Hacking en veiligheid, niveau 1

Praktijkcursus van 5 dagen - 35u
Ref : HAC - Prijs 2024 : € 3 530 excl. BTW

Deze geavanceerde opleiding leert u de noodzakelijke technieken om het beveiligingsniveau van uw informatiesysteem te meten. Als gevolg van deze aanvallen leert u de juiste reactie te activeren en het beveiligingsniveau van uw netwerk te verhogen.

PEDAGOGISCHE DOELSTELLINGEN

Na afloop van de opleiding kan de cursist:

De technieken van hackers begrijpen en aanvallen kunnen tegengaan

Het beveiligingsniveau van uw informatiesysteem meten

Uitvoeren van een indringingstest

De impact en de omvang van een kwetsbaarheid definiëren

HET PROGRAMMA

laatste update: 04/2022

1) Hacking en beveiliging

- Vormen van aanvallen, werkwijzen, actoren, belangen.
- Audits en indringingstests, plaats in een SMSI.

2) Sniffing, onderschepping, analyse, netwerkinjectie

- Anatomie van een pakket, tcpdump, Wireshark, tshark.
- Verduistering en onderschepping van communicatie (Man-in-the-Middle, aanvallen van VLAN, honingpotten).
- Pakketten: Sniffing, lezen/analyseren vanuit een pcap, extractie van nuttige gegevens, grafische weergaven.
- Scapy: architectuur, capaciteiten, gebruik.

Luisteren naar het netwerk met sniffers. Een mini C-pakketonderschepper realiseren. Scapy gebruiken (command line, python script): injecties, onderschepping, pcap-lezen, scan, DoS, MitM.

3) Herkenning, scanning en opsomming

- Intelligence gathering, hot reading, darknet exploitatie, Social Engineering.
- Herkenning van service, systeem, topologie en architecturen.
- Soorten scans, filterdetectie, firewalking, fuzzing.
- Camouflage door usurpatie en rebound, identificatie van routes met traceroute, source routing.
- Ontsnapping van IDS en IPS: fragmentatie, covert channels.
- Nmap: scannen en exporteren van resultaten, de opties.
- De andere scanners: Nessus, OpenVAS.

Gebruik van de nmap-tool, schrijven van een NSE-script in LUA. Detectie van filtering.

4) Webaanvallen

- OWASP: organisatie, hoofdstukken, Top10, handleidingen, tools.
- Ontdekking van de infrastructuur en bijbehorende technologieën, sterke en zwakke punten.

DEELNEMERS

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

VOORAFGAANDE VEREISTEN

Goede kennis van IS-beveiliging, netwerken, systemen (met name Linux) en programmeren. Of gelijkwaardige kennis als 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.

- Klantzijde: clickjacking, CSRF, diefstal van cookies, XSS, componenten (flash, java). Nieuwe vectoren.
- Serverzijde: authenticatie, diefstal van sessies, injecties (SQL, LDAP, bestanden, commando's).
- Inclusie van lokale en externe bestanden, cryptografische aanvallen en vectoren.
- Ontwijking en omzeiling van beveiligingen: voorbeeld van de omzeilingstechnieken van WAF.
- Tools Burp Suite, ZAP, Sqlmap, BeEF.

Implementatie van verschillende webaanvallen in reële omstandigheden aan server- en klantenzijde.

5) Applicatie-aanvallen en aanvallen na exploitatie

- Aanval op Microsoft authenticaties, PassTheHash.
- Van C naar assembler naar machinecode. De shellcodes.
- Shellcodes coderen, NULL bytes verwijderen.
- De Rootkits. Procesexploitaties: Buffer Overflow, ROP, Dangling Pointers.
- Bescherming en omzeiling: Flag GS, ASLR, PIE, RELRO, Safe SEH, DEP. Shellcodes met hard gecodeerde adressen/LSD.
- Metasploit: architectuur, functies, interfaces, workspaces, exploit schrijven, Shellcodes genereren.

Metasploit: exploitatie, gebruik van de databank. Msfvenom: genereren van shellcodes, afvangen van bestanden. Buffer overflow onder Windows of Linux, exploitatie met Meterpreter shellcode.

DATA

KLAS OP AFSTAND
2024 : 01 jul, 14 okt

BRUSSEL
2024 : 01 jul, 14 okt