CAS IT-Interceptor

Formation « Certificate of Advanced Studies »

> Description détaillée des contenus de la formation.

Structure, objectifs et contenu de la formation

La formation est structurée en 3 modules :

1. **Bases de l'interception IT**
   6 jours de formation, pour enquêteurs et spécialistes

2. **Approfondissement : Interception dans les réseaux téléphoniques**
   6 jours de formation, pour spécialistes

3. **Approfondissement : Interception dans les réseaux informatiques**
   8 jours de formation, pour spécialistes

Le module de base s'adresse aux enquêteurs qui doivent effectuer des interceptions usuelles avec ISS et comprendre les résultats. Ce module fournit les connaissances réseaux de base nécessaires lors du travail avec ISS. Il peut être suivi séparément des deux modules d'approfondissement.

Les deux modules d'approfondissement fournissent des connaissances plus approfondies sur les technologies des réseaux informatiques et téléphoniques. Ils s'adressent aux enquêteurs spécialistes qui doivent effectuer des interceptions complexes, notamment multi-services, et interpréter les éléments techniques des données interceptées. Les deux modules d'approfondissement peuvent être suivis après avoir accompli et réussi le module de base.

Module 1 : Bases de l'interception IT

Ce module de base donne une introduction aux réseaux informatiques et réseaux téléphoniques. Il fournit au participant les connaissances de bases nécessaires lors du travail avec ISS. Le public cible est les enquêteurs qui doivent effectuer des interceptions usuelles avec ISS et être capables d'interpréter les résultats.

Les objectifs généraux de ce module de base sont :

- comprendre le fonctionnement des principaux services de communication sur Internet tels quels courrier électronique, Web, chat, VoIP, P2P, transfert de fichiers
- comprendre l'architecture d'Internet, ses éléments fonctionnels ainsi que ses principes de fonctionnement
- comprendre l'architecture et les principes de fonctionnement des réseaux téléphoniques fixes
- comprendre l'architecture et les principes de fonctionnement des réseaux mobiles (GSM, UMTS)
- avoir des connaissances de bases de l'utilisation du système d'interception ISS.

Chapitre	Objectifs	Vol.
1. Bases des réseaux informatiques • Types de commutation (circuit, paquets) • Modèle OSI • Types de réseaux informatiques (LAN, WLAN, WAN, Internet) • Eléments d'un réseau informatique	• Comprendre les différences entre la commutation de circuits et de paquets • Connaître les notions de protocole, paquet, systèmes intermédiaire, terminaux • Connaître les différents types de réseaux d'ordinateurs • Connaître les notions switch, routeur, passerelle, serveur, terminal	4 h
2. Fonctionnement d'Internet • Structure d'Internet • Le protocole IP et l'acheminement des paquets • Adressage IP (structure d'adresses IP, adresses publiques et privées, NAT) • Les protocoles TCP et UDP • La configuration dynamique des ordinateurs (DHCP) • Le système DNS : notions de base	• Comprendre la structure d'Internet comme réseaux interconnectés • Comprendre l'acheminement des données sur Internet • Comprendre l'importance des adresses IP • Connaître la structure des adresses IP • Comprendre la différence entre adresses publiques et privées • Comprendre le fonctionnement d'un NAT • Connaître les protocoles TCP et UDP et leurs utilisations • Comprendre le protocole DHCP • Comprendre le système DNS	8 h
3. Principaux services et applications sur Internet • Le Web ○ Architecture, fonctionnement, HTTP, HTML • Les réseaux sociaux	• Comprendre le fonctionnement du WWW • Connaître les principaux réseaux sociaux sur Internet • Comprendre le fonctionnement du courrier électronique • Connaître les entités utilisées pour le courrier électronique (client mail,	12 h

• Le courrier électronique
  ○ Architecture, fonctionnement, protocoles
• Le chat (IRC) et la messagerie instantanée (IM), Twitter
  ○ Architecture, fonctionnement, protocoles
• La téléphonie sur IP
  ○ Fonctionnement de la VoIP
• Les réseaux P2P
  ○ Fonctionnement général
  ○ Principaux réseaux et applications P2P
• Le transfert de fichier
  ○ Principales applications
• Laboratoire pratique (4h)
	serveur SMTP, boîte email, clients Web)
	• Comprendre le fonctionnement du chat et de la messagerie instantanée sur Internet
	• Comprendre le fonctionnement de la téléphonie sur Internet
	• Comprendre le fonctionnement du P2P
	• Connaître les possibilités de transfert de fichiers	

4. Bases de la téléphonie fixe
• Transmission analogique et transmission numérique
• Téléphonie analogique
  ○ Architecture d'un réseau de téléphonie analogique
  ○ Boucle locale
  ○ Communication entre téléphone et central
  ○ Gestion des méta-données (HLR, CDR)
• Réseau numérique (ISDN)
  ○ Principes d'ISDN
  ○ Architecture d'un réseau ISDN
• Téléphonie sans fil (DECT)
	• Connaître les principes de la transmission analogique et la transmission numérique
	• Connaître l'architecture d'un réseau de téléphonie analogique
	• Comprendre la communication analogique entre un téléphone et le central
	• Connaître les principes de fonctionnement d'ISDN
	• Connaître les principes de la téléphonie DECT
		4 h

5. Bases de la téléphonie mobile
• Structure d'un réseau de téléphonie mobile
• Les réseaux GSM
  ○ Interface radio
  ○ Identification de terminaux (SIM)
  ○ Services (voix, WAP, SMS, MMS, GPRS)
  ○ Géolocalisation
• Autres types de réseaux mobiles (UMTS, CDMA)
• Principaux systèmes d'exploitation et applications des
	• Comprendre la structure d'un réseau de téléphonie mobile
	• Comprendre la transmission radio entre le téléphone et la station de base
	• Comprendre l'identificateur des terminaux par carte SIM
	• Connaître les différentes techniques de géolocalisation dans la téléphonie mobile
	• Connaître les principaux OS et applications mobiles
		8 h

téléphones mobiles		
6. **Organes gouvernementaux et cadres juridiques** • Organes gouvernementaux : SCPT, SCOCI & MELANI, ... • Cadre juridique (droit suisse)	• Connaître les tâches, le fonctionnement et l'organisation des principaux organes gouvernementaux luttant contre la criminalité sur Internet • Connaître le cadre juridique pour l'interception de données • Savoir comment manipuler et préserver les données interceptées	4 h
7**. Introduction au système ISS** • Vue d'ensemble • Scénarios typiques d'interception • Démonstration pratique : interprétation des données interceptées, fonctions d'analyse avancées proposées par l'ISS. • Laboratoire pratiques (4 h)	• Connaître le fonctionnement global du système ISS • Savoir mettre en place une interception de données • Savoir effectuer des scénarios d'interception typiques • Savoir consulter et interpréter globalement les données interceptées	8 h
		48 h

Module 2 : Interception dans les réseaux téléphoniques

Ce module se construit sur les connaissances acquises dans le module de base. Il fournit des approfondissements sur les technologies des réseaux téléphoniques.

Il s'adresse aux enquêteurs spécialistes qui doivent effectuer des interceptions complexes et interpréter les éléments techniques des données interceptées ainsi que les méta-données. Les objectifs généraux de ce module d'approfondissement sont :

- approfondir les notions de téléphonies fixe et mobile abordées dans le module de base
- savoir interpréter et analyser les données interceptées de téléphonies fixe et mobile
- savoir utiliser les outils d'analyse du système d'interception de données de téléphonies fixe et mobile

Chapitre	Objectifs	Vol.

1. Téléphonie fixe
• Architecture des réseaux téléphoniques commutés publics
• Communications
  ○ Liaisons entre centraux, et entre abonnés et centraux (lignes classiques, coaxiaux, fibres), canaux de communication
  ○ Commutation automatique
  ○ xDSL
• Réseaux commutés et opérateurs en Suisse, interconnexions et dépendances entre opérateurs
• Relation entre téléphonie fixe et le réseau IP, la VoIP, fonctionnement de la VoIP, interconnexions
	• Comprendre l'architecture des réseaux de téléphonie fixe, leurs interconnexions entre opérateurs
	• Comprendre les interconnexions des réseaux de téléphonie fixe, en particulier pour les opérateurs en Suisse
	• Comprendre les relations entre réseaux de téléphonie fixe et IP
	• Comprendre les relations entre la téléphonie fixe et la VoIP
		8 h

2. Téléphonie mobile
• Radiocommunication
  ○ Principales normes
  ○ Structures détaillées des principaux réseaux (GSM, UMTS, 4G) et interconnexion avec les réseaux commutés
  ○ Codage des signaux, utilisation des fréquences
  ○ Sécurité des communications (chiffrement, authentification)
  ○ Transferts d'un terminal entre cellules et réseaux
	• Comprendre les principales normes de radiocommunication en téléphonie mobile
	• Comprendre le besoin d'infrastructures séparées pour l'interception de GSM, UMTS, 4G
	• Comprendre l'architecture détaillée des principaux réseaux de téléphonie mobile et leurs interconnexions avec les réseaux de téléphonie fixe et avec le réseau Internet
	• Comprendre l'utilisation des fréquences, la sécurité des communications et le transfert d'un terminal entre cellules ("handover") et réseaux ("roaming")
		20 h

mobiles
• Géolocalisation et "tracking"
  ○ Antennes relais, directionnelles
  ○ Triangulation par cellules
  ○ GPS, géo-localisation WLAN
  ○ Technologies hybrides
• Les services
  ○ La diffusion (broadcast) de messages et le "paging"
  ○ Les SMS, MMS,
  ○ Internet : WAP, GPRS, ...
• Le terminal mobile
  ○ Identification de l'appareil
  ○ Identification de l'abonné
  ○ Systèmes d'exploitation et applications
  ○ Sécurité des terminaux mobiles (malware, accès, ...)
• Les opérateurs en Suisse et en Europe
	• Comprendre les différentes techniques de géolocalisation et de "tracking" dans la téléphonie mobile
	• Connaître de manière détaillée les différents services en téléphonie mobile, en particulier ceux utilisant Internet
	• Comprendre les mécanismes d'identification des appareils et des abonnés
	• Connaître les principales menaces et vulnérabilités sur les terminaux mobiles
	• Connaître les principaux opérateurs en Suisse et en Europe, ainsi que leurs relations	

3. ISS : fonctions d'analyse de trafics téléphoniques fixe et mobile • Vue d'ensemble des fonctions d'analyse • Géolocalisation de téléphones mobiles • Démonstrations pratiques	• Connaître et maîtriser les outils d'analyse de ISS	4 h
4. Laboratoire : interception et analyse de trafic sur les réseaux de téléphonie fixe • Premier laboratoire pratique sur la base de scénarios réalistes	• Savoir interpréter et analyser les données interceptées de téléphonie fixe et mobile.	8 h
5. Laboratoire : interprétation et analyse de trafic sur dans les réseaux de téléphonie mobile • Deuxième laboratoire pratique sur la base de scénarios réalistes	• Savoir interpréter et analyser les données interceptées de téléphonie fixe et mobile	8 h
		48 h

1.1 Module 3 : Interception dans les réseaux informatiques

Ce module se construit sur les connaissances acquises dans le module de base. Il fournit des connaissances plus approfondies sur les technologies des réseaux informatiques. Il s'adresse aux enquêteurs spécialistes qui doivent effectuer des interceptions complexes, notamment multi-protocoles, et interpréter et mettre en liaison les éléments techniques des données interceptées.

Les objectifs généraux de ce module d'approfondissement sont :

- approfondir les notions Internet (réseaux, services, applications) abordées dans le module de base
- savoir interpréter et analyser les données interceptées sur des réseaux IP
- savoir utiliser les outils d'analyse du système d'interception de données IP ISS.

Chapitre	Objectifs	Vol.

1. Le réseau Internet : notions avancées
• Rappel : IP, TCP/UDP
• Bases du routage sur Internet
• Adressage IP : classes, whois, RIR, introduction à IPv6
• La géolocalisation des adresses IP
• L'annuaire d'Internet : le système DNS
  ○ Base de données répartie du DNS, domaines géographiques et génériques, registrar, registry
  ○ La recherche de noms, système de cache
  ○ Format des messages
• Les fournisseurs d'accès en Suisse et en Europe
  ○ Fournisseurs régionaux
  ○ Backbones
  ○ Les logs : durée de conservation, correspondance IP/ménage, ...
	• Comprendre les principes du routage sur Internet
	• Comprendre comment fonctionne l'attribution des adresses IP
	• Comprendre le fonctionnement et les limites de la géolocalisation des adresses IP
	• Comprendre le fonctionnement du DNS
	• Savoir interpréter les messages DNS
		8 h

2. Technologies des réseaux locaux et sans fils • Structure de réseaux locaux • Réseaux Ethernet • Sécurité des réseaux : VPN, pare-feux • Réseaux sans fils (WLAN) • Sécurité des réseaux sans fils (WEP, WPA, WPA2)	• Connaître la structure d'un réseau LAN • Comprendre le fonctionnement d'Ethernet • Connaître le fonctionnement de la communication sans fils WLAN • Connaître les principaux éléments de la sécurité des réseaux locaux et sans fils	8 h

3. Applications et services Internet (approfondissement)
• Protocoles, formats et applications sur le Web
  ○ Architecture, fonctionnement, protocole HTTP, format HTML, système de cache
  ○ Les principales applications sur le web : réseaux sociaux, moteurs de recherche, blogs, etc.
• Le courrier électronique
  ○ Architecture, fonctionnement, SMTP, POP3, IMAP, clients Web (webmail)
  ○ Format du courrier électronique (MIME)
• Le chat (IRC) et la messagerie instantanée
  ○ Architecture, fonctionnement, protocoles et applications
• La téléphonie sur IP
  ○ Architecture, fonctionnement et protocoles de la VoIP
  ○ Interprétation des messages SIP
  ○ Fonctionnement de Skype
• Les réseaux P2P
  ○ Architecture, fonctionnement, protocoles et formats des principaux réseaux P2P
  ○ Fonctionnement des principales applications P2P
• Le transfert de fichier
  ○ Architecture, fonctionnement, protocoles et formats des principales applications de transfert de fichier sur Internet (mail, HTTP, FTP, P2P, applications chat)
	• Comprendre le fonctionnement du WWW
	• Savoir interpréter les messages HTTP
	• Savoir interpréter les contenus HTML
	• Connaître les principales applications sur le Web
	• Comprendre le fonctionnement du courrier électronique
	• Connaître les entités utilisées pour le courrier électronique (client mail, serveur SMTP, boîte email, clients Web)
	• Savoir interpréter les messages SMTP et leurs contenus (MIME)
	• Comprendre le fonctionnement du chat et de la messagerie instantanée sur Internet
	• Comprendre le fonctionnement de la téléphonie sur Internet
	• Savoir interpréter les entêtes de messages SIP
	• Comprendre le fonctionnement du P2P
	• Savoir interpréter le trafic P2P
	• Savoir interpréter les différentes possibilités de transfert de fichiers
		20 h

4. Bases de la sécurité sur Internet • Principes du chiffrement • Services sécurisés avec SSL/TLS • Principes de l'authentification, mots de passe des différents services et applications sur Internet	• Connaître les principes du chiffrement de données • Comprendre la sécurisation de services avec SSL/TLS • Connaître les principes de l'authentification sur Internet • Savoir repérer et extraire les différents mots de passe dans les services et application Internet	8 h
5. ISS : fonctions d'analyse de trafic Internet • Vue d'ensemble des fonctions d'analyse • Connaître les outils d'analyse externe à l'ISS (Wireshark,	• Connaître et maîtriser les outils d'analyse de ISS	4 h

CASEPilot, Quickview PRO, …) • Démonstrations pratiques		
6. Laboratoire : interception et analyse de trafic Internet • Premier laboratoire pratique sur la base de scénarios réalistes	• Savoir interpréter et analyser les données interceptées de réseaux IP.	8 h
7. Laboratoire : interception et analyse de trafic Internet • Deuxième laboratoire pratique sur la base de scénarios réalistes	• Savoir interpréter et analyser les données interceptées de réseaux IP.	8 h
		64 h