2011 januari examen

Groep 2

1. Er worden 5 weaknesses gegeven
    1. Zet ze in volgorde van erg naar minder erg.
    2. Als er nog geen update/patch voor handen is voor deze exploit, hoe zou je voorkomen dat er misbruik van wordt gemaakt?
2. Een vertrouwelijke mail
    1. Hoe kan ik aan deze mail geraken?
    2. Hoe beveilig ik tegen de voorgestelde methodes?
3. 3 waar of niet stellingen:
    1. SQL injection is enkel gevaarlijk in formulieren waar wordt ingevoegd of verwijderd.
    2. Een poortscan wordt steeds door een IDS opgemerkt
    3. XSS is niet gevaarlijk, enkel hinderlijk
4. Leg uit en geef voorbeelden:
    1. Risico / Risk
    2. In depth security

Groep 1

1. Er worden 5 security advisors gegeven (dit is een vraag die altijd terug komt)
    1. Zet ze in volgorde van erg naar minder erg. (dit moet je kunnen verdedigen. Een security adviser die meld dat een lokale gebruiker admin rechten kan krijgen is voor een systeembeheerder een groot probleem, maar voor een gebruiker op zijn thuiscomputer niet)
    2. Als er nog geen update/patch voor handen is voor deze exploit, hoe zou je voorkomen dat er misbruik van wordt gemaakt?
2. Een webmail
    1. Hoe kan een buitenstaander aan de inloggegevens geraken en geef een schaal van 1 op 10 naar moeilijkheid? (hier zou je er toch 7 tot 10 moeten op kunnen geven)
    2. Hoe beveilig ik tegen de voorgestelde methodes?
3. 3 waar of niet stellingen:
    1. Een portscan is een vorm van passieve verkenning
    2. Een webinterface waar het wachtwoord in een hash is bewaard met salting is onmogelijk om een bruteforce op te doen
    3. Welk van de 2 zal het meeste false positives genereren: anomaly detection of patroon detectie

4. Termen kunnen verduidelijken met voorbeelden (eigen voorbeelden worden het meest geapprecieerd, voorbeelden die in de cursus staat of tijdens de les zijn gegeven minder)
    1. least privileged
    2. Security through obscurity

Revision #1
Created 31 October 2021 22:25:24 by Jasper G.
Updated 16 January 2022 15:02:33 by Jasper G.