SETC Training Corporate Logo

Formation la sécurité informatique: Analyse criminalistique du réseau (NFOREFR, 4 jours)

Description

Le cours Formation la sécurité informatique : Analyse crimanilistique du réseau explore les complexités de la collecte de preuves numériques sur un réseau. La formation commence par une discussion générale sur les types de preuves et les techniques connexes de collecte de preuves. Elle est suivie d'une exploration détaillée des outils fondamentaux de la criminalistique numérique, notamment le serveur proxy Squid et les outils courants d'analyse de paquets, dont tcpdump, Wireshark et NetFlow. Le cours comprend une étude détaillée des protocoles et services au niveau des applications, des pare-feu, des systèmes de détection d'intrusion (IDS) et des responsables de la sécurité du réseau. La formation se termine par une exploration de la journalisation centralisée, de la pile Elastic, des considérations relatives aux réseaux sans fil, du cryptage et de l'inspection SSL.

Tarifs

- Tarification: $3,750/person
- Rabais de 10% lorsque vous inscrivez 3 personnes.

Plan de cours

Notions fondamentales de réseau (uniquement si nécessaire)

- Le modèle de référence OSI et la structure des paquets
- Concepts IP essentiels : Adresses IP et sous-réseaux
- Obtention d'une adresse IP : Adressage statique et dynamique
- Concepts IP essentiels : Protocoles de transport (TCP et UDP)
- Comportement IP : Comprendre les sockets, les ports et les protocoles d'application
- Comprendre les routeurs et les commutateurs de couche 3
- Travailler avec et comprendre les VLAN
- Explorer les technologies VOIP

Introduction à l'analyse légale des réseaux

- Qu'est-ce que l'analyse médico-légale ?
- Qu'est-ce qu'une preuve valable ?
- Aperçu de l'analyse criminalistique numérique
- En savoir plus sur l'acquisition de preuves en réseau
- Principaux types de preuves réseau : Paquet complet, journaux et NetFlow
- L'importance de l'intégrité des données : Pourquoi les ports SPAN ne suffisent pas
- Exploration des dispositifs de capture : NetFlow, commutateurs, TAP et dispositifs de couche 7

Les outils fondamentaux du métier : le calmar

- Comprendre les exigences de l'analyse médico-légale
- Concevoir notre réseau pour l'analyse médico-légale
- Le rôle du serveur proxy de mise en cache
- Configuration du serveur proxy Squid
- Configuration de la journalisation dans Squid
- Configuration du logiciel d'analyse des journaux Squid
- Configuration et utilisation de l'extraction du cache

Les outils fondamentaux du métier : Analyse des paquets

- Comprendre la structure des paquets du réseau
- Configuration de tcpdump
- Exploration des options de tcpdump
- Limiter les données capturées avec tcpdump

- Recherche des résultats de Trace avec grep
- Installation de la dernière version de Wireshark
- Configuration des filtres dans Wireshark
- Utilisation de Wireshark pour inspecter les paquets
- Conseils et astuces pour la capture de paquets

Protocoles clés au niveau des applications : HTTP

- Explorer les communications basées sur HTTP
- Révision de la spécification HTTP
- Comprendre le comportement HTTP dans un scénario de routage
- Comprendre la structure et les champs clés de l'en-tête HTTP
- Analyse des requêtes HTTP et des réponses HTTP
- Extraction d'artefacts
- Mise en œuvre de la journalisation
- Application de la méthodologie médico-légale à HTTP
- Exploration et analyse du trafic FTP

Protocoles clés au niveau des applications : DNS

- Comment fonctionnent les serveurs DNS
- Révision des opérations DNS courantes : Résolution de noms, transferts de zones et autres
- Comment fonctionne un tunnel
- Exploration du fast-flux et des DGA
- Mise en œuvre de la journalisation
- Utilisations courantes du DNS dans les stratégies d'attaque
- Exploration des attaques par amplification

Pare-feu, systèmes de détection d'intrusion et surveillance de la sécurité des réseaux

- Le rôle des pare-feu et des systèmes de détection des intrusions
- Le rôle de la surveillance de la sécurité des réseaux
- Mise en œuvre des règles de pare-feu : Windows, Linux et Cisco
- Exploration de NAT et Masquerade
- Mise en œuvre de la journalisation du pare-feu
- Mise en œuvre des systèmes de détection d'intrusion
- Mise en œuvre de la surveillance de la sécurité des réseaux
- Explorer les caractéristiques et la fonctionnalité de Bro NSM
- Mise en œuvre de Bro NSM

Mise en œuvre de la journalisation centralisée

- Exploration de la spécification syslog
- Explorer le format des événements
- Mise en œuvre d'un serveur central syslog
- Utilisation de rsyslog et d'autres outils
- Exploration de Microsoft Eventing
- Explorer l'agrégation des journaux : Avantages et vulnérabilités
- Mise en œuvre d'une solution d'agrégation de journaux

Travailler avec Elastic Stack

- Qu'est-ce que l'Elastic Stack ?
- Les rôles spécifiques d'Elastisearch, Logstash et Kibana
- À propos d'Elastic Stack et de l'agrégation de journaux
- Installation d'un serveur Elastisearch
- Installation et configuration de Logstash
- Utilisation de Kibana pour des visualisations puissantes

NetFlow et analyse du trafic

- Exploration de l'architecture, des composants et des protocoles de NetFlow

Configuration de NetFlow sur les routeurs Cisco
Examen du trafic à l'aide de NetFlow
Utilisation de NetFlow pour le trafic crypté
Utilisation de NetFlow pour le trafic Linux : NFS, SSH et Apache
Utilisation de NetFlow avec les protocoles Microsoft : Exchange, Outlook, SMB et IIS

Communications modernes : Réseaux sans fil

Comprendre la communication et l'authentification sans fil
Explorer l'authentification : WEP et WPA
Capture de paquets basée sur le matériel et le logiciel
Exploration des champs de protocole utiles
Utilisation du matériel : Dispositif WIFI PineApple
Logiciels utilisés : aircrack-ng et Airventroliquist
Travailler avec Moloch
Travailler avec NetworkMiner

La magie de SSL

Exploration des algorithmes de chiffrement : Symétrique et asymétrique
Plus d'informations sur le chiffrement asymétrique : AES et RSA
Exploration d'une session HTTPS typique
Profilage des sessions SSL
Exploration du Perfect Forward Secrecy et de ses exigences
Les mécanismes d'une attaque de l'homme du milieu (MITM)
Réalisation d'attaques par ingénierie inverse de protocoles de réseau

Tout mettre en place