Publicatiedatum : 30/01/2024

Opleiding : Detectie van hackers

Hoe kan men veiligheidsincidenten beheren

Praktijkcursus - 4d - 28u00 - Ref. INT

Prijs : 2520 € V.B.

3,9 / 5

Deze theoretische en praktische cursus toont de meest geavanceerde aanvalstechnieken tot nu toe en laat zien hoe men deze het hoofd kan bieden. Op basis van aanvallen uitgevoerd op geïdentificeerde doelwitten (webservers, clients, netwerken, firewall, databases...) leren de cursisten welke actie ondernomen moet worden starten (anti-trojan filtering, filtering van een slecht gevormde URL, spamdetectie en inbraakdetectie in real time met IDS-sonde).

Pedagogische doelstellingen

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

- Analyse- en detectietechnieken identificeren en begrijpen
- Kennis verwerven om verschillende tools voor inbraakdetectie uit te rollen
- Implementeren van oplossingen voor inbraakpreventie en -detectie
- Beheer van een inbraakincident
- Kennis over het juridische kader

Doelgroep

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

Voorafgaande vereisten

Goede kennis van TCP/IP netwerken. Basiskennis in cyberveiligheid.

Praktische modaliteiten

Praktisch werk

Beveiligde en "normaal" beschermde architecturen (firewall multi-DMZ, beveiligde applicaties) zijn het doelwit van de aanvallen.

Opleidingsprogramma

DEELNEMERS

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

VOORAFGAANDE VEREISTEN

Goede kennis van TCP/IP netwerken. Basiskennis in cyberveiligheid.

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 De wereld van de cyberveiligheid.

- “Officiële” definities: hacker, hacking.
- De gemeenschap van hackers over de hele wereld, de "goeroes", de "scriptkiddies".
- De mentaliteit en cultuur van de hacker.
- Conferenties en belangrijke beveiligingssites.

Praktisch werk

Underground Navigation. Nuttige informatie weten te vinden.

2 TCP/IP voor firewalls en inbraakdetectie

- IP, TCP en UDP vanuit een andere hoek.
- Focus op ARP en ICMP.
- Geforceerde routing van IP-pakketten (source routing).
- IP-fragmentatie en regels voor herassemblage.
- Het nut van een serieuze filtering.
- Uw servers beveiligen: een must.
- Parades per technologie: van filtrerende router tot firewall stateful inspection; van proxy tot reverse proxy.
- Snel overzicht van oplossingen en producten.

Praktisch werk

Visualisatie en analyse van klassiek verkeer. Gebruik van verschillende sniffers.

3 De aanvallen op TCP/IP begrijpen

- IP-spoofing.
- Denial of service aanvallen.
- Voorspelling van de TCP volgnummers.
- Diefstal van TCP sessie: Hijacking (Hunt, Juggernaut).
- Aanvallen op SNMP.
- Aanval door TCP Spoofing (Mitnick): demystificatie.

Praktisch werk

Injectie van op het netwerk geproduceerde pakketten. Gebruik naar keuze van de deelnemers van grafische tools, Perl, C of specifieke scripts. Hijacking van een telnet verbinding.

4 Intelligence Gathering: de kunst van het camoufleren

- Sporen zoeken: bevragen van Whois databases, DNS servers, zoekmotoren.
- Identificatie van de servers.
- Context begrijpen: resultaten analyseren, filterregels bepalen, specifieke gevallen.

Praktisch werk

Zoeken met behulp van niet-intrusieve technieken naar informatie over een potentiële doelgroep (naar keuze van de deelnemers). Gebruik van netwerkscans.

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 Bescherming van gegevens

- Wachtwoordsystemen: ongecodeerd, per challenge, versleuteld.
- Stand van zaken over authenticatie onder Windows.
- Info over SSH en SSL (HTTPS).
- Sniffing van een switched netwerk: ARP poisonning.
- Aanvallen op versleutelde gegevens: "Man in the Middle" op SSH en SSL, "Keystoke Analysis" op SSH.
- Sniffer detectie: geavanceerde tools en methoden.
- Aanvallen op wachtwoorden.

Praktisch werk

Decodering en diefstal van SSH-sessie: "Man in the Middle" aanval. Wachtwoorden doorbreken met LophtCrack (Windows) en John The Ripper (Unix).

6 Detectie van trojans en backdoors

- State of the art van backdoors onder Windows en Unix.
- Opzetten van backdoors en trojans.
- Het uploaden van scripts naar clients, het gebruik van bugs van browsers.
- De "Covert Channels": client-server applicatie die ICMP gebruikt.
- Voorbeeld van communicatie met gedistribueerde denial of service agenten.

Praktisch werk

Analyse van Loki, client-server die ICMP gebruikt. Toegang krijgen tot privé-informatie via uw browser.

7 Verdedigen van online diensten

- Overname van een server: zoeken en exploiteren van kwetsbaarheden.
- Voorbeelden van het plaatsen van "backdoors" en het verwijderen van sporen.
- Hoe omzeilen we een firewall (netcat en rebounds)?
- Het zoeken naar denial of service.
- Gedistribueerde denial of service (DDoS).
- Overflowaanvallen (buffer overflow).
- Gebruik van fouten in de broncode. Gelijkwaardige technieken: “Format String”, “Heap Overflow”.
- Kwetsbaarheden in webapplicaties.
- Diefstal van informatie uit een database.
- RootKits.

Praktisch werk

Exploitatie van de bug die gebruikt wordt door de worm "Code Red". Verkrijgen van een Shell root door verschillende soorten buffer overflow. Test van een denial of service (Jolt2, Ssping). Netcat gebruiken om een firewall te omzeilen. Gebruik van "SQL Injection" technieken om webauthenticatie te verbreken.

8 Hoe kan men een incident beheren?

- Tekenen van een succesvolle inbraak in een informatiesysteem.
- Wat hebben de hackers gekregen? Hoe ver zijn ze gegaan?
- Hoe te reageren op een geslaagde inbraak?
- Welke servers zijn betrokken?
- Het punt van binnenkomst kunnen terugvinden en het lek dichten.
- De Unix/Windows toolbox voor het zoeken naar bewijs.
- Schoonmaken en opnieuw in productie brengen van gecompromitteerde servers.

9 Conclusie: welk juridisch kader?

- Het juiste antwoord op hackers.
- De Franse wet inzake hacking.
- De rol van de overheid, de officiële instanties.
- Wat te verwachten van het Centraal Bureau voor Criminaliteitsbestrijding (OCLCTIC)?
- Het zoeken naar bewijs en daders.
- En in een internationale context?
- De indringingstest of domestic hacking?
- Binnen een wettelijk kader blijven, de dienstverlener kiezen, zeker zijn van het resultaat.

Data en plaats

KLAS OP AFSTAND
2026 : 21 apr., 19 mei, 29 sep., 6 okt., 1 dec., 8 dec.

PARIS LA DÉFENSE
2026 : 19 mei, 6 okt., 8 dec.