveillante sont également étudiés. Protocole réseau : une attention particulière est proposée afin d'identifier les communications réseau inhabituelles d'un système Windows ainsi que la caractérisation de certaines attaques (tunnel DNS, TOR).

Jours 4 et 5

Artefacts : l'étude ces artefacts forensic les plus importants (prefetch, srum, amcache, navigation) afin de compléter la chronologie de la malveillance. Les méthodes de collecte et d'acquisition sont également présentées afin de mettre à disposition les fichiers à étudier par l'analyste (DFIR ORC). Analyse mémoire : les techniques d'acquisition et d'identification d'éléments suspects sont abordées afin de compléter l'analyse des éléments hors ligne. Processus en cours d'exécution, connexion réseau, fichiers en cache, injection mémoire et API hooking. Étude de cas : plusieurs images sont proposées aux participants afin de mettre en pratique l'ensemble des techniques étudiées durant les 5 jours. Ces images regroupent des données variées comme une image disque, une capture mémoire et des captures réseau.

Forensic Linux

5 jours | Niveau junior



Description

L'investigation numérique permet de reconstruire et comprendre de manière détaillée la chronologie des activités présentes et passées d'un système. Dans le cas présent, nous nous intéressons au noyau Linux et deux types de distribution Linux. Les exemples et illustrations sont retenus pour des distributions sur des bases apt et rpm, néanmoins la plupart des éléments présentés dans la formation peuvent être généralisés.

Lors d'un incident de sécurité ou d'une recherche de malveillance informatique, les premières questions posées concernent à établir le périmètre de compromission et le mode opératoire de l'attaquant. La démarche technique d'une telle investigation se veut la plus exhaustive possible et surtout reproductible.

Au cours de ces cinq jours de formation, il sera exposé aux différents participants les fondamentaux à connaître afin de mener une investigation numérique pour une distribution Linux et ainsi identifier les traces d'une malveillance. Chaque module sera illustré par des travaux pratiques guidés permettant d'appliquer les notions théoriques enseignées préalablement. La formation inclut une mise en situation sur plusieurs artefacts (disque, mémoire, pcap).

- 5 jours (35 heures)
- 12 modules de cours couvrant les fondamentaux de l'investigation Linux
- Approche à froid ou à chaud pour couvrir plusieurs situations
- Travaux dirigés sur des artefacts afin d'illustrer au mieux la théorie

Public et prérequis

Cette formation a été conçue pour des personnes ayant une première expérience sur la compréhension des environnements Linux (administration, troubleshooting, utilisation avancée) et désirant aller plus loin dans le domaine de l'investigation numérique.

- Utilisateurs expérimentés
- Administrateurs système
- Analystes SOC niveau 2 ou équipe de cybersécurité
- Analystes forensique débutants

Des notions de sécurité offensive et de bonnes connaissances Unix sont un plus pour la compréhension de cette formation.

Jour 1

Prises en main et la ligne de commande : prise en main de l'environnement de formation (machine virtuelle, système Linux). Rappel des principales commandes en ligne de commande pour Linux. Linux et distribution : description du fonctionnement de Linux dont les processus, file descriptor, modèle de sécurité (user/group, ACL, cgroup), les canaux nommés, signaux, terminal et interpréteur de commande, X11. Système de fichiers : principaux types de système de fichiers rencontrés dans les systèmes Linux (ext4, LVM, XFS). Caractéristiques et particularités pour le forensic : gestion des dates, fichiers effacés, métadonnées, etc. Cas de LUKS et des disques virtuels (qcow, vmdk).

Jour 2

Séquence de démarrage : identifier la séquence de démarrage afin de vérifier l'intégrité de la chaîne de lancement (grub, initramfs, cas UEFI). Recherche de backdoor sur Systemd. Cas du SecureBoot et de la signature des modules noyaux. Gestion des programmes : contrôle des programmes installés sur le système (intégrité, permissions). Format ELF : programme et bibliothèque. Utilisation des gestionnaires de paquets apt et rpm. Journalisation : type de journaux (/var/log) et processus associés (syslog, auditd). Traces de compromission.

Jour 3

Mécanisme de persistance : moyens de persistance système et utilisateur, gestionnaire des périphériques, Systemd. Analyse des processus : outils de diagnostique des processus, principaux processus Linux (ssh, X11), exécution à distance, /proc Analyse réseau : configuration réseau, outils de diagnostic réseau, socket réseau, protocole généralement rencontré et tunnel, capture réseau.

Jour 4

Codes malveillants : outils et méthodes d'analyse permettant mener une première étude sur un code malveillant et ainsi extraire les informations d'intérêt (comportement, IOC, etc.). Artefact : autres artefacts (coredump, viminfo) Analyse mémoire : les techniques d'acquisition et d'identification d'éléments suspects sont abordées afin de compléter l'analyse des éléments hors ligne. Processus en cours d'exécution, connexion réseau, fichiers en cache, injection mémoire et API hooking.

Jour 5

Conteneur : recherche de traces dans conteneurisation et reconstitution du système. Collecte de données : extraction de fichiers (copie de disque) et sélective (velociraptor) Étude de cas : plusieurs images sont proposées aux participants afin de mettre en pratique l'ensemble des techniques étudiées durant les 5 jours. Ces images regroupent des données variées comme une image disque, une capture mémoire et des captures réseau.

Forensic Mobile

5 jours | Niveau junior

Description

Le téléphone mobile se transforme depuis plusieurs années comme le prolongement du poste de travail et devient une cible privilégiée, car au plus près de la donnée. L'investigation numérique de ce type de dispositif vise à identifier des traces en lien avec des activités criminelles, à détecter des traces d'activités malveillantes et de compromission du téléphone mobile.

Cette formation vise à présenter les principaux artefacts présents sur les environnements Android et iOS, majoritaires sur le marché, et de disposer d'une trousse à outils open source afin de les analyser. Des méthodologies d'analyse adaptées seront présentées afin de pallier l'approche « boîte noire » de certains systèmes et de leurs applications pré-installées qui complexifient l'audit du téléphone.

Cette formation aborde exclusivement le cas où les secrets de déverrouillage du téléphone sont connus.

- 4 jours (28 heures)
- 2 systèmes d'exploitation mobile : Android (≥ 10) & iOS (≥ 14)

Public et prérequis

Cette formation est adaptée pour des personnes ayant des notions en sécurité ou en administration de système Linux. Elle s'adresse principalement aux équipes informatiques souhaitant disposer de méthodes de premier niveau dans l'investigation de téléphones et ne disposant pas d'un logiciel dédié à cette activité. Plus généralement, toute personne souhaitant enrichir son parcours professionnel avec une composante sécurité dans le domaine mobile.

- Équipes informatique
- Administrateurs système
- Équipes sécurité

Des notions de sécurité offensive et de bonnes connaissances Unix sont un plus pour la compréhension de cette formation.

Un iPhone et un téléphone Android sont fournis durant la formation pour les manipulations.

Jour 1

Introduction : description de l'écosystème de l'investigation mobile, de ses principaux services et acteurs. Présentation des principales menaces, vecteurs d'infections et des dernières campagnes connues. Fondamentaux : description des principales sources d'informations en lien avec un appareil mobile (carte SIM, Warrant Return), des spécificités et problématiques des méthodes d'acquisition par rapport au forensic classique. Formats de données utilisés pour stocker de l'information et méthodologie d'analyse commune aux environnements iOS et Android. Fondamentaux iOS P1 : représentation de l'architecture et des principaux services.

Jour 2

Fondamentaux iOS P2 : description du système de fichiers et des emplacements d'intérêts, du modèle de sécurité et de ses impacts. Méthodes d'acquisition et formats de données spécifiques. Artefacts systèmes iOS : revue de l'activité de l'ensemble du téléphone en recherchant diverses traces d'exécution ou présence d'applications.

Jour 3

Artefacts applicatifs iOS : présentation des applications natives et des applications tierces (analyse de l'activité, données spécifiques). Analyse de sauvegardes chiffrées : méthodes d'acquisition et d'analyse en l'absence de copie complète du téléphone. Autres artefacts : sources d'informations systèmes alternatives. Nouveaux artefacts introduit dans les dernières versions d'iOS. Analyse live : acquisition de données systèmes live et d'activités réseau.

Jour 4

Fondamentaux Android : présentation de l'architecture, des principaux services et des mécanismes de communication. Système de fichiers, emplacements d'intérêts et modèle de sécurité. Méthodes d'acquisition spécifiques aux constructeurs. Artefacts systèmes Android : revue de l'activité de l'ensemble du téléphone en recherchant diverses traces d'exécution ou présence d'applications.

Jour 5

Artefacts applicatifs : présentation des applications natives (Android et constructeur) et des applications tierces (analyse de l'activité, données spécifiques). Analyse live : analyse avec ADB en l'absence de copie complète du téléphone. Analyse d'APK malveillant : méthodologie et outils d'analyse statique et dynamique.

Analyse de Malwares Windows

5 jours | Niveau intermédiaire

Description

Dans le cadre du traitement d'incidents de sécurité, il est fréquent de découvrir des codes malveillants. Cette formation a pour objectif de donner les clés de compréhension d'un code malveillant Windows et extraire les éléments d'intérêt.

Durant la formation, plusieurs types de codes malveillants sont illustrés selon le langage utilisé ou encore la phase de l'attaque (exploitation, persistance). Les différentes méthodes d'analyse statique et dynamique sont expliquées afin de fournir des approches complémentaires à l'analyse du code malveillant. Une partie assez importante de la formation concerne la mise en pratique dans le cadre d'incident de sécurité ou des modes opératoires régulièrement observés en incident. Cette formation adresse uniquement le cas des codes malveillants userland.

- 5 jours (35 heures)
- Codes malveillants analysés sur différents langages
- Étude de fichiers malveillants (Office, LNK)
- Environnement de travail prêt à l'emploi

Public et prérequis

Cette formation est adaptée pour des personnes ayant déjà fait de la programmation sous Windows ou ayant déjà engagé des analyses de programme (débogage ou codes malveillants). Elle s'adresse à toutes les personnes amenées à manipuler des codes malveillants en particulier les équipes de sécurité (SOC, CSIRT, équipe sécurité) ou souhaitant monter en compétences sur ce sujet.

De bonnes connaissances Windows sont recommandées pour mieux comprendre le fonctionnement des codes.

Contenu

Jour 1

Qualification d'un code premier niveau : OSINT, bac à sable automatique. Environnement de travail : installation d'un environnement d'analyse (isolé / ouvert) pour procéder aux traitements de codes malveillants. Structure PE : comprendre le format et les aspects utilisés par les codes. Analyse statique et dynamique d'un code : concepts et exemples simples.

Jour 2

Assembleur x86(-64) : premiers pas, contrôle du flot d'exécution et des instructions importantes. Windows : API Windows, bibliothèque à connaître et utiliser par les codes malveillants. Désassembleur 101: prise en main, cas des décompilateurs. Debugger 101: prise en main, étude pas-à-pas & point d'arrêt.

Jour 3

Intrusion initiale : type de code utilisé et exploitation. Scripts malveillants : analyse de sites web, désobfuscation Javascript. Analyse de fichiers malveillants : PDF, Office (OLE, macros VBA/XLM, pcode), désobfuscation Vbscript, RTF. Analyse de code Powershell : code powershell et émulation des shellcodes. Analyse de techniques de dissimulation : LNK, ISO, HTA.

Jour 4

Retroconception de code complexe : aller plus loin sur les types de codes rencontrés, unpacking Méthode anti-rétroconception : debug, bac-à-sable, rétroconception statique. Automatisation des analyses : scripting pour automatiser la rétroconception de code obfusqué

Jour 5

Rétroconception de code .NET : introduction à .NET et CIL, analyse de malware .NET. Rétroconception de code Go : introduction à Go, analyse de malware golang. Cas d'analyse de code modulaire

SYNACKTIV