Systeem- en netwerkbeveiliging, niveau 2

Praktijkcursus van 4 dagen - 28u
Ref : SEA - Prijs 2024 : € 2 860 excl. BTW

Tijdens deze gevorderde stage kunt u het beveiligingsniveau van uw informatiesysteem meten met behulp van tools voor indringingsdetectie, detectie van kwetsbaarheden, audit... De stage biedt u kennis in geavanceerde oplossingen om het gewenste veiligheidsniveau te handhaven en met de tijd te laten ontwikkelen naargelang uw behoeften.

PEDAGOGISCHE DOELSTELLINGEN

Na afloop van de opleiding kan de cursist:

Het veiligheidsniveau van het informatiesysteem meten

Hulpmiddelen gebruiken voor indringingsdetectie, detectie van kwetsbaarheden en audit

Verbetering van de beveiliging van het informatiesysteem

De werking van een AAA-architectuur kennen (Authentication, Autorization, Accounting)

Implementatie van SSL/TLS

HANDS-ON WORK

Er zullen talrijke tools gebruikt worden door de deelnemers. IDS SNORT sonde, kwetsbaarheidsscan met NESSUS, analyse en scan van netwerken met ETHEREAL en NMAP. Beveiliging van een wifi-netwerk.

HET PROGRAMMA

laatste update: 04/2022

1) Herinneringen

- Het TCP/IP protocol.
- De translatie van adressen.
- De architectuur van de netwerken.
- Firewall: voordelen en beperkingen.
- Proxys, reverse-proxy: applicatiebescherming.
- Gedemilitariseerde zones (DMZ).

2) Aanvalstools

- Veiligheidsparadigma's en classificatie van aanvallen.
- Principes van aanvallen: spoofing, flooding, injectie, capture, enz.
- Librairies: Libnet, Libpcap, Winpcap, Libbpf, Nasl, lua.
- Tools: Scapy, Hping, Ettercap, Metasploit, Dsnif, Arpspoof, Smurf.

Protocolanalyse met Wireshark. Gebruik van Scapy en Arpspoof.

3) Cryptografie, toepassing

- De veiligheidsdiensten.
- Cryptografische principes en algoritmen (DES, 3DES, AES, RC4, RSA, DSA, ECC).
- Specifieke certificaten en profielen voor de diverse servers en klanten (X509).
- IPSEC protocol en virtuele private netwerken (VPN).
- SSL/TLS en VPN-SSL protocollen. Problemen met gegevenscompressie.

Gebruik van Openssl en implementatie van OpenPGP. Genereren van X509 v3 certificaten.

DEELNEMERS

Managers, programmeurs van veiligheidssystemen. Technici en beheerders van systemen en netwerken.

VOORAFGAANDE VEREISTEN

Goede kennis van TCP/IP en beveiliging van bedrijfsnetwerken. Of kennis gelijkwaardig aan die van de stage "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.

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.

4) AAA-architectuur (Authentication, Autorization, Accounting)

- Het AAA-netwerk: authenticatie, autorisatie en traceerbaarheid.
- One Time Password: OTP, HOTP, Google Authentificator, SSO (Kerberos Protocol).
- De plaats van LDAP in authenticatieoplossingen.
- De modules PAM en SASL.
- Architectuur en protocol Radius (Authentication, Autorization, Accounting).
- Mogelijke aanvallen.
- Hoe kunnen we ons beschermen?

Aanval op een AAA-server.

5) Indringing detecteren

- Werkingsprincipes en detectiemethoden.
- Marktspelers, overzicht van de betrokken systemen en applicaties.
- Netwerkscanners (Nmap) en applicatiescanners (Web applications).
- IDS (Intrusion Detection System).
- De voordelen en beperkingen van deze technologieën.
- Hoe plaatsen we ze in de architectuur van de onderneming?
- Marktoverzicht, gedetailleerde studie van SNORT.

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

6) De integriteit van een systeem controleren

- De werkingsprincipes.
- Welke producten zijn er beschikbaar?
- Presentatie van Tripwire of AIDE (Advanced Intrusion Detection Environment).
- Audit van kwetsbaarheden.
- Principes en methoden en organismen voor het beheer van kwetsbaarheden.
- Referentiesite en overzicht van de audittools.
- Opstellen van een veiligheidsbeleid.
- Bestudering en implementatie van Nessus (status, werking, ontwikkeling).

Audit van kwetsbaarheden van netwerken en servers met behulp van Nessus en Nmap.
Audit van kwetsbaarheden van een website.

7) Beheren van veiligheidsincidenten

- Verwerking van de informatie die door de verschillende veiligheidsvoorzieningen wordt doorgegeven.
- Consolidatie en correlatie.
- Presentatie van SIM (Security Information Management).
- SNMP-beheer en -protocol: sterke en zwakke veiligheidspunten.
- Beveiligingsoplossing van SNMP.

SNMP aanvalsmontage.

8) Beveiliging van wifi-netwerken

- Hoe kan een wifi-netwerk beveiligd worden?
- De intrinsieke zwakheden van wifi-netwerken.
- Welke bijdrage levert SSID Broadcast, MAC Filtering?
- Heeft het WEP nog belang?
- WPA-protocol, eerste aanvaardbare oplossing.
- Implementatie van WPA in gedeelde sleutelmodus, volstaat dat?
- WPA, Radius en AAA server, corporate implementatie.
- De normen 802.11i en WPA2, welke oplossing is tegenwoordig het meest succesvol?
- Injectie van verkeer, wifisleutels kraken.

Configuratie van de tools voor het vastleggen van verkeer, het scannen van netwerken en het analyseren van wifi-verkeer. Opzetten van een AP (Access Point) en implementeren van beveiligingsoplossingen.

9) Beveiliging van IP-telefonie

- De concepten van voice over IP. Presentatie van de applicaties.

- De architectuur van een VoIP-systeem.
- Het SIP-protocol, open standaard van voice over IP.
- Zwakke punten van het SIP-protocol.
- De problematiek van NAT.
- Aanvallen op IP-telefonie.
- Wat zijn de veiligheidsoplossingen?

10) De veiligheid van de mailbox

- Architectuur en werking van de mailbox.
- Protocollen en toegang tot e-mail (POP, IMAP, Webmail, SMTP, enz.).
- Problemen en classificatie van e-mailaanvallen (spam, fishing, identiteitsdiefstal, enz.).
- Spelers in de strijd tegen SPAM.
- Methoden, architectuur en tools om spam te bestrijden.
- Tools voor het verzamelen van e-mailadressen.
- De geïmplementeerde oplossingen tegen SPAM.

DATA

KLAS OP AFSTAND	BRUSSEL
2024 : 03 sep, 12 nov	2024 : 03 sep, 12 nov