algemeen

Studiepunten	3
Aandeel PE/Examen	30% - 70%
Examen vorm	Mondeling met schriftelijke voorbereiding

De lessen zijn een combinatie van theorie en demo's. Aanwezigheid in de lessen is zeer aan te raden, omdat alle examenvragen wel eens zullen voorkomen.

De permanente evaluatie bestaat uit twee taken. De eerst is het digitaal onderteken van een email of JAR-file. De tweede taak is een mini-project over een door jou gekozen onderwerp, maar uiteraard moet het wel iets met beveiliging te maken hebben.

Het examen is theoretisch. Je moet je hacking-skills dus niet ten toon stellen. Je dient gewoon de gevaren en de oplossingen te kennen van de geziene beveiligings. Het is toegestaan de artikels op export af te drukken en mee te nemen naar het examen.

Lijst van technieken

Dit is een lijst van technieken die je kan gebruiken voor het kraken van allerhande beveiligingen, het saboteren van websites, etc. De lijst is zeker en vast niet volledig dus vul hem gerust aan. Indien je een van deze technieken, voor welke reden dan ook, wilt uitproberen. Zorg er dan voor dat je ZEKER EN VAST een getekende toestemming hebt van de eigenaar/verantwoordelijke van het systeem, of zet zelf een systeem op. Virtuele machines kunnen wonderen doen als je het bij jezelf wilt uitproberen. Je zal voor deze technieken wel zelf moeten opzoeken wat dat ze betekenen. Note: Als iemand tijd en zin heeft, mag die altijd beschrijvingen toevoegen :)

1. Portscanning
2. XSS exploits
3. CSRF (uitgesproken als seasurf) exploits
4. SQL injections
5. FTP server exploiten
6. DNS records veranderen
7. Smurf attack
8. Cookie stealing
9. Session hijacking (in browsers)
10. Log poisoning

11. E-mail spoofing
12. Phishing
13. ARP-Spoofing
14. Man in the middle attacks
15. Passive sniffing
16. Social engineering
    1. Even telefoneren...
    2. Dumpsterdiving
17. botnet

Revision #4
Created 31 October 2021 22:21:31 by Jasper G.
Updated 16 January 2022 15:02:33 by Jasper G.