Publicatiedatum : 24/01/2024

Opleiding : Systeem- en netwerkbeveiliging, niveau 2

Praktijkcursus - 4d - 28u00 - Ref. SEA
Prijs : 2460 € V.B.

4,1 / 5

BEST

Deze geavanceerde cursus stelt u in staat om het beveiligingsniveau van uw informatiesysteem te meten met behulp van intrusion detection, vulnerability detection en audit tools, etc. De cursus biedt u kennis van geavanceerde oplossingen om het gewenste beveiligingsniveau in de loop van de tijd te handhaven en te upgraden, in overeenstemming met uw behoeften.

Pedagogische doelstellingen

Aan het einde van de training is de deelnemer in staat om:

- Het beveiligingsniveau van informatiesystemen meten
- Tools voor inbraakdetectie, detectie van kwetsbaarheden en auditing gebruiken
- De beveiliging van informatiesystemen versterken
- Begrijpen hoe AAA (Authentication, Authorisation, Accounting) architectuur werkt
- SSL/TLS implementeren

Doelgroep

Beveiligingsmanagers en -architecten. Systeem- en netwerktechnici en -beheerders.

Voorafgaande vereisten

Goede kennis van TCP/IP en beveiliging van bedrijfsnetwerken. Of kennis die gelijkwaardig is aan die van de cursus "Systeem- en netwerkbeveiliging, niveau 1" (ref. FRW).

Praktische modaliteiten

Praktisch werk

Een breed scala aan tools zal worden ingezet door de deelnemers. SNORT IDS probe, kwetsbaarheden scannen met NESSUS, netwerkanalyse en scannen met ETHEREAL en NMAP. Beveiligen van een Wi-Fi netwerk.

Opleidingsprogramma

DEELNEMERS

Beveiligingsmanagers en -architecten. Systeem- en netwerktechnici en -beheerders.

VOORAFGAANDE VEREISTEN

Goede kennis van TCP/IP en beveiliging van bedrijfsnetwerken. Of kennis die gelijkwaardig is aan die van de cursus "Systeem- en netwerkbeveiliging, niveau 1" (ref. FRW).

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.

1 Herinneringen

- Het TCP/IP-protocol.
- Adresvertaling.
- Netwerkarchitectuur.
- De firewall: voordelen en beperkingen.
- Proxy's, reverse-proxy's: bescherming van toepassingen.
- Gedemilitariseerde zones (DMZ's).

2 Aanvalsgereedschappen

- Beveiligingsparadigma's en classificatie van aanvallen.
- Aanvalsprincipes: spoofing, flooding, injectie, capture, enz.
- Bibliotheken : Libnet, Libpcap, Winpcap, Libbpf, Nasl, lua.
- Gereedschappen: Scapy, Hping, Ettercap, Metasploit, Dsnif, Arpspoof, Smurf.

Praktisch werk

Protocolanalyse met Wireshark. Gebruik van Scapy en Arpspoof.

3 Cryptografie, toepassing

- De veiligheidsdiensten.
- Cryptografische principes en algoritmen (DES, 3DES, AES, RC4, RSA, DSA, ECC).
- Certificaten en specifieke profielen voor verschillende servers en clients (X509).
- IPSEC-protocol en virtuele privénetwerken (VPN).
- SSL/TLS en VPN-SSL protocollen. Problemen met gegevenscompressie.

Praktisch werk

Grip krijgen op openssl en implementeren van OpenPGP. Genereren van X509 v3 certificaten.

4 AAA-architectuur (Authenticatie, Autorisatie, Accounting)

- Het AAA-netwerk: authenticatie, autorisatie en traceerbaarheid.
- Eenmalig wachtwoord: OTP, HOTP, Google Authentificator, SSO (Kerberos-protocol).
- De plaats van de LDAP-directory in verificatieoplossingen.
- De modules PAM en SASL.
- Architectuur en Radius-protocol (Authenticatie, Autorisatie, Accounting).
- Mogelijke aanvallen.
- Hoe kan ik mezelf beschermen?

Praktisch werk

Aanval op een AAA-server.

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.

5 Indringers detecteren

- Werkingsprincipes en detectiemethoden.
- Marktspelers, overzicht van de betrokken systemen en toepassingen.
- Scanners voor netwerken (Nmap) en toepassingen (webtoepassingen).
- IDS (Intrusion Detection System).
- De voordelen en beperkingen van deze technologieën.
- Hoe moeten ze worden gepositioneerd in de bedrijfsarchitectuur?
- Marktoverzicht, gedetailleerde studie van SNORT.

Praktisch werk

Installatie, configuratie en implementatie van SNORT, schrijven van aanvalshandtekeningen.

6 De integriteit van een systeem controleren

- Werkingsprincipes.
- Welke producten zijn beschikbaar?
- Presentatie van Tripwire of AIDE (Advanced Intrusion Detection Environment).
- Kwetsbaarheidsaudits.
- Principes, methoden en organisaties voor kwetsbaarheidsmanagement.
- Referentiesite en overzicht van audittools.
- Definitie van een beveiligingsbeleid.
- Studie en implementatie van Nessus (status, werking, ontwikkeling).

Praktisch werk

Controle van netwerk- en serverkwetsbaarheden met Nessus en Nmap.
Controle op kwetsbaarheden van websites.

7 Beveiligingsgebeurtenissen beheren

- Informatie verwerken die wordt gerapporteerd door de verschillende veiligheidsvoorzieningen.
- Consolidatie en correlatie.
- Presentatie van SIM (Security Information Management).
- SNMP beheer en protocol: sterke en zwakke punten in beveiliging.
- SNMP beveiligingsoplossing.

Praktisch werk

SNMP-aanval instellen.

8 WiFi-netwerkbeveiliging

- Hoe beveiligt u een WiFi-netwerk?
- De intrinsieke zwakheden van WiFi-netwerken.
- SSID Broadcast, MAC Filtering, wat heb u eraan?
- Heeft WEP nog zin?
- Het WPA-protocol, de eerste aanvaardbare oplossing.
- Is de WPA-implementatie in gedeelde sleutelmodus voldoende?
- WPA, Radius en AAA-server, bedrijfsimplementatie.
- 802.11i en WPA2: welke oplossing is vandaag de dag het meest succesvol?
- Verkeersinjectie, WiFi-sleutels kraken.

Praktisch werk

Configureren van tools voor het vastleggen van verkeer, scannen van netwerken en analyseren van WIFI-verkeer. Configuratie van een AP (Access Point) en implementatie van beveiligingsoplossingen.

9 De beveiliging van IP-telefonie

- Voice over IP-concepten. Overzicht van toepassingen.
- De architectuur van een VoIP-systeem.
- Het SIP-protocol, een open standaard voor spraak over IP.
- De zwakke punten van het SIP-protocol.
- NAT-problemen.
- Aanvallen op IP-telefonie.
- Wat zijn de beveiligingsoplossingen?

10 E-mailbeveiliging

- Architectuur en werking van berichtenverkeer.
- E-mailprotocollen en -toegang (POP, IMAP, Webmail, SMTP, enz.).
- Problemen en classificaties van e-mailaanvallen (spam, fishing, identiteitsdiefstal, enz.).
- Spelers in de strijd tegen SPAM.
- Methoden, architecturen en hulpmiddelen voor het bestrijden van SPAM.
- Hulpmiddelen voor het verzamelen van e-mailadressen.
- Oplossingen geïmplementeerd om SPAM tegen te gaan.

Data en plaats

KLAS OP AFSTAND
2026 : 7 apr., 14 apr., 16 juni, 16 juni, 18 aug., 18 aug., 22 sep., 27 okt., 1 dec., 15 dec., 15 dec.

PARIS LA DÉFENSE
2026 : 14 apr., 16 juni, 18 aug., 27 okt., 15 dec.

LILLE
2026 : 16 juni, 15 dec.