Systeem- en netwerkbeveiliging, niveau 1

Praktijkcursus van 4 dagen - 28u
Ref : FRW - Prijs 2024 : € 2 990 excl. BTW

In deze praktische opleiding leert u hoe u de belangrijkste beveiligingsmiddelen voor systemen en netwerken kunt toepassen. Na bestudering van enkele bedreigingen van het informatiesysteem leert u wat de rol is van de verschillende beveiligingssystemen voor de bescherming van het bedrijf, zodat u in staat zult zijn een beveiligingsarchitectuur te ontwerpen en uit te voeren.

PEDAGOGISCHE DOELSTELLINGEN

Na afloop van de opleiding kan de cursist:

Kennis van de zwakke plekken en bedreigingen van informatiesystemen

Beheersing van de rol van de verschillende veiligheidsuitrustingen

Een passende beveiligingsarchitectuur ontwerpen en implementeren

Implementeren van de belangrijkste netwerkbeveiligingsmiddelen

Beveiliging van een Windows- en Linux-systeem

HANDS-ON WORK

Implementatie van een HTTP proxy-oplossing onder Windows of Linux, van een antivirusoplossing op de netwerkstromen. Ontwerp en implementatie van een multi-firewall, multi-DMZ architectuur. Toepassing van de basistechnieken voor de beveiliging van het besturingssysteem.

HET PROGRAMMA

laatste update: 10/2021

1) Risico's en bedreigingen

- Inleiding tot beveiliging.
- Stand van zaken van IT-beveiliging.
- Vocabularium van IT-beveiliging.
- Aanvallen op de "onderste lagen".
- Sterke en zwakke punten van het TCP/IP-protocol.
- Illustratie van aanvallen van het type ARP en IP Spoofing, TCP-SYNflood, SMURF enz.
- Denial of service en distributed denial of service.
- Applicatie-aanvallen.
- Intelligence gathering.
- HTTP, een bijzonder kwetsbaar protocol (SQL injection, Cross Site Scripting enz.).
- DNS: Dan Kaminsky-aanval.

Installatie en gebruik van de Wireshark netwerk analyzer. Uitvoering van een applicatie-aanval.

2) Beveiligingsarchitecturen

- Welke architecturen voor welke behoeften?
- Beveiligd adresseringsplan: RFC 1918.
- Adresvertaling (FTP als voorbeeld).
- De rol van gedemilitariseerde zones (DMZ's).
- Voorbeelden van architecturen.
- Beveiliging van de architectuur door virtualisatie.
- Firewall: hoeksteen van de beveiliging.
- Werking en beperkingen van traditionele netwerk-firewalls.

DEELNEMERS

Beveiligingsverantwoordelijken, -architecten. Systeem- en netwerkbeheerders en -technici.

VOORAFGAANDE VEREISTEN

Goede kennis van netwerken en systemen.

VAARDIGHEDEN VAN DE CURSUSLEIDER

De deskundigen die de cursus leiden zijn specialisten op het betreffende vakgebied. Zij werden geselecteerd door onze pedagogische teams zowel om hun vakkennis als hun pedagogische vaardigheden voor elke cursus die zij geven. Zij hebben minstens vijf tot tien jaar ervaring in hun vakgebied en oefenen of oefenden verantwoordelijke bedrijfsfuncties uit.

BEOORDELINGSMODALITEITEN

De cursusleider beoordeelt de pedagogische vooruitgang van de deelnemer gedurende de gehele cursus aan de hand van meerkeuzevragen, praktijksituaties, praktische opdrachten, …
De deelnemer legt ook van tevoren en naderhand een test af ter bevestiging van de verworven kennis.

PEDAGOGISCHE EN TECHNISCHE MIDDELEN

• De gebruikte pedagogische middelen en cursusmethoden zijn voornamelijk: audiovisuele hulpmiddelen, documentatie en cursusmateriaal, praktische oefeningen en correcties van de oefeningen voor praktijkstages, casestudies of reële voorbeelden voor de seminars.
• Na afloop van de stages of seminars verstrekt ORSYS de deelnemers een evaluatievragenlijst over de cursus die vervolgens door onze pedagogische teams wordt geanalyseerd.
• Na afloop van de cursus wordt een presentielijst per halve dag verstrekt, evenals een verklaring van de afronding van de cursus indien de stagiair alle sessies heeft bijgewoond.

TOEGANGSMODALITEITEN EN -TERMIJNEN

De inschrijving dient 24 uur voor aanvang van de cursus plaatsgevonden te hebben.

TOEGANKELIJKHEID VOOR MINDERVALIDEN

Is voor u speciale toegankelijkheid vereist? Neem contact op met mevr. FOSSE, contactpersoon voor mindervaliden, via het adres psh-accueil@ORSYS.fr om uw verzoek en de haalbaarheid daarvan zo goed mogelijk te bestuderen.

- Technologische evolutie van firewalls (Appliance, VPN, IPS, UTM...).
- Firewalls en virtuele omgevingen.
- Proxy server en applicatie relay.
- Proxy of firewall: concurrenten of complementair?
- Reverse proxy, content filtering, caching en authenticatie.
- SMTP-relay, een verplichting?

Toepassing van een Cache/Authenticatie proxy.

3) Gegevensbeveiliging.

- Cryptografie.
- Symmetrische en asymmetrische versleutelingen. Hash-functies.
- Cryptografische diensten.
- Authenticatie van de gebruiker.
- Het belang van wederzijdse authenticatie.
- X509-certificaten. Elektronische handtekening. Radius. LDAP.
- Wormen, virussen, Trojaanse paarden, malware en keyloggers.
- Huidige trends. Het antivirusaanbod, de complementariteit van de elementen. EICAR, een "virus" dat u moet kennen.

Toepassing van een SMTP relay en een HTTP/FTP Antivirus proxy. Toepassing van een servercertificaat.

4) Beveiliging van de uitwisselingen

- WiFi-beveiliging.
- Risico's die inherent zijn aan draadloze netwerken.
- De beperkingen van WEP. Het WPA- en WPA2-protocol.
- De soorten aanvallen.
- Man in the Middle-aanval met de scareware AP.
- Het IPSec-protocol.
- Presentatie van het protocol.
- Tunnel- en transportmodi. ESP en AH.
- Analyse van het protocol en de bijbehorende technologieën (SA, IKE, ISAKMP, ESP, AH...).
- SSL-/TLS-protocollen.
- Presentatie van het protocol. Details van de onderhandeling.
- Analyse van de belangrijkste kwetsbare plekken.
- Sslstrip- en sslsnif-aanvallen.
- Het SSH-protocol. Presentatie en functies.
- Verschillen met SSL.

Uitvoering van een Man in the Middle-aanval op een SSL-sessie. Toepassing van IPSec transport/PSK-modus.

5) Een systeem beveiligen, "Hardening"

- Presentatie.
- Ontoereikendheid van de standaardinstallaties.
- Evaluatiecriteria (TCSEC, ITSEC en gemeenschappelijke criteria).
- Beveiliging van Windows.
- Beheer van accounts en autorisaties.
- Controle van de diensten.
- Netwerk- en auditconfiguratie.
- Beveiliging van Linux.
- Kernelconfiguratie.
- Bestandssysteem.
- Service- en netwerkbeheer.

Voorbeeld van de beveiliging van een Windows- en Linux-systeem.

6) Audit en beveiliging in de dagelijkse praktijk

- De beschikbare instrumenten en technieken.

- Inbraaktests: instrumenten en middelen.
- Detectie van kwetsbare plekken (scanners, IDS-sondes enz.).
- Tools voor realtime opsporing IDS-IPS, agent, sonde of onderbreking.
- In alle omstandigheden doeltreffend reageren.
- Toezicht en administratie.
- Organisatorische gevolgen.
- Technologische monitoring.

7) Casestudy

- Voorafgaande studie.
- Behoefteanalyse
- Een architectuur uitwerken.
- Het actieplan bepalen.
- Toepassing.
- Procedure voor het installeren van de elementen.
- Toepassing van het filterbeleid.

Uitwerking van een flow control.

DATA

KLAS OP AFSTAND
2024 : 10 sep, 19 nov

BRUSSEL
2024 : 10 sep, 19 nov