Vraag 1.

Bij bovenstaand loginformulier hoort onder meer de volgende code:

QueryString = "SELECT \* FROM users WHERE " +

              "Username = '" + GetUsername +

              "' AND Password = '" + GetPassword + "'"

De variabelen GetUserName en GetPassword bevatten de tekst die de gebruiker invult in het formulier.

Deze code is kwetsbaar voor SQL-injectie. Hieronder staan een aantal mogelijkheden om het formulier in te vullen.

Geef aan welke daarvan in dit geval leiden tot een succesvolle SQL-injectie.

(Er zijn meerdere goede antwoorden mogelijk).

SELECT \* FROM users WHERE Name = 'admin--'' AND Password = ''--'

Syntax is niet correct

SELECT \* FROM users WHERE Name = 'admin--' AND Password = 'yolo'

Syntax is correct maar gebruiker en wachtwoord waarschijnlijk niet goed.

SELECT \* FROM users WHERE Name = 'admin' AND Password = 'xxx' OR 'yolo'='yolo'

Deze werkt (always true)

SELECT \* FROM users WHERE Name = 'admin'--' AND Password = 'xxx'OR 'X\*1'='1\*X'

Deze werkt (commenting vanaf de --)

Vraag 2

|  |
| --- |
| Koppel de genoemde tools zo goed mogelijk aan de stappen. |
| |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | Question | Correct Match | | 1: Profiling | Correct A.  Google Chrome en Facebook | | 2: Enumeration | Correct C.  NMap (portscanning-tool) | | 3: Vulnerability Analysis | Correct B.  de CVE-website | | 4: Exploitation | Correct H.  Kali Linux | | 5: Reporting | Correct I.  Microsoft Word en Powerpoint | | |

Vraag 3

Een hacker stuurt je een mail met het verzoek op een linkje (in de mail) te klikken en daarna op de website van je bank in te loggen.

De link ziet er als volgt uit:

 https://debank.nl/inloggen?session=cookie.txt

|  |
| --- |
| Beantwoord de volgende deelvragen:   1. Welke hack-methode(s) past de hacker hier toe (volledige naam)? *(1 punt)* 2. Als je op deze link klikt, kom je dan op de echte site van de bank terecht? *(2 punten)* |
| |  |  | | --- | --- | | Correct Answer: | Correct   1. phishing in combinatie met Reflected Cross Site Scripting 2. Ja | |

Vraag 4

|  |
| --- |
| Hieronder staan een aantal bedreigingen.  Geef aan welke van deze bedreigingen vallen onder Social Engineering (meerdere antwoorden mogelijk) |
| |  |  | | --- | --- | | Answers: | ransomwaring | |  | Correct  phishing | |  | Correct  dumpster diving | |  | trolling | |  | Correct  shoulder surfing | |  | Correct  baiting | |  | ghosting | |  | Correct  vishing | |

Vraag 5

|  |
| --- |
| Auke wil een bericht aan Bauke sturen. Dit bericht mag niet door onbevoegden worden afgeluisterd. Ze spreken af hun berichten te versleutelen met een **asymmetrisch**algoritme.   1. Welke sleutel moet Auke gebruiken om het bericht te versleutelen?*(1 punt)* 2. Waarom kan hacker Eef het bericht niet ontsleutelen? *(1 punt)* |
| |  |  | | --- | --- | | Correct Answer: | Correct   1. De public key van Bauke 2. Eef kan het bericht niet ontsleutelen omdat hij (of zij) de private key van Bauke niet heeft. | |

Vraag 6

|  |
| --- |
| Een website gebruikt een self-signed certificaat. Een gebruiker maakt een https://verbinding met deze website.  Is dit een veilige verbinding? |
| |  |  | | --- | --- | | Answers: | Ja, er wordt een certificaat gebruikt dus is de verbinding veilig | |  | Nee, het certificaat is niet uitgegeven door een CA. | |  | Nee, de gebruiker kan de website niet authenticeren. | |  | Correct  Ja, maar alleen als de gebruiker zeker weet van wie het certificaat afkomstig is. | |

Response Feedback:

Wanneer de gebruiker zeker weet dat het certificaat echt is (niet door een hacker gemaakt) is de verbinding verder veilig.

Vraag 7

|  |
| --- |
| Geef van onderstaande bedreiging aan welk van de CIA-termen hiermee is gemoeid.  Een groot bedrijf kopieert alle toetsaanslagen van alle medewerkers naar een centrale server. Hierdoor raakt het netwerk overbelast. |
| |  |  | | --- | --- | | Answers: | Confidentiality | |  | Integrity | |  | Correct  Availability |  |  |  | | --- | --- | | Response Feedback: | Door de overbelasting is het systeem nog wel beschikbaar maar niet goed bruikbaar. | |

Vraag 8

|  |
| --- |
| Het berekenen van een HMAC van data is gericht op een of meer aspecten van informatiebeveiliging. Welke? |
| |  |  | | --- | --- | | Answers: | Confidentiality | |  | Correct  Integrity | |  | Availability | |  | Correct  Authentication | |  | Authorization | |  | Non-Repudiation |  |  |  | | --- | --- | | Response Feedback: | Een HMAC is een met een (gedeelde) sleutel versleutelde hashcode die meegestuurd wordt. Dit garandeert de Integrity en zorgt tevens voor Authenticatie omdat de sleutel bij beide partijen bekend is. | |

Vraag 9

|  |
| --- |
| Mag een ethische hacker een Black Box penetratietest doen? Motiveer je antwoord. |
| |  |  | | --- | --- | | Correct Answer: | Correct  Een Black Box penetratietest betekent alleen dat je vooraf niets weet over het te hacken systeem. Dus een ethische hacker mag dat ook doen. | | Response Feedback: | [None Given] | |

Vraag 10

|  |
| --- |
| Geef een korte definitie van de volgende begrippen zoals die in de informatiebeveiliging gebruikt worden *(1 punt per begrip)*:   1. Asset 2. Threat Agent 3. Authentication |
| |  |  | | --- | --- | | Correct Answer: | Correct   1. Alles van waarde (voor een organisatie) 2. Een persoon of organisatie die een specifieke dreiging zou kunnen uitvoeren. 3. Het vaststellen van de identiteit van een persoon/systeem | |

Vraag 11

|  |
| --- |
| Het onderstaande codefragment laat een functie zien die de inhoud van een door de gebruiker op te geven directory leest en deze laat zien op de console. Hiervoor wordt het systeemcommando 'dir' gebruikt.  (de .NET functies tot en met proc.start laten een systeemcommando door het operating system uitvoeren).  // taal: C#   public void ShowDirectory(string userDirName) {    string command = "dir " + userDirname System.Diagnostics.ProcessStartInfo procStartInfo = new System.Diagnostics.ProcessStartInfo("cmd", "/c " + command);  System.Diagnostics.Process proc = new System.Diagnostics.Process();  proc.StartInfo = procStartInfo;  proc.Start(); }  Beantwoord de volgende deelvragen:   1. Welke kwetsbaarheden wordt door deze code in het programma geintroduceerd ? *(1 punt)* 2. Hoe zou het programma moeten worden aangepast om deze kwetsbaarheid te verhelpen?*(1 punt)* |
| |  |  | | --- | --- | | Correct Answer: | Correct   1. path traversal en code injection 2. input sanitation en bescherming van de server. | |

Vraag 12

|  |
| --- |
| Op de website van een bank zie je dat de URL als volgt is opgebouwd:  https://debank.nl/get-page.asp?file=balance.csv  Een hacker voert de volgende URL in in de browser:  https://debank.nl/get-page.asp?file=../corona/bestand.pdf  Beantwoord de volgende deelvragen:   1. Als de website zich bevind in directory /usr/htdocs, welk bestand probeert de hacker hier te laden ? 2. Hoe heet deze hacking techniek ? |
| |  |  | | --- | --- | | Correct Answer: | Correct   * 1. /usr/corona/bestand.pdf   2. Path traversal. (of directory traversal) | |

Vraag 13

|  |
| --- |
| Wat is een zombie bij een botnet? |
| |  |  | | --- | --- | | Correct Answer: | Correct  Een computer onder controle van een zogeheten command center. Het command center kan via de zombie bijvoorbeeld spam versturen of bij een DDOS-aanval inzetten. | |

Vraag 14

|  |
| --- |
| Koppel de omschrijving aan het juiste begrip |
| |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | Question | Correct Match | | Gewone data | Correct G.  Plaintext | | Versleutelingsalgoritme waarbij 1 sleutel wordt gebruikt voor versleuteling en ontsleutelen | Correct B.  Symmetrisch algoritme |  |  | | --- | | All Answer Choices | | A.  Sleutel | | B.  Symmetrisch algoritme | | C.  Substitutie en transpositie | | D.  Message Digest | | E.  Geheim algoritme | | F.  Asymmetrisch algoritme | | G.  Plaintext | | H.  Openbaar algoritme | |  |  |  | | --- | --- | | Response Feedback: | Gewone data: Plaintext  Versleutelingsalgoritme waarbij 1 sleutel wordt gebruikt voor versleuteling en ontsleutelen:  Symmetrisch algoritme | |

Vraag 15

|  |
| --- |
| Je bent bezig met een penetratietest in opdracht van een organisatie. Je ontdekt dat je in staat bent om de website van deze organisatie over te nemen. Je beste vriend biedt je veel geld om een grappige afbeelding op die website te zetten.  Wat doe je? |
| |  |  | | --- | --- | | Correct Answer: | Correct  Netjes melden bij de organisatie die je heeft ingehuurd, en niet doen natuurlijk. En je vriend streng toespreken. | |

Vraag 16

|  |
| --- |
| Een gebruiker is ingelogd op de website van een bank (https://defoutebank.nl).  Een hacker stuurt deze gebruiker een (phishing) mail met daarin ondermeer de volgende link:  <a href="https://defoutebank.nl/transfer.do?acct=HACKER\_IN\_ENG\_LAND&amount=234">Klik hier!</a>  Beantwoord de volgende deelvragen:   1. Welke hacking-techniek probeert de hacker hier via deze phishing mail toe te passen ? (*1 punt)* 2. Wat hoopt de hacker hiermee te bereiken? *(1 punt)* 3. Noem een manier om de website te beveiligen tegen deze kwetsbaarheid ? (*1 punt*) |
| |  |  | | --- | --- | | Correct Answer: | Correct   * 1. CSRF (Cross Site Request Forgery)   2. Hij hoopt dat de gebruiker klikt op de link en dat dan de transactie naar de bank wordt gestuurd en uitgevoerd   3. Een manier om sessies beter te beveiligen, niet alleen via de cookies. | |

Vraag 17

|  |
| --- |
| Koppel de begrippen aan de juiste betekenis |
| |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | Question | Correct Match | | Plaintext | Correct D.  Gewone data | | Symmetrisch algoritme | Correct G.  Versleutelingsalgoritme waarbij 1 sleutel wordt gebruikt voor versleuteling en ontsleutelen |  |  | | --- | | All Answer Choices | | A.  Geheim algoritme | | B.  Openbaar algoritme | | C.  One-way function om data samen te vatten | | D.  Gewone data | | E.  Substitutie en transpositie | | F.  Versleutelingsalgoritme met twee sleutels, 1 voor het versleutelen, een andere voor ontsleutelen | | G.  Versleutelingsalgoritme waarbij 1 sleutel wordt gebruikt voor versleuteling en ontsleutelen | | H.  Kort stukje data wat gebruikt wordt bij een versleutelingsalgoritme | | |