Stage pratique de 5 jour(s)
Réf : HAC

Participants

Responsables, architectes sécurité. Techniciens et administrateurs systèmes et réseaux.

Pré-requis

Bonnes connaissances en sécurité SI, réseaux, systèmes (en particulier Linux) et en programmation. Ou connaissances équivalentes à celles du stage "Sécurité systèmes et réseaux, niveau 1" (réf. FRW).

Prix 2020 : 3490€ HT

Dates des sessions

AIX
16 nov. 2020, 25 jan. 2021
12 avr. 2021, 17 mai 2021
23 aoû. 2021

ANGERS
22 fév. 2021, 21 juin 2021
16 aoû. 2021

BORDEAUX
16 nov. 2020, 25 jan. 2021
12 avr. 2021, 17 mai 2021
23 aoû. 2021

BRUXELLES
15 fév. 2021, 19 avr. 2021
14 juin 2021, 09 aoû. 2021

CLASSE A DISTANCE
02&23 nov. 2020, 14 déc. 2020
11 jan. 2021, 01 fév. 2021
08 mar. 2021, 26 avr. 2021
17 mai 2021, 21 juin 2021
26 juil. 2021, 09 aoû. 2021
20 sep. 2021

DIJON
15 fév. 2021, 26 avr. 2021
16 aoû. 2021

GENEVE
25 jan. 2021, 17 mai 2021
19 juil. 2021

GRENOBLE
01 fév. 2021, 12 avr. 2021
14 juin 2021, 02 aoû. 2021

LILLE
25 jan. 2021, 12 avr. 2021
17 mai 2021, 23 aoû. 2021

LIMOGES
15 fév. 2021, 26 avr. 2021
16 aoû. 2021

LUXEMBOURG
11 jan. 2021, 03 mai 2021
05 juil. 2021

LYON
23 nov. 2020, 18 jan. 2021
15 mar. 2021, 14 juin 2021
16 aoû. 2021, 13 sep. 2021

MONTPELLIER
01 fév. 2021, 12 avr. 2021
14 juin 2021, 02 aoû. 2021
27 sep. 2021

NANCY
22 fév. 2021, 21 juin 2021

Hacking et sécurité, niveau 1

Cette formation avancée vous apprendra les techniques indispensables pour mesurer le niveau de sécurité de votre Système d'Information. A la suite de ces attaques, vous apprendrez à déclencher la riposte appropriée et à élever le niveau de sécurité de votre réseau.

OBJECTIFS PEDAGOGIQUES

Comprendre les techniques des pirates informatiques et pouvoir contrer leurs attaques
Mesurer le niveau de sécurité de votre Système d'Information
Réaliser un test de pénétration
Définir l'impact et la portée d'une vulnérabilité

1) Le Hacking et la sécurité
2) Sniffing, interception, analyse, injection réseau
3) La reconnaissance, le scanning et l'énumération
4) Les attaques Web
5) Les attaques applicatives et post-exploitation

1) Le Hacking et la sécurité

- Formes d'attaques, modes opératoires, acteurs, enjeux.
- Audits et tests d'intrusion, place dans un SMSI.

2) Sniffing, interception, analyse, injection réseau

- Anatomie d'un paquet, tcpdump, Wireshark, tshark.
- Détournement et interception de communications (Man-in-the-Middle, attaques de VLAN, les pots de miel).
- Paquets : Sniffing, lecture/analyse à partir d'un pcap, extraction des donnés utiles, représentations graphiques.
- Scapy : architecture, capacités, utilisation.

Travaux pratiques
Ecouter le réseau avec des sniffers. Réaliser un mini intercepteur de paquets en C. Utiliser scapy (ligne de commande, script python) : injections, interception, lecture de pcap, scan, DoS, MitM.

3) La reconnaissance, le scanning et l'énumération

- L'intelligence gathering, le hot reading, l'exploitation du darknet, l'Ingénierie Sociale.
- Reconnaissance de service, de système, de topologie et d'architectures.
- Types de scans, détection du filtrage, firewalking, fuzzing.
- Le camouflage par usurpation et par rebond, l'identification de chemins avec traceroute, le source routing.
- L'évasion d'IDS et d'IPS : fragmentations, covert channels.
- Nmap : scan et d'exportation des résultats, les options.
- Les autres scanners : Nessus, OpenVAS.

Travaux pratiques
Utilisation de l'outil nmap, écriture d'un script NSE en LUA. Détection du filtrage.

4) Les attaques Web

- OWASP : organisation, chapitres, Top10, manuels, outils.
- Découverte de l'infrastructure et des technologies associées, forces et faiblesses.
- Côté client : clickjacking, CSRF, vol de cookies, XSS, composants (flash, java). Nouveaux vecteurs.
- Côté serveur : authentification, vol de sessions, injections (SQL, LDAP, fichiers, commandes).
- Inclusion de fichiers locaux et distants, attaques et vecteurs cryptographiques.
- Évasion et contournement des protections : exemple des techniques de contournement de WAF.
- Outils Burp Suite, ZAP, Sqlmap, BeEF.

Travaux pratiques
Mise en œuvre de différentes attaques Web en conditions réelles côté serveur et côté client.

5) Les attaques applicatives et post-exploitation

- Attaque des authentifications Microsoft, PassTheHash.
- Du C à l'assembleur au code machine. Les shellcodes.
- L'encodage de shellcodes, suppression des NULL bytes.
- Les Rootkits. Exploitations de processus: Buffer Overflow, ROP, Dangling Pointers.
- Protections et contournement: Flag GS, ASLR, PIE, RELRO, Safe SEH, DEP. Shellcodes avec adresses hardcodées/LSD.
- Metasploit : architecture, fonctionnalités, interfaces, workspaces, écriture d'exploit, génération de Shellcodes.

Travaux pratiques

23 aoû. 2021

NANTES

25 jan. 2021, 12 avr. 2021
17 mai 2021, 23 aoû. 2021

NIORT

22 fév. 2021, 21 juin 2021
16 aoû. 2021

ORLEANS

18 jan. 2021, 12 avr. 2021
28 juin 2021, 02 aoû. 2021

PARIS

02&23 nov. 2020, 11&18 jan. 2021
01 fév. 2021, 08 mar. 2021
26 avr. 2021, 17 mai 2021
14&21 juin 2021, 26 juil. 2021
09&16 aoû. 2021, 20 sep. 2021

REIMS

22 fév. 2021, 21 juin 2021
23 aoû. 2021

RENNES

01 fév. 2021, 12 avr. 2021
14 juin 2021, 02 aoû. 2021
27 sep. 2021

ROUEN

22 fév. 2021, 28 juin 2021
16 aoû. 2021

SOPHIA-ANTIPOLIS

25 jan. 2021, 12 avr. 2021
17 mai 2021, 23 aoû. 2021

STRASBOURG

16 nov. 2020, 25 jan. 2021
12 avr. 2021, 17 mai 2021
23 aoû. 2021

TOULON

22 fév. 2021, 28 juin 2021
16 aoû. 2021

TOULOUSE

23 nov. 2020, 25 jan. 2021
12 avr. 2021, 17 mai 2021
23 aoû. 2021

TOURS

18 jan. 2021, 12 avr. 2021
28 juin 2021, 02 aoû. 2021

Modalités d'évaluation

L'évaluation des acquis se fait tout au long de la session au travers des multiples exercices à réaliser (50 à 70% du temps).

Compétences du formateur

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent

Metasploit : exploitation, utilisation de la base de données. Msfvenom : génération de Shellcodes, piégeage de fichiers. Buffer overflow sous Windows ou Linux, exploitation avec shellcode Meterpreter.

ou ont occupé des postes à responsabilité en entreprise.

Moyens pédagogiques et techniques

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.

• A l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.

• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.