**Hogeschool PXL**



Departement IT

|  |  |
| --- | --- |
| 1. Vak: Basic Security – **Voorbeeld examen**   Resultaat PE: /40  Resultaat Examen: /60 Eindresultaat: /100 => /20 | |
|  |  |
| 1. Door student in te vullen:   Naam:  Voornaam:  Klas:  Lector: | 1. Datum:   Klassen: 2TIN  Lectoren:   * Bram Heyns |
|  |  |
| 1. Praktische examenrichtlijnen voor de studenten:   Het examen is schriftelijk gesloten boek, **zonder laptop** | 1. Elke student(e) is verantwoordelijk voor de correcte samenstelling van zijn/haar bundeltje. Eventuele afwijkingen moeten onmiddellijk aan één van de toezichthoudende lectoren gesignaleerd worden.   Samenstelling van het bundeltje:  … Getypte bladen  … Kladblad |
|  |  |
| 1. Aanvangsuur examen: 8u30 | Einde examen: **11u00 (!)** |



De groepsopdracht (PE) voor het OLOD ‘Basic Security’ stond op 40%, en dit schriftelijk examen staat op 60%.

Zorg dat de neergeschreven antwoorden duidelijk leesbaar zijn. Een onleesbaar antwoord is hetzelfde als een fout antwoord.

Structuur examen en onderverdeling van punten (op 60):

* Hoofdvragen (/40)
* Concepten (/20)

Hoofdvragen:

Ieder aspect van deze vragen dient uitvoerig en gedetailleerd beantwoord te worden.

Concepten:

De concepten kunnen kort en bondig (enkele zinnen) beantwoord worden.

1. **Hoofdvragen ( /40)**
   1. **Hybride cryptografie (/20)**

Hybride cryptografie is de combinatie van hashing, symmetrische-, en asymmetrische cryptografie. Dit principe vormt de basis van alle veilige communicatie over het Internet. Door deze combinatie efficiënt en correct toe te passen, kan A een bericht sturen naar B, zodat B met (redelijke) zekerheid kan zeggen, dat:

1. Het bericht van A afkomstig is
2. Het bericht onveranderd is gebleven tijdens het transport
3. B de enige was die de inhoud van het bericht terug kan lezen
4. En A kan zelfs niet meer ontkennen dat het bericht van hem/haar afkomstig was.

Leg (aan de hand van een **schets**) uit hoe deze efficiënte combinatie werkt (zowel de **encryptie bij A**, als de **decryptie bij B**). Geef steeds duidelijk aan **welk algoritme** gebruikt wordt, en **welke key** (indien van toepassing). Bewijs hoe en waar in het ganse proces de **4 bovenstaande zekerheden** gegarandeerd worden.

Puntenverdeling:

* Algemene werking (schets): /8
* Bewijs principe i. /3
* Bewijs principe ii. /3
* Bewijs principe iii. /3
* Bewijs principe iv. /3

**(vervolg 1.1 – hybride crypto)**

* 1. **PKI – certificaten (/10)**

Public Key Infrastructure (PKI) is de verzamelnaam voor de uitgifte en beheer van X.509v3 certificaten. Zo’n infrastructuur bestaat uit verschillende onderdelen, en concepten.

Leg onderstaande **onderdelen/concepten** uit, en **omschrijf het proces** om een certificaat te bekomen bij zo’n PKI.

1. Wat is een certificaat (2 belangrijkste items in een certificaat + waarom is het te vertrouwen)? (/2)
2. Registration Authority (RA) (/1)
3. Certification Authority (CA) (/1)
4. Validation Authority (VA) (/1)
5. Certification Policy (CP) (/1)
6. Certification Practise Statement (CPS) (/1)
7. Certification Revocation List (CRL) (/1)
8. Proces van een certificaat aanvraag (inclusief Proof of Possession principe) (/2)
   1. **Vulnerability Scanner (/10)**

Een vulnerability scanner is een belangrijk hulpmiddel in de strijd tegen cybercriminelen. Iedere vulnerability scanner bestaat uit 3 hoofdcomponenten, nml. een poortscanner (met service detection), een vulnerability database, en een rapportage systeem (false positives, false negatives). Leg deze 3 componenten grondig uit, waarbij voldoende aandacht moet worden besteed aan mogelijke problemen rond classificatie van vulnerabilities (confusion matrix).

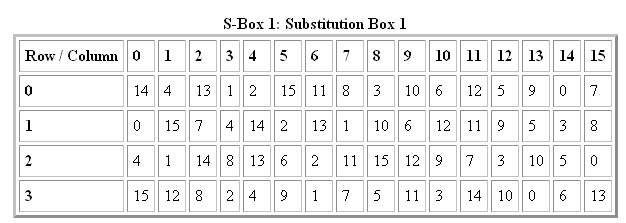
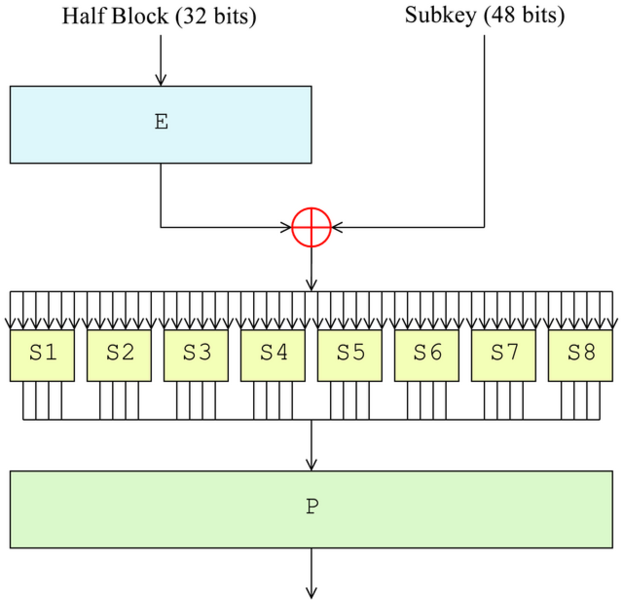
Puntenverdeling:

* Poortscanner, met service detection: /3
* Vulnerability DB: /1
* Rapportage, met confusion matrix: /6

1. **Concepten ( /20)**

Leg onderstaande concepten kort en bondig uit. Wees duidelijk en to the point (gebruik eventueel een schets om het concept iets te verduidelijken). Ieder concept staat op 2 punten.

* 1. **SIEM server (/2)**
  2. **SYN flood (/2)**
  3. **Avalanche effect bij symmetrische cryptografie (/2)**
  4. **Birthday attack tegen hashes (/2)**
  5. **Diffie-Hellman sleuteluitwisseling (/2)**
  6. **OCSP (/2)**
  7. **Rootkit (/2)**
  8. **ARP Poisoning (/2)**
  9. **S-box (bij DES encryptie) (/2)**



* 1. **Cookie stealing via reflected XSS attack (/2)**

KLADBLAD

KLADBLAD2