Alphorm.com

Catalogue de formations

Le meilleure de la formation IT, en ligne. Pour les Pros.


Sécurité

pfSense (2/2): Le firewall open source de référence

Transformez pfSense en un UTM grâce à ses packages complémentaires

Une formation Alphorm.com Durée : 4h46min

Public concerné :
Administrateur réseau, Responsable sécurité, Ingénieur réseaux / sécurité.

Description :
Dans cette deuxième formation pfsense, nous allons découvrir des fonctionnalités plus avancéesde pfSense, notamment les VPNs, avec un exemple de mise en place de VPNs via IPSEC (Exemple avec du Site-To-Site) et via OpenVPNs (Exemple avec du Point-To-Site).
Nous allons aussi pouvoir découvrir comment mettre en place des plans de haute disponibilité et redondance sans oublier la partie Bridging et Routing, spécialement la mise en place de Multi-Wan grâce à ofsense.

Prérequis :
• Connaissances de bases en réseaux informatiques et TCP/IP
• Formation pfSense (1/2) : Le firewall open source de référence

Objectifs :
• Mettre en place des VPNs avec IPSEC sous pfSense
• Mettre en place des VPNs avec OPENVPN sous pfSense
• Mettre en place des plans de Haute disponiblité et redondance sous pfSense
• Mettre en place du routing et bridging sous pfSense
• Mettre en place des IDS/PS sous pfSense
• Mettre en place des modules de filtrage de domaine sous pfSense

Programme détaillé :
voir page suivante

pfSense (2/2): Le firewall open source de référence

Transformez pfSense en un UTM grâce à ses packages complémentaires

Une formation Alphorm.com Durée : 4h46min

Programme détaillé >>>

- Présentation de la formation
- Les VPNs
- la Haute disponibilité et la redondance
- Routing et Bridging
- Packages complémentaires
- Troublshooting et test de sécurité
- Conclusion et perspectives

pfSense: Le firewall open source de référence

Comprendre et déployer avec succès le firewall open source pfSense

Une formation Alphorm.com Durée : 4h41min

Public concerné :
Administrateur réseau, Responsable sécurité, Ingénieur réseaux / sécurité

Description :
Dans cette première formation pfsense, nous allons pouvoir découvrir un bon nombre d'éléments de configuration de base, que nous allons détailler ensemble au niveau de la deuxième partie qui sera beaucoup plus pointue que la cette première.
Dans cette première formation pfsense, nous allons découvrir la solution pfSense, apprendre comment effectuer les configurations de bases (DHCP, DNS ,DDNS, NTP, SNMP, MAJ..), comment configurer des VLANs, comment effectuer des opérations de firewaling (Règles, NAT, Port Forwarding, Scheduling, Aliases…) ou encore comment garantir une QoS minimal grâce ce dernier.

Prérequis :
• Connaissances de bases en réseaux informatiques et TCP/IP

Objectifs :
• Découvrir la solution pfSense
• Configurer les différents services de pfSense (DHCP,DNS,DDNS,NTP,SNMP,MAJ..)
• Configurer les VLANs au niveau de pfSense
• Firewalling au niveau de pfSense (Règles, NAT, Port Forwarding,Scheduling, Aliases…)
• Configurer les Traffic Shappers

Programme détaillé :
voir page suivante

pfSense: Le firewall open source de référence

Comprendre et déployer avec succès le firewall open source pfSense

Une formation Alphorm.com Durée : 4h41min

Programme détaillé >>>

- Présentation de la formation
- Introduction et configuration de base de pfSense
- Les VLANss
- Firewalling
- Qualité de Service
- Conclusion et perspectives

La cryptomonnaie : décrypter son mystère

Découvrez la notion de blockchain et décryptez l'écosystème des cryptomonnaies.

Une formation Alphorm.com Durée : 4h44min

Public concerné :
Toute personne s'intéressant à la blockchain et aux cryptomonnaies

Prérequis :
• Aucun prérequis n'est nécessaire pour suivre cette formation

Description :
Grâce à cette formation sur les cryptomonnaies d'initiation, vous allez pouvoir comprendre la notion de blockchain, savoir acquérir, gérer et stocker de manière sécurisée des cryptomonnaies et découvrir le potentiel des cryptomonnaies.
Durant cette formation sur les cryptomonnaies, le formateur vous présentera plusieurs démonstrations pratiques pour vous familiariser avec les cryptomonnaies et leurs écosystème et outils.

Objectifs :
• Comprendre la notion de blockchain
• Appréhender la notion de crytomonnaie
• Comprendre, acheter et stocker de manière sécurisée des cryptomonnaies (incluant les altcoins)
• Découvrir la notion d'ICOs
• Comprendre les enjeux technologiques et économiques de la technologie des cryptomonnaies, du bitcoin et de la blockchain.

Programme détaillé :
voir page suivante

La cryptomonnaie : décrypter son mystère

Découvrez la notion de blockchain et décryptez l'écosystème des cryptomonnaies.

Une formation Alphorm.com Durée : 4h44min

Programme détaillé >>>

- Présentation de la formation
- Introduction à la Blockchain
- Les Cryptomonnaies
- Les Altcoins
- Régulation et Lois
- Conclusion et Perspectives

Comprendre le RGPD : Règlement Général Européen sur la Protection des Données

Comprendre et me se conformer au RGPD simplement et rapidement.

Une formation Alphorm.com Durée : 3h03min

Public concerné :

DPO, CIL et RSSI, Dirigeants, Responsables juridiques, Toute personne concernée par le traitement des données personnelles.

Prérequis :

• Aucune connaissance préalable n'est requise pour suivre cette formation.

Description :

Cette formation RGPD vous permettra d'effectuer le point sur les impacts du règlement européen sur les organismes et de proposer un plan de mise en conformité pour le RGPD. Elle vous donnera un guide RGPD à suivre pour définir la démarche à entreprendre et les bonnes pratiques pour se mettre en conformité avec le RGPD. Et enfin vous allez pouvoir dresser un plan d'actions de mise en conformité des traitements de données à caractère personnel

Objectifs :

• Effectuer le point sur les impacts du règlement européen sur les organismes et de proposer un plan de mise en conformité pour le RGPD,
• Définir la démarche à entreprendre et les bonnes pratiques pour se mettre en conformité avec le RGPD,
• Proposer un plan d'actions de mise en conformité des traitements de données à caractère personnel.

Programme détaillé :

voir page suivante

Comprendre le RGPD : Règlement Général Européen sur la Protection des Données

Comprendre et me se conformer au RGPD simplement et rapidement.

Une formation Alphorm.com Durée : 3h03min

Programme détaillé >>>

- Présentation de la formation
- Introduction au RGPD
- Etape 1 : Désigner un DPO
- Etape 2 : CARTOGRAPHIER VOS TRAITEMENTS DE DONNÉES PERSONNELLES
- Etape 3 : Prioriser les actions à mener
- Etape 4 : GÉRER LES RISQUES
- Etape 5 : ORGANISER LES PROCESSUS INTERNES
- Etape 6 : DOCUMENTER LA CONFORMITÉ
- Conclusions

CND (Certified Network Defender) 2/2 : Réussir la certification CND

Préparez et réussissez votre certification CND (Certified Network Defender), la meilleure en matière de défense.

Une formation Alphorm.com Durée : 9h25min

Public concerné :
Responsable sécurité, Toute personne impliquée dans des opérations réseaux.

Description :
Cette formation CND vous permettra de découvrir les différentes méthodologies et approches afin de pouvoir configurer, déployer et exploiter correctement différents périphériques de sécurité (HIDS, IDS, VPN, Firewall), la supervision des réseaux informatiques, la gestion des backups, ainsi que la découverte d'une nouvelle notion très importante et qui concerne la sécurité organisationnelle, avec la gestion du risque et des incidents de sécurité informatique.

Prérequis :
• Connaissances de base de la pile TCP/IP,
• Connaissances de base configuration OS,
• Avoir suivis le Tome 1 de la Certified Network Defender.

Objectifs :
• Durcissement et supervision des réseaux et des systèmes,
• Mise en place et configuration sécurisée des firewalls, VPN, IDS,
• Effectuer des analyses de risques,
• Mise en place des plans d'intervention et de réponse sur incident.

Programme détaillé :
voir page suivante

CND (Certified Network Defender) 2/2 : Réussir la certification CND

Préparez et réussissez votre certification CND (Certified Network Defender), la meilleure en matière de défense.

Une formation Alphorm.com Durée : 9h25min

Programme détaillé >>>

- Présentation de la formation
- Durcissement et sécurité hôte
- Configuration et gestion sécurisé des firewalls
- Configuration et gestion sécurisé des IDS
- Configuration et gestion sécurisé des VPN
- Protection des réseaux sans fils
- Supervision et analyse du traffic réseau
- Risques réseaux et vulnerability management
- Data backup et recovery
- Gestion et réponses aux incidents réseau
- Conclusion et perspectives

CND (Certified Network Defender) 1/2 : Réussir la certification CND

Préparez et réussissez votre certification CND (Certified Network Defender), la meilleure en matière de défense.

Une formation Alphorm.com Durée : 8h52min

Public concerné :

Administrateurs réseaux, Administrateurs sécurité réseaux, Ingénieur sécurité réseaux, Technicien défense du réseau, Analyste CND, Analyste sécurité, Responsable sécurité, Toute personne impliquée dans des opérations réseaux.

Description :

Le Certified Network Defender (CND) est un cours vendor-neutral, c'est à dire sans orientation technique vis à vis d'un quelconque fournisseur de matériel ou d'éditeur de solutions de sécurité des réseaux informatiques.
Le cursus CND est un cours 50 % pratique sous forme de labs, modélisant les activités courantes d'administrateurs réseaux, basés sur les outils et techniques les plus utilisés dans la sécurité réseau.

Prérequis :

- Connaissances de base de la pile TCP/IP,
- Connaissances de base configuration OS,
- Première expérience dans le domaine IT,
- Motivation et passion.

Objectifs :

- Atténuer et se défendre des attaques informatiques,
- Durcissement réseaux et systèmes,
- Mise en place de politique de sécurité réseau,
- La sécurité physique,
- Défense des réseaux informatiques,
- Périphériques de sécurité réseaux,
- Techniques de Hacking.

Programme détaillé :

voir page suivante

CND (Certified Network Defender) 1/2 : Réussir la certification CND

Préparez et réussissez votre certification CND (Certified Network Defender), la meilleure en matière de défense.

Une formation Alphorm.com Durée : 8h52min

Programme détaillé >>>

• Présentation de la formation
• Réseaux informatiques et fondamentaux de la sécurité défensive
• Menaces, Vulnérabilités et attaques sur les réseaux
• Contrôles de sécurité, protocoles et périphériques réseaux
• Conception et implémentation d'une politique de sécurité réseau
• Sécurité Physique
• Sécurité de l'hôte
• Conclusion et Perspectives

Comptia Security+ (2/2) : Réussir la certification SY0-401

Maîtrisez les bases de la sécurité et Réussissez votre certification Comptia Security+ SY0-401.

Une formation Alphorm.com Durée : 7h54min

Public concerné :
Techniciens, Ingénieur, RSSI, DSI, Toute personne désirant entrer dans le monde de la sécurité informatique.

Description :
La certification CompTIA Security + est une validation de connaissances indépendante des constructeurs et éditeurs de solutions de sécurité.
L'obtention de l'examen valide les compétences requises pour identifier les risques, proposer des solutions, mettre en place des architectures sécurisées et maintenir un niveau de sécurité adéquat.
Durant la formation, des ateliers pratiques sont mis en place et une préparation à l'examen sera offerte aux abonnés d'Alphorm.

Prérequis :
• Avoir une connaissance de base de la pile TCP/IP,
• Savoir configurer et paramétrer une machine,
• Avoir une première expérience dans le domaine IT (Idéalement),
• Avoir suivis le tome 1 de la formation CompTIA Security +.

Objectifs :
• Identifier les menaces et risques en matière de sécurité des systèmes d'informations,
• Mettre en place un système de gestion d'identité et de droits,
• Superviser la sécurité de son infrastructure,
• Appréhender la notion de sécurité offensive.

Programme détaillé :
voir page suivante

Comptia Security+ (2/2) : Réussir la certification SY0-401

Maîtrisez les bases de la sécurité et Réussissez votre certification Comptia Security+ SY0-401.

Une formation Alphorm.com Durée : 7h54min

Programme détaillé >>>

• Présentation de la formation
• Menaces et vulnérabilités : Vulnérabilités Applicatives
• Menaces et vulnérabilités : Scanning et Sécurisation des réseaux
• Contrôle d'accès, Authentification et Authaurisation
• Hôte, données et sécurité applicative
• Cryptographie
• Administration Sécurisé
• Disaster Recovery and Incident Response
• Sécurité Opérationnelle
• Conclusion

Azure Active Directory RMS et Azure Information Protection

Apprenez à sécuriser votre environnement Microsoft grâce à Azure Active Directory RMS et Azure Information Protection.

Une formation Alphorm.com Durée : 4h28min

Public concerné :
Ingénieur IT, Consultant It, Ingénieur / consultant Sécurité, Geek qui souhaite apprendre de nouvelles technologies.

Description :
Cette formation sur Azure RMS et Azure Information protection qui fait partie du cursus Formation EMS est destinées aux passionnés de sécurités. Dans cette formation, les participants vont apprendre toutes les notions de sécurités au niveau des mails et fichiers avec Azure RMS.
Cette formation traite aussi bien la partie Design, implémentation, administration, troubleshooting que la partie Monitoring. De plus, la formation traite la partie data classification des documents et mail qui sont importants au sein d'un système d'information.

Prérequis :
• Connaissance Active Directory,
• Connaissance Office 365 de base,
• Connaissance de base le monde du cloud Microsoft Azure,
• Connaissance de base en sécurité informatique.

Objectifs :
• Activer le service Azure RMS,
• Utiliser Office 365,
• Sécuriser les échanges de mail et fichiers au sein du système d'information,
• D'Administrer Azure RMS,
• Dépanner Azure RMS,
• Classifier les documents et Mail.

Programme détaillé :
voir page suivante

Azure Active Directory RMS et Azure Information Protection

Apprenez à sécuriser votre environnement Microsoft grâce à Azure Active Directory RMS et Azure Information Protection.

Une formation Alphorm.com Durée : 4h28min

Programme détaillé >>>

- Présentation de la formation
- Démarrer avec Azure RMS et information protection
- Préparation de l'environnement client
- Chiffrement des e-Mails
- Chiffrement des fichiers
- Data classification avec Azure Infirmation protection
- Gestion et Surveillance de l'environnement
- Retour d'expérience
- Conclusion

Comptia Security+ (1/2) : Réussir la certification SY0-401

Maîtrisez les bases de la sécurité et Réussissez votre certification Comptia Security+.

Une formation Alphorm.com Durée : 7h53min

Public concerné :
Techniciens, Ingénieur, RSSI, DSI, Toute personne désirant entrer dans le monde de la sécurité informatique.

Description :
Lors de cette formation, les participants pourront découvrir les bases de la sécurité réseau, les dispositifs de sécurité logiciels et matériels, les menaces et vulnérabilités des systèmes, la sécurité des utilisateurs et des applications, la gestion de l'identité et des autorisations et les méthodes de cryptographie.
La certification CompTIA est accréditée par l'ISO sous la référence ISO 17024.

Prérequis :
• Avoir une connaissance de base de la pile TCP/IP,
• Savoir configurer et paramétrer une machine,
• Avoir une première expérience dans le domaine IT (Idéalement),

Objectifs :
• Identifier les menaces et risques en matières de sécurité des systèmes d'informations,
• Découvrir les solutions logicielles et matérielles nécessaire à la mise en place d'une infrastructure sécurisé,
• Mettre en place un système de gestion d'identité et de droits,
• Superviser la sécurité de son infrastructure,
• Appréhender la notion de sécurité offensive.

Programme détaillé :
voir page suivante

Comptia Security+ (1/2) : Réussir la certification SY0-401

Maîtrisez les bases de la sécurité et Réussissez votre certification Comptia Security+.

Une formation Alphorm.com Durée : 7h53min

Programme détaillé >>>

- Présentation de la formation
- Sécurité réseau : Identification des composants réseaux
- Sécurité réseau : Sécurité des réseaux sans fils
- Les Menaces et Vulnérabilités
- La sécurité opérationnelle, Partie 1 : Initiation
- Conclusion

Stormshield version 3 : Comprendre les mises à jour

Devenez expert sur les modules les plus utilisés sur Stormshield v3.

Une formation Alphorm.com Durée : 2h18min

Public concerné :
Responsables informatique, Administrateurs réseaux, Tout technicien informatique souhaitant administrer Stormshield, Toute personne souhaitant découvrir et apprendre Stormshield.

Description :
Suite aux formations Stormshield Network Administrateur, et stormshield expert.
Mathieu BAYLE vous a préparé cette nouvelle formation Stormshield Network V3 afin d'approfondir vos connaissances et maîtriser de nouvelles techniques avancées sur Stormshield et les nouvelles fonctionnalités de la version 3 sortie début 2017.

Prérequis :
• Avoir suivi les formations Stormshield Network Administrateur, et Stormshield Experts
• Avoir de bonnes connaissances en TCP/IP.

Objectifs :
• Approfondir votre connaissance sur les équipements Stormshield,
• Devenir expert sur les modules les plus utilisés et découvrir les autres modules de la version 3 sur Stormshield.

Programme détaillé :
voir page suivante

Stormshield version 3 : Comprendre les mises à jour

Devenez expert sur les modules les plus utilisés sur Stormshield v3.

Une formation Alphorm.com Durée : 2h18min

Programme détaillé >>>

- Présentation de la formation
- La Version 3
- Conclusion

Microsoft ATA 2016 : Installation et Configuration

Découvrez le fonctionnement du produit ATA pour sécuriez mieux votre infra Microsoft.

Une formation Alphorm.com Durée : 3h28min

Public concerné :
Consultant infrastructure, Ingénieur système et réseaux, Consultant Sécurité, et geek.

Prérequis :
• Connaissance Windows Server 2012 R2 / ou encore windows Server 2016,
• Connaissance des notions de sécurité et réseaux.

Description :
Cette formation ATA a pour but de vous faire découvrir le produit Microsoft ATA, c'est à dire de la présentation du produit jusqu'à sa mise en œuvre en passant par les phases de design et réflexion.
Cette formation ATA est basée sur un retour d'expérience terrain via un déploiement world wide de ce produit, ce qui permet au formateur de partager son expérience avec des cas pragmatiques rencontrés en entreprise.

Objectifs :
• Découverte le produit Microsoft ATA au sein de la suite EMS (Entreprise Mobilité + Sécurité),
• Design, planification,
• Savoir installer et configurer Microsoft ATA,
• Sécuriser son environnement Active Directory.

Programme détaillé :
voir page suivante

Microsoft ATA 2016 : Installation et Configuration

Découvrez le fonctionnement du produit ATA pour sécuriez mieux votre infra Microsoft.

Une formation Alphorm.com Durée : 3h28min

Programme détaillé >>>

- Présentation de la formation
- Réflexion / avant installation
- Installation
- Administration
- Troubleshooting
- Conclusion

Certified Ethical Hacker v9 (4/4) : Réussir CEH v9

Finalisez vos compétences en Hacking et réussissez votre certification CEH v9.

Une formation Alphorm.com Durée : 7h49min

Public concerné :
Responsables sécurité, Auditeurs, Consultant sécurité, Professionnels de la sécurité, Administrateurs de site, Toute personne concernée par la stabilité des systèmes d'information.

Description :
Dans cette formation CEH, vous allez comprendre le concept des trojan, Metasploit, des virus, et de Ver.
Pendant cette formation CEH, Hamza vous apprendra les techniques de Hacking des réseaux sans fils, ainsi que ceux des périphériques mobile, l'évasion d'IDS, Firewall et Honeypot, sans oublier la sécurité au niveau du Cloud Computing, et les contremesures contre ce genre d'attaques.

Prérequis :
• Avoir suivi la formation Certified Ethical Hacker v9 (1/4) : Réussir CEH v9,
• Avoir suivi la formation Certified Ethical Hacker v9 (2/4) : Réussir CEH v9,
• Avoir suivi la formation Certified Ethical Hacker v9 (3/4) : Réussir CEH v9.

Objectifs :
• Enrichir les bases du hacking éthique,
• Apprendre des nouvelles fonctionnalités avancées du hacking éthique,
• Comprendre et mettre en pratique les attaques sur les réseaux sans fils,,
• Comprendre les notions de bases en cryptographie,
• Préparer et réussir la certification CEH v9.

Programme détaillé :
voir page suivante

Certified Ethical Hacker v9 (4/4) : Réussir CEH v9

Finalisez vos compétences en Hacking et réussissez votre certification CEH v9.

Une formation Alphorm.com Durée : 7h49min

Programme détaillé >>>

- Présentation de la formation
- Réseaux sans fils
- Mobile
- Evasion IDS,Firewalls et pots de miel
- Cloud Computing
- Cryptographie
- Conclusion

Certified Ethical Hacker v9 (3/4) : Réussir CEH v9

Découvrez les techniques de Session Hijacking et de Hacking de serveurs ou d'applications web.

Une formation Alphorm.com Durée : 8h40min

Public concerné :
Responsables sécurité, Auditeurs, Consultant sécurité, Professionnels de la sécurité, Administrateurs de site, Toute personne concernée par la stabilité des systèmes d'information.

Description :
Voici la suite de la formation CEH v9 préparée par Hamza KONDAH, pour booster vos connaissances en matière de piratage éthique et augmenter vos chances de succès pour l'examen du CEH v9 (Certified Ethical Hacker). Dans ce 3ème volet de la formation CEH v9, Hamza KONDAH vous apprendra
- les techniques de Session Hijacking
- les techniques de hacking de serveurs
- les techniques de hacking d'applications web
Surtout, cette formation CEH v9 vous fera découvrir et maîtriser les principales contremesures grâce auxquelles vous pourrez faire face à ces attaques.

Prérequis :
• Avoir suivi la formation Certified Ethical Hacker v9 (1/4) : Réussir CEH v9,
• Avoir suivi la formation Certified Ethical Hacker v9 (2/4) : Réussir CEH v9,
• Avoir déjà des connaissances de base sur le Hacking.

Objectifs :
• Approfondir vos connaissances du hacking éthique.
• Comprendre et savoir mettre en pratique les attaques de Session Hijacking.
• Comprendre et savoir mettre en pratique les techniques de hacking de serveurs et applications web.
• Préparer et réussir la certification CEH v9.

Programme détaillé :
voir page suivante

Certified Ethical Hacker v9 (3/4) : Réussir CEH v9

Découvrez les techniques de Session Hijacking et de Hacking de serveurs ou d'applications web.

Une formation Alphorm.com Durée : 8h40min

Programme détaillé >>>

- Présentation de la formation
- Session Hijacking
- Hacking serveurs Web
- Hacking applications web
- SQL Injection
- Conclusion

Certified Ethical Hacker v9 (2/4) : Réussir CEH v9

Maîtrisez la méthodologie de piratage éthique avec la formation CEH V9 II.

Une formation Alphorm.com Durée : 5h41min

Public concerné :
Responsables sécurité, Auditeurs, Consultant sécurité, Professionnels de la sécurité, Administrateurs de site, Toute personne concernée par la stabilité des systèmes d'information.

Description :
Voici la suite de la formation CEH v9 (1/4) préparée par Hamza KONDAH, pour booster vos connaissances en matière de piratage éthique et augmenter vos chances de succès pour l'examen du CEH v9 (Certified Ethical Hacker). Ce 2nd volet vous permettra de : - comprendre les concepts de Trojan, Metasploit, Virus et Ver
- maîtriser le sniffing et le Social Engineering
- découvrir les contremesures avec DoS/DDoS
Pour aller plus loin dans la préparation de l'examen CEH v9 (Certified Ethical Hacker) : Certified Ethical Hacker v9 (3/4) : Réussir CEH v9

Prérequis :
• Avoir suivi la formation Certified Ethical Hacker v9 1/4 : Réussir CEH v9,
• Connaissances professionnelles de TCP/IP, Linux et Windows Server,
• Avoir des connaissances sur le Hacking.

Objectifs :
• Enrichir votre connaissance du hacking éthique.
• Découvrir des nouvelles fonctionnalités avancées du hacking éthique.
• Comprendre les malwares.
• Apprendre les contremesures.
• Préparer et réussir la certification CEH v9.

Programme détaillé :
voir page suivante

Certified Ethical Hacker v9 (2/4) : Réussir CEH v9

Maîtrisez la méthodologie de piratage éthique avec la formation CEH V9 II.

Une formation Alphorm.com Durée : 5h41min

Programme détaillé >>>

- Présentation général
- Présentation de la formation
- La menace des malwares
- Sniffing
- Social Engineering
- Dénis de service
- Conclusion

SOPHOS XG FIREWALL : Administration

Découvrez et maîtrisez les fonctionnalités de la nouvelle génération du parefeu Sophos XG FIREWALL.

Une formation Alphorm.com Durée : 6h44min

Public concerné :
Partenaires/Clients Sophos pour passer la Certification SCE/SCA, Administrateurs et Techniciens Réseaux, Architecte/Ingénieurs Réseaux et Sécurité, Migrant vers Sophos venant d'une autre solution : Cisco Asa, Fortinet, Anciens clients Cyberoam.

Description :
Tout au long de cette formation Sophos, Djawad vous montrera comment monter un Lab Sophos XG Firewall très complet pour faire toutes vos manipulations, ainsi, il vous montrera comment tirer profit de ce magnifique produit en suivant les astuces et les best practicies.

Prérequis :
• Avoir suivi la formation Sophos UTM : Acquérir les fondamentaux,
• Avoir suivi la formation Sophos UTM : Maîtriser les fonctionnalités avancées.

Objectifs :
• Comprendre le fonctionnement des pare-feu de nouvelle génération Sophos XG Firewall,
• Comprendre et Configurer les différents services et fonctionnalités (Interface, Réseaux, DNS, DHCP, …),
• Administrer Sophos XG Firewall.

Programme détaillé :
voir page suivante

SOPHOS XG FIREWALL : Administration

Découvrez et maîtrisez les fonctionnalités de la nouvelle génération du parefeu Sophos XG FIREWALL.

Une formation Alphorm.com Durée : 6h44min

Programme détaillé >>>

- Introduction à la formation
- Environnement de travail
- Installation et activation du produit
- Configuration du système
- La protection réseau
- Authentification
- Conclusion

Certified Ethical Hacker v9 (1/4) : Réussir CEH v9

Faites vos premiers pas vers l'ethical hacking tout en préparant votre certification CEH v9.

Une formation Alphorm.com Durée : 8h31min

Public concerné :
Responsables sécurité, Auditeurs, Consultant sécurité, Professionnels de la sécurité, Administrateurs de site, Toute personne concernée par la stabilité des systèmes d'information.

Description :
La formation permet à tous les informaticiens et passionnés d'informatique de découvrir et de maîtriser les modes opératoires et les méthodes employées par les hackers, ainsi que plus de 2.200 outils utilisés par les pirates informatiques pour contourner et déjouer les protections de sécurité.
Cette formation CEH v9 vous permettra d'acquérir une vision étendue des différents types d'attaques possibles et d'acquérir une méthodologie de piratage éthique efficace, pouvant être utilisée aussi bien lors d'un test d'intrusion que dans une situation de piratage éthique.

Prérequis :
• Connaissances professionnelles de TCP/IP, Linux et Windows Server,
• Avoir des connaissances sur le Hacking.

Objectifs :
- Comprendre les bases du hacking éthique,
- Maîtriser et mettre en œuvre la reconnaissance,
- Assimiler et pratiquer les techniques du scanning,
- Comprendre l'énumération et le hacking des systèmes,
- Préparer et réussir la certification CEH v9.

Programme détaillé :
voir page suivante

Certified Ethical Hacker v9 (1/4) : Réussir CEH v9

Faites vos premiers pas vers l'ethical hacking tout en préparant votre certification CEH v9.

Une formation Alphorm.com Durée : 8h31min

Programme détaillé >>>

- Présentation général
- Introduction au Hacking Éthique
- Reconnaissance
- Scanning
- Enumération
- Hacking de Systèmes
- Conclusion

Stormshield Network Expert (2/2)

Devenez un Expert Stormshield Network.

Une formation Alphorm.com Durée : 10h44min

Public concerné :
Responsables informatique, Administrateurs réseaux, Tout technicien informatique souhaitant administrer Stormshield, Toute personne souhaitant découvrir et apprendre Stormshield.

Description :
Pendant cette formation Stormshield, vous allez voir et maîtriser les modules avancés de Stormshield : la Haute disponibilité, le routage avec plusieurs passerelles, la partie PKI, la gestion des utilisateurs avec LDAP Interne, la gestion des utilisateurs avec LDAP Externe, l'interaction avec les utilisateurs et les groupes, la mise en application de l'antivirus, la mise en application de la partie anti SPAM, les règles complexes avec inspection de Flux SSL, les filtrages d'URL avancés avec options payantes, la mise en place d'un portail captif...

Prérequis :
• Avoir suivi la formation Stormshield Network Administrator,
• Avoir de bonnes connaissances en TCP/IP.

Objectifs :
• Approfondir votre connaissance sur les équipements Stormshield,
• Utiliser de manière avancée l'IHM sur Stormshield,
• Connaître la partie VPN sur le bout des doigts,
• Gérer la configuration Stormshield dans les cas les plus complexes,
• Créer un cluster haute disponibilité.

Programme détaillé :
voir page suivante

Stormshield Network Expert (2/2)

Devenez un Expert Stormshield Network.

Une formation Alphorm.com Durée : 10h44min

Programme détaillé >>>

- Présentation de la formation
- Les Modules avancés
- Conclusion

Les sciences forensiques : L'investigation numérique

Découvrez et maîtrisez les techniques forensiques utilisées dans les investigations numériques.

Une formation Alphorm.com Durée : 7h34min

Public concerné :
Tout membre d'une équipe de réponse d'investigation numérique qui est amené à traiter des incidents de sécurité complexes et ayant besoin de la forensique dans son activité.

Description :
Avec cette formation sur les sciences forensiques pour l'investigation numérique, vous allez apprendre à collecter correctement les preuves nécessaires à des poursuites judiciaires mais aussi d'acquérir de l'expérience sur les différentes techniques d'investigation et l'acquisition de preuve virtuelle, dans la gestion et l'analyse de façon légale.

Prérequis :
- Avoir des notions de bases Linux,
- Avoir suivi la formation Hacking et Sécurité, l'essentiel,
- Avoir suivi la formation Hacking & Sécurité, Avancé,
- Notions de bases administration Windows.

Objectifs :
- Comprendre les méthodes et procédures d'investigations numériques,
- Identifier et analyser les traces laissées lors de l'intrusion dans un système informatique,
- Collecter et Analyser des informations à des fins d'investigation,
- Bypasser les protections,
- Tracking,
- Retrouver les traces : personnes ou journaux.

Programme détaillé :
voir page suivante

Les sciences forensiques : L'investigation numérique

Découvrez et maîtrisez les techniques forensiques utilisées dans les investigations numériques.

Une formation Alphorm.com Durée : 7h34min

Programme détaillé >>>

- Introduction à la formation
- Les sciences Forensiques
- Investigation légale sous Windows
- Investigation légale sous Linux
- Investigation légale USB
- Investigation légale Mobile
- Stéganographie
- Investigation Réseaux
- Autres techniques d'investigation
- Rapports d'investigation
- Conclusion

Fortinet Fortigate UTM (NSE4) (2/2): Les fonctionnalités avancées

Maîtrisez les fonctionnalités avancées de Fortinet Fortigate UTM : Clustering, Routage, VDOMs, Diagnostic et les certificats.

Une formation Alphorm.com Durée : 5h13min

Public concerné :

Toute personne qui prépare la certification NSE4 (Network Security Expert), Toute personne responsable de la gestion quotidienne de l'appliance Fortigate UTM.

Description :

Dans cette formation Fortinet UTM, vous allez découvrir les fonctionnalités avancées du pare-feu Fortigate : le routage avancé, le mode transparent, les VDOMs, les certificats, la HA, les outils de diagnostic.
Les chapitres traités au cours de cette formation Fortinet UTM visent à compléter vos connaissances des pare-feu Fortigate UTM et vous permettre de déployer des architectures de sécurité réseau complexes. La formation Fortinet Fortigate UTM (NSE4) et cette formation les Fonctionnalités avancées vous préparent et vous aident à réussir la certification NSE4 (Network Security Expert).

Prérequis :

- Avoir suivi la formation Fortinet Fortigate UTM (NSE4),
- Connaissance des couches OSI,
- Connaissance des concepts de pare-feu dans un réseau IPv4

Objectifs :

- Déployer des Fortigate en Cluster,
- Inspecter le trafic en mode transparent,
- Analyser la table de routage d'un Fortigate,
- Utiliser des domaines virtuels (VDOM) sur les Fortigate,
- Diagnostiquer et corriger des problèmes,
- Dimensionner un produit Fortigate,
- Comprendre le support Fortinet,
- Préparer et réussir la certification NSE4 (Network Security Expert).

Programme détaillé :

voir page suivante

Fortinet Fortigate UTM (NSE4) (2/2): Les fonctionnalités avancées

Maîtrisez les fonctionnalités avancées de Fortinet Fortigate UTM : Clustering, Routage, VDOMs, Diagnostic et les certificats.

Une formation Alphorm.com Durée : 5h13min

Programme détaillé >>>

- Présentation de la formation
- Le routage
- La virtualisation de pare-feu
- Le mode Transparent
- Les certificats
- La haute disponibilité (HA)
- Les outils de diagnostic
- Dimensionnement et support
- Conclusion

Stormshield (1/2) : Le Guide Complet

Installez et protégez votre réseau avec le puissant Stormshield.

Une formation Alphorm.com Durée : 10h14min

Public concerné :
Responsables informatique, Administrateurs réseaux, Tout technicien informatique souhaitant administrer avec Stormshield, Toute personne souhaitant découvrir et apprendre Stormshield.

Description :
Nous allons voir ensemble au cours de cette formation Stormshield comment construire des règles de Firewall afin de vous protéger mais également conseiller. Vous aborderez les bases de la logique à adopter pour construire une protection efficace mais également rendre disponible vos ressources sur Internet. Connaître et configurer les fonctionnés majeurs des produits Stormshield, reprendre la main sur le firewall en cas d'erreur de configuration et Installer un tunnel VPN entre des sites distants.

Prérequis :
• Avoir de bonnes connaissances en TCP/IP,
• Les logiciels suivants : Firefox, PuTTY (ou tout autre client SSH), WinSCP (ou client SCP équivalent), Wireshark, VirtualBox ou équivalent Vmware (Vmware player ou Vmware workstation).

Objectifs :
• Découvrir et connaître les systèmes Stormshield,
• Etre capable d'installer et configurer les systèmes Stormshield,
• Mettre en place l'UTM Stormshield dans un réseau.

Programme détaillé :
voir page suivante

Stormshield (1/2) : Le Guide Complet

Installez et protégez votre réseau avec le puissant Stormshield.

Une formation Alphorm.com Durée : 10h14min

Programme détaillé >>>

- Présentation de la formation
- Introduction
- Configuration de base
- Les services
- Conclusion

Hacking & Sécurité, Expert : Les vulnérabilités des Réseaux

Protégez votre réseau des attaques en détectant et en corrigeant ses vulnérabilités les plus critiques.

Une formation Alphorm.com Durée : 8h59min

Public concerné :
Concepteurs réseaux, Chefs de projet réseaux, Consultant en sécurité informatique, Responsable de la sécurité informatique, Responsables DSI, Toute personne en charge de la sécurité informatique.

Description :
Pendant cette formation Hacking et Sécurité sur les Vulnérabilités Réseaux, nous mettons l'accent sur la compréhension technique et pratique des différentes formes d'attaques existantes, en mettant l'accent sur les vulnérabilités et exploitations les plus critiques.
Vous pourrez, au terme de cette formation Hacking et Sécurité sur les Vulnérabilités Réseaux, réaliser des audits de sécurité (test de pénétration) au sein de votre infrastructure réseau, que ça soit en milieu entreprise ou personnel.

Prérequis :
• Avoir suivi la formation Hacking et Sécurité Expert, Vulnérabilités Web,
• Avoir suivi la formation Hacking et Sécurité, l'essentiel,
• Avoir suivi la formation Hacking & Sécurité, Avancé,
• Avoir suivi la formation Hacking et Sécurité Expert - Réseaux sans fils,
• Avoir suivi la formation Hacking et Sécurité Expert, Metasploit

Objectifs :
• Exploitation basique et avancée,
• Protégez vos réseaux,
• Mise en situation réelle d'attaques réseaux,
• Approche Python dans le pentesting,
• Maîtriser les attaques réseaux avec Wireshark.

Programme détaillé :
voir page suivante

Hacking & Sécurité, Expert : Les vulnérabilités des Réseaux

Protégez votre réseau des attaques en détectant et en corrigeant ses vulnérabilités les plus critiques.

Une formation Alphorm.com Durée : 8h59min

Programme détaillé >>>

- Introduction
- Notions de base
- Attaques sur les routeurs
- Environnement Windows
- Post Exploitation
- Attaques sur le client
- Attaques avancées
- Python : Puissance et Élégance
- Contremesures & Défenses
- Conclusion et Perspectives

Hacking et Sécurité, Expert : Les vulnérabilités Web

Protégez vos applications Web en détectant et en corrigeant leurs vulnérabilités.

Une formation Alphorm.com Durée : 7h10min

Public concerné :
Pentesteur, Développeur chargé de la sécurité des applications web, Responsables DSI, Consultant en sécurité informatique, Responsables sécurité informatique, Toute personne en charge de la sécurité informatique.

Description :
A la suite de cette formation Hacking et Sécurité sur les Vulnérabilités Web, vous serez capable de bien comprendre les vulnérabilités web les plus critiques, les exploiter mais aussi les sécuriser. On aura aussi l'opportunité d'attaquer sous différents vecteurs, en exploitant par exemple le Client Side ou encore le server side par apport à la plateforme Web.

Prérequis :
• Avoir suivi la formation Hacking et Sécurité, l'essentiel,
• Avoir suivi la formation Hacking & Sécurité, Avancé,
• Avoir suivi la formation Hacking et Sécurité Expert - Réseaux sans fils,
• Avoir suivi la formation Hacking et Sécurité Expert, Metasploit.

Objectifs :
• Test de pénétration des applications web,
• Exploitation basique et avancée,
• Attaques au niveau de plusieurs couches des applications web,
• Adopter une approche offensive,
• Protéger les applications web,
• Structuration des connaissances,
• Mise en situation réel de hacking des applications web.

Programme détaillé :
voir page suivante

Hacking et Sécurité, Expert : Les vulnérabilités Web

Protégez vos applications Web en détectant et en corrigeant leurs vulnérabilités.

Une formation Alphorm.com Durée : 7h10min

Programme détaillé >>>

- Introduction
- Reconnaissance
- Exploitation
- Client Side
- Attaque sur l'authentification
- CMS
- Contremesures et reporting
- Conclusion et Perspectives

Sophos UTM (2/2) : Maîtriser les fonctionnalités avancées

Devenez un as de la protection et sécurité en maîtrisant Sophos UTM 9 et ses fonctionnalités très avancées.

Une formation Alphorm.com Durée : 5h59min

Public concerné :
Administrateurs et Ingénieurs réseau et sécurité utilisant Sophos UTM 9, Ceux qui veulent passer la certification SCE et SCA (Sophos Certified Engineer/Architect), Toute personne qui veut maîtriser Sophos UTM.

Description :
Djawad vous accompagnera tout au long de cette formation Sophos UTM 9, pour comprendre et maîtriser la solution Sophos UTM 9 avec des explications techniques, théoriques et des démonstrations des meilleures pratiques avec un LAB que vous pouviez reprendre chez vous afin de consolider les connaissances et les compétences acquises dans cette formation Sophos UTM 9.

Prérequis :
• Avoir suivi la formation Sophos UTM 9,
• Connaissances des réseaux informatiques et protocoles TCP/IP,
• Connaissances de base sur les pare-feu de nouvelle génération.

Objectifs :
• Comprendre le fonctionnement des modules de Sophos UTM 9,
• Préparation de la certification Sophos Certified Engineer SCE,
• Protéger votre infrastructure web avec Sophos UTM 9,
• Implémenter la protection des emails via Sophos UTM 9.

Programme détaillé :
voir page suivante

Sophos UTM (2/2) : Maîtriser les fonctionnalités avancées

Devenez un as de la protection et sécurité en maîtrisant Sophos UTM 9 et ses fonctionnalités très avancées.

Une formation Alphorm.com Durée : 5h59min

Programme détaillé >>>

- Introduction à la formation
- Les fondamentaux - La suite
- Protection Web
- Email Protection
- Endpoint Protection
- Wireless Protection
- Webserver Protection
- Gestion de RED
- VPN site à site
- Accès à distance
- Reporting et journalisation
- Dimensionnement et Support
- Conclusion

Hacking et Sécurité, Expert : Metasploit

Maîtrisez Metasploit, le framework ultra-puissant, indispensable à tout "white hacker".

Une formation Alphorm.com Durée : 5h29min

Public concerné :
Pentesteur, Consultant en sécurité informatique, Responsables sécurité informatique, Toute personne en charge de la sécurité informatique.

Description :
A la suite de cette formation Hacking et Sécurité Expert, Metasploit, vous serez capable de bien comprendre les différents composants de Metasploit, pouvoir effectuer des tests de pénétration complets en exploitant la puissance de ce Framework, coder des modules, coder des scripts post exploitation, comprendre la notion de développement d'exploit, le débogage et le fuzzing, effectuer des attaques avancées et bien d'autres surprises.

Prérequis :
• Avoir suivi la formation Hacking et Sécurité, l'essentiel, formation Hacking & Sécurité, Avancé et la formation Hacking et Sécurité Expert - Réseaux sans fils,
• Culture dans la sécurité des SI,
• Connaissances de base sur les réseaux informatiques.

Objectifs :
• Test de pénétration via Metasploit,
• Comprendre l'architecture Metasploit,
• Comprendre les modules Metasploit,
• Notion et développement d'exploits,
• Attaquer au niveau de plusieurs couches,
• Approfondir ses connaissances en pentesting,
• Mise en situations réelles de hacking via Metasploit.

Programme détaillé :
voir page suivante

Hacking et Sécurité, Expert : Metasploit

Maîtrisez Metasploit, le framework ultra-puissant, indispensable à tout "white hacker".

Une formation Alphorm.com Durée : 5h29min

Programme détaillé >>>

- Présentation de la formation
- Introduction à Metasploit
- Coding sous Metasploit
- Développement d'exploits sous Metasploit
- Importation d'exploits
- Attaques avancées
- SET : Social Engennering toolkit
- Conclusion

Hacking et Sécurité, Expert : Réseaux sans Fil

Protégez vos réseaux sans fil en détectant et en corrigeant leurs vulnérabilités.

Une formation Alphorm.com Durée : 5h03min

Public concerné :
Futur Hacker éthique, Administrateurs réseaux, Responsables sécurité SI, Toute personne en charge de la sécurité, Particulier : Vous disposez d'un réseau WiFi ? Sécurisez-le !

Description :
A la suite de cette formation Hacking et Sécurité WiFi, vous serez capable de prévoir une surface d'attaque, suivre et structurer une méthodologie d'attaque des réseaux sans fils, attaquer les réseaux sans fils de différentes manières et enfin pouvoir sécuriser vos réseaux wifi et effectuer du reporting pour ainsi faire une bonne remonté de l'information.

Prérequis :
• Avoir suivi la formation Hacking et Sécurité, l'essentiel et la formation Hacking & Sécurité, Avancé,
• Culture dans la sécurité des SI,
• Connaissances de base Réseaux informatiques,
• Connaissances de base Réseaux Sans Fils.

Objectifs :
• Comprendre la sécurité Wifi,
• Comprendre les vulnérabilités au niveau des réseaux WiFI,
• Sécuriser son WiFI personnel et d'entreprise,
• Effectuer des rapports relatifs à des tests de pénétration de réseaux sans fils.

Programme détaillé :
voir page suivante

Hacking et Sécurité, Expert : Réseaux sans Fil

Protégez vos réseaux sans fil en détectant et en corrigeant leurs vulnérabilités.

Une formation Alphorm.com Durée : 5h03min

Programme détaillé >>>

- Présentation de la formation
- Préparation du Lab
- Introduction à la sécurité des réseaux sans fils
- Bypasser l'authentification
- Vulnérabilités chiffrement WLAN
- Attaquer l'infrastructure
- Attaquer le Client
- Attaques avancées
- Attaquer WPA-Entreprise et Radius
- WPS & Probes
- Méthodologie
- Conclusion

Citrix Netscaler 11 : Acquérir les fondamentaux

Apprenez les bonnes pratiques pour intégrer Netscaler 11 dans Citrix XenDesktop et XenApp.

Une formation Alphorm.com Durée : 7h29min

Public concerné :
Utilisateurs de NetScaler Gateway pour les accès à distance, Toute personne intéressée par l'intégration de NetScaler Gateway avec Citrix XenApp et Citrix XenDesktop, Candidats préparant à l'examen (1Y0-253).

Description :
Durant cette formation Citrix Netscaler 11, Fabrice SFORZA vous accompagnera depuis les concepts de base de Citrix Netscaler 11, sa terminologie et son architecture, jusqu'à sa surveillance et son dépannage.
Aussi pendant cette formation Citrix Netscaler 11, vous allez apprendre comment faire une répartition de charge optimale, performante et surtout sécurisée via votre appliance Citrix Netscaler 11.

Prérequis :
• Connaissances de base des concepts réseaux (routage, switch, VLAN, fonctionnalité des firewalls),
• Avoir des connaissances sur Windows Server 2012 R2, 2008, sur SQL Server, sur Active Directory et les stratégies de groupe, sur RDS (Remote Desktop Services) 2008/RDS 2012.

Objectifs :
• Comprendre les concepts de base et l'architecture du Citrix Netscaler 11,
• Intégrer Citrix Netscaler 11 avec Unified Gateway,
• Mettre en place les stratégies d'accès de Citrix Netscaler 11,
• Intégrer Citrix Netscaler 11 avec Citrix XenApp et Citrix XenDesktop,
• Préparer à l'examen (1Y0-253).

Programme détaillé :
voir page suivante

Citrix Netscaler 11 : Acquérir les fondamentaux

Apprenez les bonnes pratiques pour intégrer Netscaler 11 dans Citrix XenDesktop et XenApp.

Une formation Alphorm.com | Durée : 7h29min

Programme détaillé >>>

- Présentation de la formation
- Les bases
- La haute disponibilité
- Intégrer Netscaler avec Unified Gateway
- La gestion de charge
- SSL et sécurité
- Les systèmes d'authentification et autorisation
- Les stratégies d'accès
- Accès au NetScaler
- Connexion avec Xenapp et XenDesktop
- Admin et monitoring
- Conclusion

Fortinet UTM (1/2): Acquérir les fondamentaux

Maîtrisez le pare-feu Fortinet Fortigate UTM pour mieux protéger votre réseau, et préparez votre certification NSE4.

Une formation Alphorm.com Durée : 10h53min

Public concerné :
Toute personne responsable de la gestion quotidienne de l'appliance Fortigate UTM.

Prérequis :
• Expérience en TCP/IP et une compréhension basique des concepts firewall.

Description :
Durant cette formation Fortinet Fortigate UTM, vous allez vous familiariser avec les fonctionnalités Fortigate UTM de base. Dans les exercices interactifs, nous découvrirons : les règles de sécurité, les VPN, la détection des menaces, le filtrage web, le contrôle applicatif, l'authentification utilisateurs, et plus encore.
Ces fondamentaux vous fourniront une solide compréhension de comment intégrer la solution de sécurité du réseau Fortigate UTM, et par la suite, avec la formation Fortinet Fortigate UTM (NSE4) : Les fonctionnalités avancées vous apprendrez d'autres techniques plus performantes.

Objectifs :
• Décrire les fonctionnalités de l'UTM Fortigate,
• Accéder de manière sécurisée au réseau grâce au VPN SSL de Fortigate UTM,
• Établir un tunnel VPN IPSec sécurisé entre deux boitiers Fortigate UTM,
• Comparer les VPN IPSec tunnel-based vs. Interface-based,
• Appliquer la redirection de port, NAT source et destination,
• Interpréter des entrées de journal,
• Préparation à la certification NSE4.

Programme détaillé :
voir page suivante

Fortinet UTM (1/2): Acquérir les fondamentaux

Maîtrisez le pare-feu Fortinet Fortigate UTM pour mieux protéger votre réseau, et préparez votre certification NSE4.

Une formation Alphorm.com Durée : 10h53min

Programme détaillé >>>

- Présentation de la formation
- Introduction à l'UTM Fortigate
- Journalisation et surveillance
- Le Pare-feu
- Proxy Explicite
- Authentification Proxy
- VPN SSL
- VPN IPSec
- l'UTM
- Conclusion

Sophos UTM (1/2) : Acquérir les fondamentaux

Apprenez à administrer Sophos UTM 9.x pour assurer une protection complète et préparer votre certification SCE/SCA.

Une formation Alphorm.com Durée : 9h17min

Public concerné :
Partenaires/Clients Sophos pour passer la Certification SCE/SCA, Administrateurs et Techniciens Réseaux, Ingénieurs Sécurité des réseaux et systèmes.

Description :
Au début de cette formation Sophos UTM 9, le formateur vous montrera comment monter un Lab Sophos UTM 9 très complet pour faire toutes vos manipulations.
A l'issue de cette formation Sophos UTM 9, vous allez être capable d'implémenter les fonctionnalités du Sophos UTM dans sa version 9.3, et de le configurer suivant votre besoin interne dans votre entreprise, ou pour vos clients.

Prérequis :
• Avoir un bon niveau en réseau informatique et protocole TCP/IP,
• Des connaissances sur les pare-feu de nouvelle génération, UTM et Anti-virus,
• Des notions en Hardware et virtualisation.

Objectifs :
• Comprendre le fonctionnement des UTM,
• Se familiariser avec les produits Sophos,
• Déployer Sophos UTM, l'installer et le configurer,
• Comprendre et Configurer les différents services et fonctionnalités (Interface, Réseaux, DNS, DHCP, QoS, …),
• Administrer Sophos UTM.

Programme détaillé :
voir page suivante

Sophos UTM (1/2) : Acquérir les fondamentaux

Apprenez à administrer Sophos UTM 9.x pour assurer une protection complète et préparer votre certification SCE/SCA.

Une formation Alphorm.com Durée : 9h17min

Programme détaillé >>>

- Introduction à la formation
- Les fondamentaux
- Installation et vue d'ensemble
- Configuration du système
- Définition des objets
- Interfaces et Routage
- Authentification
- Services réseau
- Protection des réseaux
- Conclusion

Hacking et Sécurité : Maîtriser les techniques avancées

Tout savoir sur les techniques, les pratiques et les méthodologies utilisées par les hackers dans le cadre d'intrusions dans les réseaux et les applications.

Une formation Alphorm.com Durée : 11h04min

Public concerné :
Responsable sécurité SI, Consultants en sécurité, Ingénieurs et Techniciens, Administrateurs systèmes et réseaux, Développeurs.

Description :
Dans cette formation Hacking & Sécurité - Avancé nous mettons l'accent sur la compréhension technique et pratique des différentes formes d'attaques existantes, en s'attardant sur les vulnérabilités les plus critiques : le Social engineering, le Déni de service, le Fuzzing, les Botnets, Attaques Server-Side, Le Brute Force, Le cracking de mot de passe, Attaques Client-Side, MiTM Proxy, Elévation de privilège, Attaques Web, Attaques sur les réseaux sans fil, Bypassing HSSI, Bypassing MAC adress Authentication, Attaque WEP, Attaque WPA et WPA2, Clonage de points d'accès, L'attaque DoS.

Prérequis :
• Avoir suivi la première formation sur L'essentiel du Hacking & Sécurité,
• Bonnes connaissances de Linux en ligne de commande,
• Connaissances (de base) Réseaux Sans Fils,
• Connaissances Réseaux informatiques,
• Connaissances Développement Web.

Objectifs :
• Tester la sécurité de votre réseau/application,
• Comprendre et détecter les attaques sur un SI,
• Exploitation et portée d'une vulnérabilité,
• Corriger les vulnérabilités,
• Sécuriser un réseau/application,
• Appliquer des mesures pour lutter contre le hacking.

Programme détaillé :
voir page suivante

Hacking et Sécurité : Maîtriser les techniques avancées

Tout savoir sur les techniques, les pratiques et les méthodologies utilisées par les hackers dans le cadre d'intrusions dans les réseaux et les applications.

Une formation Alphorm.com Durée : 11h04min

Programme détaillé >>>

- Présentation de la formation
- Test de pénétration
- Mise en place du Lab
- Identification
- Social engineering
- Dénis de service
- Attaques Server-Side
- Attaques Client-Side
- Attaques Web
- Attaques sur les réseaux sans fils
- Reporting
- Contre-mesures
- Conclusion

Hacking et Sécurité : Acquérir les fondamentaux

Apprendre les techniques pratiques de base utilisées par un Hacker.

Une formation Alphorm.com Durée : 7h20min

Public concerné :
Administrateurs systèmes / réseaux, Techniciens, Responsables DSI, Responsables sécurité SI, Chefs de projets, Développeurs, Toute personne en charge de la sécurité, Toute personne désirant apprendre de nouvelles choses.

Description :
La présentation des techniques d'attaques et des vulnérabilités potentielles sera effectuée sous un angle "pratique", au sein d'un lab de test de pénétration.
Cette formation vous apportera la compréhension technique et pratique des différentes formes d'attaques existantes, en mettant l'accent sur les vulnérabilités les plus critiques.
Il s'agit d'une formation d'initiation, qui permet d'accéder ensuite à nos autres formations sur le Hacking et Sécurité.

Prérequis :
• Culture dans la sécurité des SI,
• Connaissances de base en Réseaux informatiques,
• Connaissances de base en Développement Web,
• Connaissances de base en Développement Applications.

Objectifs :
• Tester la sécurité de votre réseau / application,
• Comprendre les principaux scénarios d'attaques et savoir les détecter,
• Corriger les vulnérabilités, sécuriser votre réseau/application et mettre en place des mesures de prévention.

Programme détaillé :
voir page suivante

Hacking et Sécurité : Acquérir les fondamentaux

Apprendre les techniques pratiques de base utilisées par un Hacker.

Une formation Alphorm.com Durée : 7h20min

Programme détaillé >>>

- Présentation de la formation
- Introduction à la sécurité informatique
- Préparation Lab
- Prise d'informations
- Vulnérabilités postes clients
- Vulnérabilités Web
- Vulnérabilités Réseau
- Vulnérabilités applicatives
- Contremesures
- Conclusion

Active Directory Certificate Services 2012 R2 : Maîtriser le PKI

Mettez en œuvre et gérez une infrastructure PKI avec ADCS 2012 R2.

Une formation Alphorm.com Durée : 11h21min

Public concerné :
Techniciens de support Administrateurs, Ingénieurs systèmes, Architecture informatique, Spécialiste en sécurité, Spécialiste en PKI d'entreprise, Passage des certifications Microsoft (70-412).

Description :
Cette formation Le PKI avec ADCS 2012 R2 vous propose une découverte opérationnelle des PKI, à la fois panorama des solutions disponibles sur le marché, apprentissage des fondamentaux théoriques et mise en pratique sur la solution du marché la plus universelle.

Prérequis :
• Connaissances de base sur la gestion des systèmes d'exploitation Windows,
• Connaissances de base sur les réseaux,
• Connaissances sur l'Active Directory,
• Pas de prérequis sur la cryptographie (couvert par la session).

Objectifs :
• Connaître les éléments structurant une PKI,
• Déployer une solution de PKI d'entreprise,
• Installer, publier des certificats automatiquement,
• Sauvegarder/Récupérer des certificats émis,
• Configurer un serveur Web en HTTPS.

Programme détaillé :
voir page suivante

Active Directory Certificate Services 2012 R2 : Maîtriser le PKI

Mettez en œuvre et gérez une infrastructure PKI avec ADCS 2012 R2.

Une formation Alphorm.com Durée : 11h21min

Programme détaillé >>>

- Présentation de la formation
- Cryptographie
- Autorité de certification Entreprise
- Inscription de certificats
- Sites Web sécurisés
- Révocation de certificats
- Sécurisation d'une infrastructure de clé publiques
- Autres rôles Pki
- Conclusion

hak5 : WiFi Pineapple

Découvrez le hacking hardware avec le module WiFi Pineapple du puissant pack hak5

Une formation Alphorm.com Durée : 2h33min

Public concerné :
Consultants sécurité informatique, Pentesteurs, Administrateurs, Ingénieurs réseaux/systèmes, Ingénieurs sécurité informatique, Passionnées en cybersécurité

Description :
Cette formation Pentest Hardware : Wifi Pineapple englobe une analyse et compréhension des attaques ainsi qu'une structuration des connaissances avant de passer aux attaques qui sont axées pratiques à 100 %, et vise à vous donner la capacité d'effectuer des tests de pénétration sur les réseaux sans fils de manière complète à l'aide du WiFi Pineapple.

Prérequis :
• Avoir suivis la formation Hacking et Sécurité l'essentiel et les techniques avancées
• Avoir suivis la formation Hacking et Sécurité, Expert : Les réseaux sans fils

Objectifs :
• Découverte du WiFi Pineapple
• Maîtrise des modules WiFi Pineapple
• Déploiement de modules WiFi Pineapple
• Effectuer des pentests avec le WiFi Pineapple

Programme détaillé :
voir page suivante

hak5 : WiFi Pineapple

Découvrez le hacking hardware avec le module WiFi Pineapple du puissant pack hak5

Une formation Alphorm.com Durée : 2h33min

Programme détaillé >>>

- Présentation de la formation
- Mise en place et configuration
- Rappels
- Modules
- Conclusion et perspectives