Catalogue de formations 2017

devUp

Software security startup

Formation pour les Dev

La sécurité web
Le top 10 OWASP 2017
(attaque et défense)

Durée : 3 jours consécutifs (7h/jour)

1er Jour :

- Le top 10 des risques du WEB selon l'OWASP
- Architecture d'une application WEB classique
- Le protocole HTTP
- Injection SQL, XPath, XXE, LDAP, PHP
- Violation de gestion d'authentification et de session (session hijacking, faiblesse des mdp et session)
- XSS stocké (stored), XSS Réfléchi (reflected), XSS DOM (Document Object Model)
- Références directes non sécurisées à un objet
- Les entrées cachées non contrôlés

2ème Jour :

- Mauvaise configuration de sécurité
- Exposition de données sensibles
- Manque de contrôle d'accès au niveau fonctionnel
- Local/remote file inclusion (LFI/RFI)
- Host Header Attack, User-agent spoofing, SSRF, XSPA
- Cross Site Request Forgery (CSRF)
- Exploitation de vulnérabilités connues
- WPScan , Nikto, OpenVAS, Qualys SSL Labs
- Redirections et renvois non validés

3ème Jour :

- Pentest en boîte blanche, noire, grise
- A l'aide du "testing guide" OWASP vérification des différents points de contrôle.
- Utilisation des outils d'automatisation tels que Beef, Burp, Sqlmap
- Création d'un rapport d'audit avec modèle

La sécurité mobile
Le top 10 OWASP 2016
(attaque et défense)

Durée : 3 jours consécutifs (7h/jour)

1er Jour :

- Le top 10 des risques du Mobile selon l'OWASP
- Architecture d'une application Mobile
- Installation de la plateforme (NOX + Burp + DIVA)
- Utilisation inappropriée des préconisations Android
- Découverte d'ADB
- Stockage de données sensibles (SQLite, logs, manifest.xml, etc)
- Injection SQL
- Défaut de configuration des serveurs WEB

2ème Jour :

- Étude des différents scénarios liés à une communication non sécurisée
- Démonstration d'une attaque MITM avec Ettercap et protection
- Authentification non-sécurisée avec le stockage des clés privées (API)
- Recherche de credentials dans une l'APK à l'aide d'APKTOOL
- Études des bonnes et mauvaises méthodes cryptographiques (MD5, SHA1, SSLV2)
- Authentification mal-sécurisée et protection
- Insecure Direct Object Reference (IDOR)

3ème Jour :

- Mauvaise qualité de code
- XSS DOM, Buffer flow et protection
- Falsification de code avec modification d'APK et scénarios possibles
- Désassemblage d'une APK et recherche de "strings" avec données sensibles
- Fonction étrangère et mode debug actionnée
- MDM
- Chiffrement équipements
- OTP pour connexion

Python
dans un environnement de Pentest

Durée : 3 jours consécutifs (7h/jour)

1er Jour :

- Mise en place de d'une plateforme de travail Python avec Kali
- Retour rapide sur les fondamentaux du langage Python
- Utilisation des sockets avec Python
- Utilisation du multi-threading avec le module subprocess
- Mise en place d'un reverse-shell
- Création d'un trojan

2ème Jour :

- Création d'un exécutable Windows (.py to .exe)
- Mise en place d'une persistance avec winreg
- Introduction au framework Scapy
- Création d'un reverse proxy, sniffer avec Scapy
- Mise en place d'un arpping, arp poisoning, arp flood avec scapy

3ème Jour :

- Utilisation du module Beautiful Soup, Request, Urllib pour le WEB
- Recherche dans un DOM HTML d'information
- Attaque par dictionnaire avec Python
- Transfert d'informations à travers des API et encodage base64
- Chiffrement avec PyCrypto
- Étude pour la création d'extension Python pour Burp

devUp

Software security startup

Formation pour les Ops

Initiation au Pentest
et des outils appropriés

Durée : 3 jours consécutifs (7h/jour)

1er Jour :

- Retour sur quelques fondamentaux TCP/IP
- Installation de Kali, Metasploitable et différents GIT nécessaires
- Études et mise en pratique des différentes attaques TCP/IP
- Aperçu sur les différentes phases de pénétrations et terminologies
- ARP poisoning, DNS poisoning avec Ettercap, Driftnet, SSLSTRIP
- Information gathering avec Maltego, SEO et social engineering
- Énumération avec NMAP et OpenVas (scan, firewallking, recherche de CVE)

2ème Jour :

- Pénétration avec Metasploit et Empire (listener, stage, exploit)
- Pivoting avec Metasploit
- Création d'un payload personnalisé avec Veil framework
- Utilisation des outils Nishang pour Active Directory, privilege escalation, Web Shell
- Études des attaques WEB et utilisation de WPscan, Nikto, SQLMAP, BURP SUITE

3ème Jour :

- Mise en pratique d'une campagne de Spear Phishing
- Attaques WIFI avec Aircrack-ng
- Attaques physiques avec USB rubber ducky et création d'un payload
- Cassage des mots de passe avec les attaques Rainbow table, brute-force et dictionnaire (John the ripper, Cupp.py, Crunch, etc)
- Bypass d'IDS, reconnaissance d'Honeypot

Sécuriser une infrastructure (IDS, Firewall, PKI)

Durée : 3 jours consécutifs (7h/jour)

1er Jour :

- Quelles sont les principales menaces dans une infrastructure
- Comprendre la confidentialité, intégrité, disponibilité, non répudiation
- Utiliser les politiques de sécurité (password, availability, update)
- La sécurité par défaut
- La réduction des attaques de surface
- Least privilege

2ème Jour :

- Sécurité du réseau (port security, dhcp snooping, 802.1x)
- IDS avec snort (install, rules, list)
- Firewall avec Pfsense (routing, filter, bonnes pratiques)
- SIEM avec syslog

3ème Jour :

- Les bases de la Cryptographie
- Architecture et bonnes pratiques
- WIFI et sécurité
- Réduire les surface d'attaque
- Email avec gpg, SPF, DKIM

Sécuriser une infrastructure Microsoft

Durée : 3 jours consécutifs (7h/jour)

1er Jour :

- Mise en place d'un contrôleur de domaine
- Durcissement sur le serveur à l'aide des préconisations Microsoft et des templating mise à la disposition pour cet effet
- Password policy, Windows update policy, right policy
- Group and GPO best practises
- GPO policy analysis (audit policy)

2ème Jour :

- WSUS
- Bitlocker and Bitlocker to go with Active directory
- Applocker
- EFS
- MBSA, MSAT, MSCM
- IPSEC, DNSSEC, Firewall
- Network access protection (NAP & NPS)

3ème Jour :

- ADCS (PKI) bonnes pratiques
- Protéger vos scripts Powershell
- Protect memory et LSASS

devUp

Software security startup

Formation pour les managers

SecDevOps pour les managers du SI

Durée : 3 jours consécutifs (7h/jour)

1er Jour :

- Récapitulatif des acteurs autour de la sécurité application tels que :
- OWASP - MITRE - PCI-DSS - SAFECODE - HIPAA
- Etat des lieux sur les différentes sécurités autour de la sécurité applicative et DevOps telles que les navigateurs, serveurs, prestataires, outils (WAF, SAST, DAST)
- Introduction au "Process model" et "Maturity model"
- Par quoi commencer, qui est concerné ?
- Les avantages et les défauts en terme de sécurité du DevOps et des méthodes Agile
- Utiliser un modèle CAMS (Culture, Automation, Measurement, and Sharing)

2ème Jour :

- Analyser les pré-requis pour commencer un cycle de développement sécurisé avec :
- Quelles sont les existants en matière de sécurité (PSSI, SMSI, etc)
- Quelles sont les lois concernés par la sécurité applicative
- Établir in PIA (privacy impact assessment) permettant de définir la criticité des informations stockées par les applications et établir les risques et potentiel contrôles à prévoir.
- Affectation des responsabilités aux parties prenantes du projet
- "Secure by design" et la mise en place d'un plan d'action pour le durcissement des infrastructures
- Préparation à la réduction des surfaces d'attaques
- Modélisation des menaces et analyse avec les exigences de l'entreprise
- Préparation au "Secure code" avec : Analyse statique du code (démonstration des différents produits du marché) et automatisation du processus
- Code review et analyse de fonction non utiles

3ème Jour :

- Vérification de la sécurisation de l'application avec :
- Analyse dynamique avec OWASP ZAP - Fuzzing - Pentest - WAF
- Vérification des exigences de l'organisation et du cycle de développement sécurisé en place
- Création d'un plan de réponse à incident
- Présentation de BSIMM, OPENSAMM
- Mise en place de OPENSAMM

Analyse de risque à l'aide de la norme 27005 et la méthode EBIOS

Durée : 5 jours consécutifs (7h/jour)

1er Jour :

- Introduction à la gestion des risques
- Termes et définition selon la norme 31000 (management du risque)
- Définitions de la menace, vulnérabilité, risques
- L'intégration au processus PDCA
- La mise en oeuvre d'un processus PDCA de management des risques
- La création en phase plan d'action
- Introduction, programme de gestion des risques, identification et évaluation des risques selon la norme ISO 27005

2ème Jour :

- Établir le contexte (schéma directeur, répertorier les actifs, définir les process owner)
- Evaluation des risques, du traitement, de l'acceptation, de la communication et de surveillance selon la norme ISO 27005
- L'assurabilité d'un risque, calcul financier du transfert à l'assurance.
- La préparation de la déclaration d'applicabilité (SoA)

3ème Jour :

- Cas pratique avec étude et analyse de risque à rendre

4ème Jour :

- Histoire de la méthode Française EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)
- EBIOS dans une démarche ISO PDCA de type SMSI 27001
- Début d'une évaluation des risques EBIOS
- Etude du contexte, des scénarios de menaces, des événements redoutés, des risques, des mesures de sécurité

5ème Jour :

- Évaluation des vulnérabilités et des risques, selon EBIOS
- Planification de la sécurité selon EBIOS
- Utilisation du logiciel EBIOS
- Cas pratique avec étude et analyse de risque à rendre avec la méthode EBIOS

Etat de l'art de la sécurité de l'information et de la gouvernance

Durée : 5 jours consécutifs (7h/jour)

1er Jour :

- Quels sont le rôle et les responsabilités du Responsable Sécurité SI ?
- La gouvernance et ses fondamentaux
- Introduction des référentiels d'ITIL et de COBIT
- Identifier les acteurs de la sécurité dans un système d'information
- Introduction à la gestion des risques et de ses normes
- SMSI, PSSI et création d'un tableau de bord
- Sensibilisation des utilisateurs de l'organisation et communication
- Gérer la qualité, les coûts, les accords de service

2ème Jour :

- Rôle du RSSI dans le PCA / PRA
- Gérer la disponibilité et la capacité
- Gestion de crise au sein d'un système d'information
- Gestion des incidents
- Création d'un plan de réponse à incident
- Bases juridiques pour le RSSI
- Présentation des normes et référentiels (CNIL, GDPR, PCI-DSS)
- La conformité des systèmes d'information et les exigences des autorités étatiques

3ème Jour :

- Gérer les programmes et les projets, définition des exigences
- Gérer le changement organisationnel
- Gérer les changements
- Les techniques d'évaluation des coûts, les différentes méthodes de calcul, le Total Cost of Ownership (TCO), calcul du ROI
- La définition du Return On Security Investment (ROSI)

4ème Jour :

- Aspects et enjeux de la sécurité opérationnelle.
- Protection et gestion de l'identité.
- Etat de l'art de la sécurité opérationnelle.
- La mobilité sécurisée : les enjeux (BYOD).
- Threat intelligence
- Mettre en oeuvre une protection contre les attaques cybercriminels
- Sécurisation des systèmes et réseaux.
- Sécurité liaison sans fil
- Le chiffrement et les différentes solutions du marché

5ème Jour :

- La sécurité du cloud et ses enjeux
- Le Cloud, nouvelle stratégie d'entreprise
- Risques liés à la perte de maîtrise du système d'information
- Risques liés aux interventions à distance
- Risques liés à l'hébergement mutualisé
- Prise en compte de la sécurité dans le Cloud
- Principes et démarches
- Mesurer les risques et déterminer les objectifs de sécurité
- Choix du prestataire
- Assurer le cyber risque

Règlement général sur la protection des données (RGPD) enjeux, risques et obligations légales

Durée : 3 jours consécutifs (7h/jour)

Public concerné :

- Manager en sécurité de l'information
- RSSI
- Chef de projet
- DPO
- CIL

Pré-requis:

- Avoir la base de la direction des systèmes d'information

Matériel nécéssaires :

- Ordinateur sous Windows (toutes versions) ou Linux (toutes versions) avec clavier + souris
- Droits d'administration sur les machines, le cas échéant un outil de virtualisation (VirtualBox/VMWare)
- Disque dur avec 40 Giga d'espace libre minimum
- Puissance processeur 2Gz en double coeurs minimum
- 40 Giga de RAM (mémoire vive) minimum
- Des ports USB 2 ou 3 accessibles et utilisables
- Clavier + souris + écran
- Un accès à internet performant

Objectifs :

- Comprendre les enjeux, gérer les risques et obligations légales du RGPD
- Savoir développer une méthodologie pour l'implémentation d'une RGPD

Les méthodes pédagogiques :

La méthode pédagogique se base surtout sur des exercices pratiques, des mises en situation réelles et du retour d'expérience.

Outil d'évaluation utilisé après la formation :

Un QCM électronique sera utilisé

1er Jour (matin) :

- Introduction à la GDPR (contexte)
- Définitions
- Le périmètre
- Privacy by design
- Portabilité des données
- Introduction à la gestion des risques
- Termes et définitions selon la norme 31000 (management du risque)
- Définitions de la menace, vulnérabilités, risques
- Accountability
- Traitement automatique des données
- Le DPO
- Les garants du règlement
- Spécificités

1er Jour (après-midi) :

- Mise en application du règlement
- Définir un leader : le DPO
- Evaluer la maturité
- L'étude d'impact (PIA ou EIVP)
- Le plan d'action
- Etablir des règles d'entreprise contraignantes
- Certifications et labels
- Perspectives : de la conformité GDPR vers l'ISO 27000
- Le registre des données
- Les droits des citoyen
- Comprendre ses droits
- Exercer ses droits
- Consentement et violation de données à caractère personnel
- Responsabilisation des acteurs et des citoyens (notamment des mineurs)
- GDPR, Big Data et Business Intelligence

devUp

Software security startup

Formation en préparation

FORENSIC
et la réponse à l'incident

Durée : 3 jours consécutifs (7h/jour)

En cours de rédaction