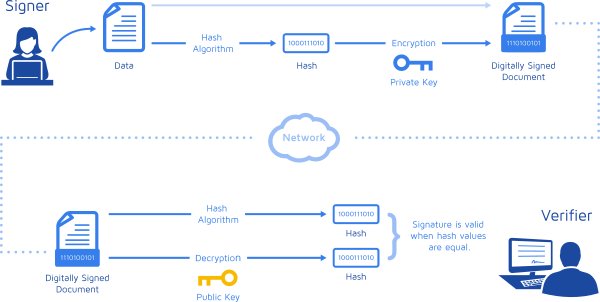
Međuispit 2015.

1. (3 boda) Skicirati postupak digitalnog potpisivanja.



1. (3 boda) Koja je razlika između savršeno sigurnih šifri i praktički sigurnih šifri.

Kod savršenog sigurnih šifri moraju biti zadovoljeni uvjeti da šifrat ne otkriva nikakve podatke na temelju kojeg otvorenog teksta je mogao nastati i da otvoreni tekst ne otkriva kakav bi šifrat mogao nastati. Dok praktično sigurne šifre moraju osigurati da trošak razbijanja šifre nadmašuje vrijednost šifrirane informacije ili vrijeme potrebno za razbijanje nadilazi vrijeme važenja šifrirane informacije.

1. (3 boda) Kako duljina ključa utječe na sigurnost šifriranja?

Duljina ključa označava koliko će vremena biti potrebno da se napadom razbije šifra. Samim time što je dulja šifra, dulje će biti potrebno da ju se razbije i tako je šifrirana informacija sigurnija.

1. (3 boda) Kako funkcionira provjera digitalnog certifikata? Na kojem dijelu digitalnog certifikata počiva povjerenje koje mu se poklanja?

Provjera digitalnog certifikata se obavlja tako da se provjerava ispravnost svih certifikata do njihovog krovnog izdavača koji mora imati povjerenje onoga koji provjerava. Također certifikat ne smije biti opozvan od nijednog izdavača u lancu do krovne institucije. Digitalni potpis izdavatelj osigurava poklonjeno povjerenje certifikata.

1. (3 boda) Navesti koja je svrha voditelja sigurnosti (CISO) u organizacijama.

* Nadzor i koordinacija aktivnosti vezanih uz sigurnost informacijskog sustava
* Iniciranje primjene dobrih praksi i prihvaćenih standarda vezanih u sigurnost informacijskog sustava
* Savjetodavna uloga u svezi sa sigurnosti informacijskog sustava

1. (3 boda) Koji je temeljni akt na kojemu se temelji sigurnost organizacije te što je njegova svrha?

Temeljni akt je **Politika sigurnosti informacijskog sustava** koji definira što za informacijski sustav znači da je siguran.

1. (2 boda) Zašto je potrebno nadzirati rad voditelja sigurnosti te tko obavlja tu zadaću?

Revizije i nadređene osobe (CEO, nadzorni odbor). (to je za CISO-a, ali pretpostavljam da je isto ukoliko struktura ima CSO)

1. (3 boda) Objasniti utjecaj ranjivosti u protokolima, implementacijama i konfiguraciji s obzirom na obuhvat te mogućnosti ispravljanja ranjivosti.

Nismo to još radili.

1. (2 boda) Zašto je fizička sigurnost temeljni preduvjet sigurnosti?

Ukoliko napadači imaju fizički pristup sustavu, većina programske i mrežne sigurnosti je uzaludna. Mogućnost uništenja servera, uništavanja diskova itd.)

1. (2 boda) Kako je zloupotrebom protokola ARP moguće izvršiti MITM napad?

Slanjem mnoštva ARP zahtjeva/odgovora moguće je preusmjeriti promet promet preko napadačevog računala. IP adresa traženog računala se krivo prevodi u MAC adresu napadačevog računala.

1. (2 boda) Koja su dva temeljna načina otkrivanja ranjivosti u mreži?

Na fer2netu stoji statička i dinamička analiza koda te fuzz testing. Ali to je za ranjivost u kodu. Na prezentacijama stoji da je provjera mrežnih ranjivosti uglavnom temeljena na testiranju poznatih ranjivosti u poslužiteljskom softveru (npr. Apache).

1. (4 boda) Objasnite osnovne postavke BLP modela (Bell- La Padula Security Model) i ilustrirajte primjerom.

Nismo to radili još.

1. (5 bodova) Neš sa tablicama u bazi vezano u sigurnost baza podataka, ali nismo to još radili.
2. (2 boda) Objasnite što je sigurnosna politika.

Interni akti koje piše voditelj sigurnosti informacijskog sustava (CISO) i definira smjernice i osnovna načela sigurnosti. Ne definira konkretne tehničke i implementacijske detalje.

1. Objasnite razliku između otvorene i zatvorene politike upravljanja pristupom.

Nismo još radili.