IT381 – Skripta

I. Blic pitanja:

1. Kodovane informacije su:

a) podaci
b) slike
e) pismo
c) ništa od navedenog
d) binarni kod

2. Komponente informacionog sistema su?

a) hardver, softver, procedure, mreža, podaci, trojanci
b) procedure, hardver, crvi, mreža, podaci, hakeri
c) ljudi, procedure, hardver, softver, mreža, podaci
d) podaci, softver, virusi, hardver, ljudi, procedure
e) procedure, ljudi, hardver, zlonamerni kod, internet, podaci

3. Bezbedonosnom uslugom se povećava?

a) upotreba softvera
b) bezbednost informacija
c) broj procedura koje se koriste u sistemu zaštite
d) korišćenje mreže za prenos podataka
e) neophodan hardver za bezbbednu komunikaciju

4. Bezbednosni mehanizmi postoje da obezbede i podrže?

a) bezbednosne ciljeve
b) bezbednosne usluge
c) kontrolu pristupa
d) neporicanje
e) raspoloživost usluga

5. Koje su tri fundamentalne bezbednosne usluge

a) poverljivost, provera identiteta, raspoloživost
b) poverljivost, integritet, raspoloživost
c) zaštita, otkrivanje, odgovor
d) integritet, neprocenivost, provera identiteta
e) procena, zaštita, otkrivanje

6. Koji je od sledećih napad na raspoloživost?

a) presecanje
b) izmena
c) fabrikacija
d) nijedan od navedenih
e) presretanje

7. Utvrđeni (bastion) host je sistem identifikovani od strane zaštitnog zida administratora kao?

a) „uska grla” između unutrašnjih i spoljnih mreža
b) jaka kritična tačka
c) tačka za audit
d) slaba kritična tačka
e) prolazna tačka

8. Koji režim rada obezbeđuje zaštitu prvenstveno za gornji sloj protokola?

a) transportni
b) autentifikacija zaglavlja
c) tunelski
d) tunelski i transportni
e) autentifikacija paketa

9. Koja dva protokola se koriste za pružanje bezbednosti na IP sloju?

a) ESP i upravljanje ključevima
b) AH i ESP
c) ESP i PGP
d) AH i upravljanje ključem
e) AH i S/MIME

10. Koja su dva osnovna režima rada IPsec protokola?

a) tunelski i kontrola pristupa
b) transportni, tunelski
c) integritet, poverljivost
d) autentifikacija, integritet
e) transportni i kontrola rutiranja

11. Koji algoritam za šifrovanja mora da podržava implementacija ESP protokola?

a) Trostruki DES
b) RCS
c) DES
d) IDEA

12. Šta obezbedjuje SSL protokol između Web klijenta i Web servera?

a) šifrovanje podataka i integritet podataka
b) komprimovanje podataka i autentifikaciju
c) komprimovanje podataka i šifrovanje podataka
d) šifrovanje podataka i autentifikaciju

13. Na kom algoritmu šifrovanja je zasnovan SSL protokol?

a) asimetričnom
b) SHA
c) MAC
d) simetričnom

14. Ako je Web server obezbeđen sa SSL slojem, kako izgleda protokolski deo linka URL za stranicu?

a) http://
b) https://
c) rtsp://
d) sips://

15. Šta je uloga AS servera u Kerberos protokolu?

a) Isporuka kljuceva
b) Isporuka ključa sesije
c) Provere identiteta korisnika
d) Isporuka karti
e) Isporuka sertifikata serverima

16. Šta je uloga TGS servera u Kerberos protokolu provere identiteta?

a) provere identiteta korisnika
b) isporuka sertifikata
c) isporuka ključeva
d) isporuka lozinki
e) isporuka karti

17. PGP (Pretty Good Privacy) je bezbednosni program za?

a) e-poštu
b) zaštitu paketa koji se prenosi
c) daljinsku autentifikaciju servera
d) izračunavanje izvoda paketa
e) šifrovanje saobraćaja

18. Koje mreže rade na većim udaljenostima (udaljenost prijemnika i odašiljača može iznositi i do 50 km)?

a) bluetooth
b) RFID
c) WPAN
d) SSL
e) Mobilna telefonija i WIMAX

19. Kojim standardom su definisane bežične mreže?

a) 801.22
b) 802.11
c) 801.11
d) 802
e) 801

20. Kako se naziva WLAN mreža u kojoj se pojedine pristupne tačke WLAN mreže mogu samostalno bežično povezati i tako proširiti WLAN mrežu bez kablovske inernet veze između njih?

a) MESH-WLAN
b) WPAN
c) Bluetooth
d) WWAN

21. Koji oblik provere identiteta zahteva IEEE802.11 standard?

a) provere identiteta deljenim ključem
b) provere identiteta upotrebom CRC algoritma
c) provera identiteta upotrebom RC4
d) provera identiteta otvorenog sistema

22. Koje tri bezbednosne usluge identifikuje GSM secifikacija?

a) provera identiteta, poverljivost podataka i anonimnost korisnika
b) provera identiteta, poverljivost i audit
c) provera identiteta, poverljivost i neporecivost
d) neporecivost, poverljivost i integritet
e) provera identiteta, poverljivost podataka i integritet

23. Mobilni uređaj je jedinstveno identifikovan preko?

a) IMSI
b) Ključa Kc
c) IMEI
d) A3
e) Ključa KI

24. Koji ključ se koristi za šifrovanje podataka koji se prenose mobilnom mrežom?

a) Korenski ključa Ki
b) Slučajni broj RAND
c) Definisan ključ algoritma A3
d) Definisan ključ algoritma A8
e) Generisani ključ Kc

25. Koji element bezbednosti štiti ljude i imovinu unutar celog poslovnog prostora, objekata ili zgrada?

a) Korporativna bezbednost
b) Logička bezbednost
c) Kontrola pristupa
d) Fizička bezbednost
e) IDS sistem

26. Na čemu se zasniva Linux tradicionalni model bezbednosti?

a) ljudi ili procesi sa "root" privilegijama mogu raditi šta god hoće-drugi ne
b) bezbednost na više nivoa
c) ograničenoj kontroli pristupa
d) kontroli pristupa na nivou mreže

7. U kom modelu je on-line aukcija jedna od mogućnosti on-line kupovine?

a) B2B
b) B2C
c) C2C
d) C2B

27. Koji bezbednosni servis plaćanja obezbeđuju anonimnost korisnika u mrežnim transakcijama, štite otkrivanje identiteta?

a) Bezbednosti smart kartica
b) Bezednosti digitalnog novca
c) Bezbednosti digitalnih čekova
d) Transakcioni
e) Bezbednosti platnih kartica

28. Podatak ili fizički objekt postaje dokaz jedino kada je prikupljen od strane?

a) Stručnog lica iz pravosuđa
b) Stručnjaka za bezbednost
c) Ovlašćenog lica
d) Lica koje ima znanja da sprovede forenziku
e) Administratora sistema

29. Koja tema bezbednosne politike uključuje definiciju informacione bezbednosti, njene ciljeve i sveukupni cilj i važnost?

a) Principi
b) Zaštita podataka
c) Sigurnost komunikacije
d) Softver
e) Operativni sistemi

30. Slabost u sistemu koje omogućava napadaču da naruši integritet sistema naziva se?

a) procena rizika
b) izloženost sistema
c) upravljanje rizikom
d) osetljivost sistema
e) ranjivost

31. Šta opisuje način na koji subjekat može pristupiti objektu?

a) objekat
b) subjekat
c) pravo pristupa
d) model
e) uloga

32. Za šta se koristi BIBA model?

a) tok informacija nagore
b) pravila za zaštitu integriteta informacija
c) za sprečavanje mešanja bezbednosnih funkcija
d) liste kontrole pristupa i liste sposobnosti
e) poverljivost klasifikovanih informacija

33. Kako se dele aktivni napadi?

a) prevencija, detekcija, odgovor i oporavak
b) presecanje, presretanje, izmena, fabrikovanje
c) presecanje, presretanje, izmena poruka, odbijanje usluga
d) ispitaj i proceni, eksploatiši i prodri, poveæaj privilegije, održi pristup
e) prerušavanje, ponovo pustiti, izmena poruka, odbijanje usluga

34. Koji je od sledećih je napad na raspoloživost?

a) presretanje
b) presecanje
c) izmena
d) fabrikacija
e) nijedan od navedenih

35. Koji je od sledećih na napad na integritet mreže?

a) presecanje
b) izmena
c) fabrikacija
d) nijedan od navedenih
e) presretanje

36. Koji model je razvijen za komercijalne aplikacije u kojima može nastati sukob interesa?

A) Model toka informacija
B)BLP model
C)Biba model
D)Clark-Wilson model
E) Chinesse Wall model

37. Osnov za dobijanje poverenja da su zahtevane bezbednosne mere efikasne i da su implementirane ispravno definiše se?

a) Funkcionalnim zahtevima
b) Bezbednosnim zahtevima
c) Zajedničkim kriterijumima
d) Zajedničkim klasama

38. Kako se naziva algoritam kod koga se otvoreni teksta obrađuje zamenom pozicija karaktera?

a) blokovska šifra
b) supstitucija
c) transpozicija
d) jednokratna beležnica

39. Pokušaj kriptoanalize u cilju otkrivanja algoritma šifre, ključa ili otvorenog teksta naziva?

a) sigurnost kriptosistema
b) šifrovanje
c) kompromitovanje
d) snaga kriptosistema
e) napad

40. Koji algoritam je do pojave kriptoanalize i napada grubom silom bio najčešće korišćen siguran hash algoritam?

a) RSA
b) DSS
c) MD5
d) SHA

41. Šta podrazumeva scenario za distribuciju ključeva pomoću centra KDC?

a) svaki korisnik deli jedinstveni javni ključ sa KDC
b) svaki korisnik deli jedinstveni privatni ključ sa KDC
c) svaki korisnik deli jedinstveni master ključ sa KDC
d) svaki korisnik deli ključ sesije sa KDC

42. Šta predstavlja algoritam sa svim mogućim otvorenim tekstovima, šifratima i ključevima?

a) šifrovanje
b) kriptografski sistem
c) dešifrovanje
d) kriptografski algoritam

43. Kojim bezbednosnim servisom se obezbedjuje zaštita od oštećenja, pomoću jednog od entiteta uključenih u komunikaciji ili deo komunikacije?

a) poverljivost
b) integritet podataka
c) kontrola pristupa
d) neodbacivanje
e) autentifikacija

44. Šta obezbedjuje ESP protokol sigurnosti na mrežnom sloju Interneta?

a) autentifikaciju i integritet podataka
b) kontrolu identiteta
c) autentifikaciju i kontrolu identiteta
d) autentifikaciju, integritet podataka i poverljivost
e) poverljivost

45. Koja su ograničenja zaštitnih zidova?

a) ne može da zaštiti od napad koji da zaobilaze, ne pruža zaštitu od internih pretnji
b) ne može da služi kao pratforma za IPSec prtokol
c) kontrola servisa, kontrola pravca
d) otkrivaju napad na osnovu definisanih sigurnosnih politika i anomalija sistema
e) kontrola korisnika, kontrola ponašanja

46. Koji napadi uključuju otkrivanje drugih korisnika, ubacivanje poruka u tranzitu izmedju klijenta i servera i ubacivanje informacija na web sajt?

a) Aktivni
b) Reprodukovanje
c) Upad
d) DoS
e) Pasivni

47. Server za izdavanje karata TGS (tiket-grant server) je deo kog protokola?

a) IP/IPSec
b) S/MIME
c) TLS
d) SSL
e) Kerberos

48. Kada započinje bezbednost Windows sistema?

a) po završetku instalacije operativnog sistema
b) odabirom softvera koji neće biti instalirani
c) konfigurisanjem bezbednosnih mehanizama
d) u trenutku instalacije aplikacije
e) u trenutku instalacije operativnog sistema

49. Koji oblik provere identiteta, kod bežičnih mreža, koristi kriptografske tehnike?

a) provere identiteta upotrebom CRC algoritma
b) provere identiteta upotrebom RC4 algoritma
c) provere identiteta otvorenog sistema
d) provere identiteta upotrebom AES algoritma
e) provere identiteta deljenim ključem

50. Kojom komandom se mogu menjati dozvole za svaku datoteku?

a) stikybit
b) setgid
c) chmod
d) useradd
e) setuid

51. Ko je najniži nivo OS-a ?

a) SRM (Security Reference Monitor)
b) LSA (Local Security Authority)
c) Object Manager
d) Jezgro – kernel
e) SD (Security Descriptor)

52. Kome se može dodeliti Linux korisnički nalog?

a) samo procesima
b) specijalnim uređajima
c) objektima
d) samo grupama
e) svima koji raspolažu mogućnost da rade sa datotekama

53. Koji su osnovni bezbednosni blokovi MS Windows arhitekture?

a) lozinka ili bilo koji mehanizam za proveru identiteta
b) bezbednosni zahtevi projektovanja, modelovanja napada
c) SRM, LSA, SAM, SD, WinLogon, NetLogon
d) SRM, LSA, SAM, AD, WinLogon, NetLogon
e) SRM, LSA, SD, WinLogon, NetLogon

54. Kako se naziva reakcija na detektovan događaja koji predstavljaju potencijalno narušavanje bezbednosti?

a) audit analizer
b) audit zapis
c) audit arhiver
d) audit provajder
e) audit odgovor

55. Kako se naziva informacija uskadištena ili prenošena u digitalnoj formi koja se koristi u sudskom postupku i mogu se koristiti na suđenju?

a) pravni dokaz
b) proveren dokaz
c) digitalni dokaz
d) informatički dokaz

56. Pojedini napadi koriste obične ljudske mane radi ostvarivanja pritupa koji su inače zabranjeni. Kako se nazivaju takvi napadi?

a) CHAP identifikator
b) socijalni napad/inženjering
c) IDS sistem
d) spoljašnje obezbeđenje
e) biometrija

57. U kom koraku digitalne forenzike se vrši izrada dokumentacije o nalazima?

a) sakupljanje
b) analiza
c) ispitivanje
d) priprema
e) izveštaj

58. U kom koraku digitalne forenzike se vrši izbor alata i opreme za forenzičku istragu?

a) ispitivanje
b) priprema
c) sakupljanje
d) analiza
e) izveštaj

59. U kom koraku kompjuterske forenzike se vrši izdvajanje dokaza iz prikupljenog materijala?

a) izveštaj
b) analiza
c) sakupljanje
d) ispitivanje
e) priprema

60. Neporicanje kao bezbednosna usluga obezbeđuje?

a)celovitost podataka
b)da korisnik koji pošalje poruku ne može kasnije poreći da je to uradio
c)da ovlašćeni korisnici imaju pristup podacima i računarskim resursima kada su im potrebni
d)da se podaci neautorizovano ne menjaju ili uništavaju

61. Bezbednosni ciljevi predstavljaju ciklus četiri faze?

a)poverljivost, integritet i raspoloživost
b)procena, prevencija, raspoloživost i odgovor
c)prevencija, detekcija, celovitost i odgovor
d)procena, prevencija, detekcija i odgovor
e)privatnost, sigurnost, poverljivost, raspoloživost

62. Zahtev da samo ovlašćeni korisnici mogu da menjaju podatke naziva se?

a)Provera identiteta
b)Raspoloživost
c)Neporicanje
d)Kontrola pristupa-
e)Integritet

63. U kojoj fazi napadač odlučuje koje resurse će napasti?

a)ispitaj i proceni
b)odbij uslugu
c)održi pristup
d)eksploatiši i prodri
e)povećaj privilegije

64. Odobrenje pristupa na određeni način jednom ili više objekata je?

a)funkcija pristupa
b)sesija
c)lista prava
d)dozvola ili pravo pristupa
e)uloga

65. Kome se dodeljuje sigurnosna oznaka u mehanizmu kontrole pristupa?

a)dodeljuje se nekom pravu pristupa
b)dodeljuje se nekom resursu
c)dodeljuje se nekom procesu
d)dodeljuje se nekoj ulozi
e)dodeljuje se nekom subjektu

66. Kako se nazivaju algoritmi kod kojih se originalna poruka šifruje po grupama (blokovima)?

a)blokovska šifra
b)supstitucija
c)transpozicija
d)šifra toka
e)jednokratna beležnica

67. Jednosmerna funkcija za autentifikaciju poruke koja ne uključuje korišćenje tajnog ključa za generisanje malog bloka podataka, poznatog je kao ?

a)kod za autentifikaciju
b)digitalni potpis
c)hash funkcija
d)šifrovanje

68. Kako se naziva pravno lice koje izdaje elektronske sertifikate u skladu sa odredbama zakona o digitalnom potpisu?

a)sertifikaciono telo
b)elektronski sertifikat
c)digitalni potpis
d)kvalifikovani elektronski sertifikat

69. Čiji cilj je da dobije pristup sistemu ili da poveća nivo privilegija na sistemu?

a)uljeza
b)pošiljaoca
c)primaoca
d)legitimnog korisnika -
e)crva

70. Detekcija uljeza zasniva se na pretpostavci?

a)da se ponašanje uljeza ne razlikuje od legitimnog korisnika na način koji se može kvantifikovati
b)da se ponašanje uljeza razlikuje od legitimnog korisnika na način koji se može kvantifikovati
c)da je ponašanje uljeza definisano modelom ponašanja prethodnih napada
d)da je ponašanje uljeza predvidljivo
e)da se ponašanje uljeza može detektovati hardverom

71. Ko beleži svaki audit zapis generisan od strane audit sistema za kolekciju?

a)menadžer
b)podsistem za upozoravanje
c)agent
d)analizator
e)operater

72. Šta obezbeđuje AH protokol sigurnosti na mrežnom sloju Interneta?

a)poverljivost
b)autentifikaciju i integritet podatak-
c)kontrolu identiteta
d)autentifikaciju, integritet podataka i poverljivost

73. Koja dva tipa upravljanja ključem određuje IPSec arhitektura dokumenta?

a)transportno i automatsko
b)tunelski i automatsko
c)fizičko i tunelski
d)fizičko i transportno

74. IPSec je skup protokola koji omogućava bezbednost na?

a)Gateway
b)Transportnom sloju
c)Zaštitnom zidu
d)Mrežnom sloju
e)Aplikativnom sloju

75. Koji protokol je izdat kao internet standard za daljinsku proveru identiteta?

a)S/MIME
b)TLS
c)SSL
d)Kerberos
e)IP/IPSec

76. Koji je bezbednosni protokol u IEEE802.11 bežičnim lokalnim mrežama?

a)IPsec
b)Bluetooth
c)WEP
d)WPA2
e)WPA

77. Koja dužina ključa za WEP protokol je definisana standardom IEE 802.11?

a)40 bita
B)128 bita
c)56 bita
d)152 bita
e)104 bita

78. Protokol IEEE802.11i pored bežičnog klijenta i pristupne tačke AP definiše?

a)WEP, EAP ključ
b)server za proveru identiteta
c)passkey, ključ sesije
d)dinamičko definisanje ključa šifrovanja
e)upareni glavni i privremeni ključ

79. Šta na Unix sistemu nije predstavljeno kao datoteka?

a)objekti i grupe
b)grupe i akcije
c)korisnici i grupe
d)korisnici i objekti
e)korisnici i akcije

80. Šta obuhvata ranjivost Linux standardnih distribucija?

a)prekoračenje bafera, problemi sinhronizacije (race), DoS napad, ranjivost Web aplikacija, napad rootkit
b)korisnik ili proces sa root privilegijama
c)prostor Linux jezgra i prostor svih ostalih servisa
d)prekoračenje bafera, DoS, neograničena kontrola pristupa
e)DoS napad, ranjivost Web aplikacija, kontrola pristupa zasnovana na ulogama

81. U kojoj datoteci su definisane grupe?

a)/etc/shadow
b)/etc/secure
c)/etc/passwd
d)/etc/root
e./etc/group

82. Koji model elektronske trgovine je danas dominantan na internetu?

a)Consumer to Consumer (C2C)
b)Consumer to Business (C2B)
c)Business to Employee (B2E)
d)Business to Consumer (B2C)
e)Business to Business (B2B)

83. Kako se naziva plastična kartica sa ugrađenim mikroprocesorom i memorijom?

a)digitalni ček
b)elektronski ček
c)elektronski novac
d)elektronska kreditna kartica
e)smart kartica

84. Kako se naziva lista formatiranih zapisa događaja?

a)audit arhiver
b)bezbednosni audit tragovi
c)audit zapis
d)audit provajder
e)audit analizer

85. Koji log fajl sadrže informacije o validnim i ne validnim pokušajima logovanja kao i događaje koji regulišu korišćenje resursa?

a)security log
b)appliction log
c)mrežni log
d)system log

86. Koji način plaćanja je najpopularniji?

a)plaćanje samo debitnim karticama
b)plaćanje debitnim karticama i homebanking
c)plaćanje debitnim i kreditnim karticama
d)homebanking
e)plaćanje kreditnim karticama i homebanking

87. Kako se naziva skup bezbednosnih protokola i formata koji omogućava korisnicima da plaćaju kreditnom karticom na otvorenoj mreži, na siguran način?

a)digitalni sertifikat
b)Payment gateway
c)sertifikaciono telo
d)SET (Secure Electronic Transaction)
e)privatnost plaćanja

88. Kako se naziva osoba ili organizacija koja prodaje robu ili usluge koje mogu da se plate karticom?

a)Payment gateway
b)dobavljač
c)vlasnik kartice
d)izdavač
e)trgovac

89. Koja tema bezbednosne politike uključuje kontrolu pristupa i zahtevano prijavljivanje na sistem?

a)softver
b)principi
c)operativni sistemi
d)sigurnost komunikacije
e)zaštita podataka

90. Zamena međusobnog položaja elemenata otvorenog teksta, tj. otvoren tekst se ne menja, menja se samo međusobni položaj elemenata otvorenog teksta je?

a)transpozicija
b)jednokratna beležnica
c)šifra toka
d)blokovska šifra
e)supstitucija

91. Ko određuje kojim sistemima je dozvoljeno da komuniciraju međusobno i jednokratan obezbeđuje ključ sesije za komunikaciju?

a)javni ključ
b)modul bezbednosnih usluga
c)stalni ključ
d)centar za distribuciju ključeva (KDC)
e)master ključ

92. Koji algoritam je izabran kao standardni MAC alat za IPS, TLS i SET protokole?

a)HMAC
b)SHA
c)MD5
d)DSS

93. Pomoću koje komponente ili procesa korisnik upravlja IDS sistemom?

a)analizator
b)agent
c)operater
d)menadžer
e)podsistem za upozoravanje

94. Bilo koja akcija koja kompromituje bezbednost jednog sistema naziva se?

a)Napad na bezbednost
b)Mehanizam bezbednosti
c)Bezbednost na mrežnom sloju
d)Bezbednosni servisi
e)Bezbednosni protokol

95. Koji zaštitni zid kontroliše saobraćaj izmedju ličnog računara ili radne stanice sa jedne strane, i Interneta ili mreže preduzeća sa druge strane?

a)zaštitni zid zasnovan na host
b)lični zaštitni zid
c)ruter
d)utvrdjeni zaštitni zid
e)SOCKS

96. Koji režim rada pruža zaštitu za ceo IP paket?

a)tunelski i transportni
b)transportni
c)tunelski
d)autentifikacija paketa
e)autentifikacija zaglavlja

97. Koji priotokol je pouzdana treća strana usluge provere identiteta?

a)Kerberos
b)S/MIME
c)SSL
d)IP/IPSec
e)TLS

98. Kojom komandom se menja vlasništvo na Linux sistemu?

a)stikybit
b)setuid
c)useradd
d)chmod
e)setgid

99. Koja komanda ako se postavi na izvršnu binarnu datoteku uzrokuje da se program "izvršava kao" da ga je pokrenuo njegov vlasnik?

a)chmod
b)stikybit
c)setuid
d)useradd
e)setgid

100. Koja komponenata obavlja proveru pristupa, generiše audit log zapise, i upravlja pravima korisnika, koji se nazivaju i privilegije?

a)SRM (Security Reference Monitor
b)WinLogon, NetLogon
c)SAM (Security Account Manager)
d)LSA (Local Security Authority)
e)SD (Security Descriptor)

101. Ko beleži svaki audit zapis generisan od strane audit sistema za kolekciju?

a)menadžer
b)podsistem za upozoravanje
c)agent
d)analizator
e)Operater

102. Pre upotrebe elektronske opreme za obradu podataka, važne informacije su najčešće čuvane u?

a)magacinu
b)sefu
c)banci
d)registrima

103. Raspoloživost kao bezbednosna usluga obezbedjuje?

a)da ovlašćeni korisnici imaju pristup podacima i računarskim resursima kada su im potrebni
b)da se podaci neautorizovano ne menjaju ili uništavaju
c)da korisnik koji pošalje poruku ne može kasnije poreći da je to uradio celovitost podataka
d)pristup informacijama samo za one korisnike koji su ovlašćeni da tim informacijama pristupe

104. Integritet kao bezbednosna usluga obezbedju?

a)pristup informacijama samo za one korisnike koji su ovlaši da tim informacijama pristupe
b.)da se podaci neautorizovano ne menjaju ili uništavaju
c)da ovlašæeni korisnici imaju pristup podacima i računarskim resursima kada su im potrebni
d)da korisnik koji pošalje poruku ne može kasnije poreći da je to uradio celovitost podataka

105. Napad tokom koga se jedan entitet pretvara da je drugi naziva se?

a)Ponovo pustiti
b)Fabrikovanje
c)Izmena poruke
d)Odbijanje usluga
e)Prerušavanje

106. Matematička funkcija koja se koristi za šifrovanje i dešifrovanje naziva se?

a)kriptografski algoritam ili šifra
b)otvoren tekst
c)ključ
d)šifrat

107. Otkrivanje ključa nekriptoanalitičkim metodama naziva:

a)snaga kriptosistema
b)napad
c)šifrovanje
d)sigurnost kriptosistema
e)kompromitovanje

108. Koji bezbednosni mehanizam se koristi za proveru integriteta poruka?

a)digitalni potpis
b)kontrola pristupa
c)šifrovanje
d)autentifikacija poruk

109. Koji IDS sistem je zasnovan na računarima koji su određeni za metu eventualnih napada?

a)IDS zasnovan na hostu
b)SNORT
c)Lažni "mamci"
d)IDS zasnovan na mreži
e)Audit zapisa

110. Koje tri funkcionalne oblasti obuhvata IPSec protokol?

a)proveru identiteta, povjerljivost i digitalni potpis
b)kontrolu rutiranja, povjerljivost i upravljanje ključevima
c)autentifikacija, integritet i upravljanje ključevima
d)proveru identiteta, povjerljivost i upravljanje ključevima
e)algoritam za šifrovanje, digitalni potpies i upravljanje ključevima

111. Oakley protokol razmene ključa zasnovan je na?

a.HMAC kodu
b.digitalnom potpisu
c.asimetričnom algoritmu šifrovanja
d.Hash kodu
e.Diffie-Hellman algoritmu

112. Koji protokoli osiguravaju transportni sloj?

a)SSL, TLS
b)Kerberos, S/MIME
c)UDP
d)IP/IPSec
e)TCP

113. Kako se naziva tehnologija malih bežičnih mreža dimenzionisanih za male udaljenosti koje u gradskim uslovima iznose od nekoliko desetina do nekoliko stotina metara?

a)Bluetooth
b)WWAN
c)RFID
d)bezična lokalna mreža - WLAN
e)WPAN

114. Kod koje bežične mreže razlikujemo "ad hoc" i "infrastrukturne" veze?

a)WWAN
b)WPAN
c)WLAN
d)Bluetooth
e)RFID

115. Kako se naziva direktna veza dva računara ili drugih uređaja koji imaju ugrađene module za WLAN komunikaciju?

a)RFID
b)WPAN
c)ad hoc
d)GSM
e)infrastrukturna

116. Ko može da menja dozvole objekta?

a)svi korisnici
b)Kernel
c)grupa
d)vlasnik
e)subjekat

117. Koji bezbednosni model je implementiran u SELinux a zasniva se na Bell-LaPadula (BLP) modelu?

a)bezbednost na više nivoa
b)Type Enforcement
c)RBAC
d)DAC
e)MAC

118. Koji bezbednosni servis obezbeđuje da se novac ne može preuzimati sa računa potrošača ili smart kartice bez eksplicitne dozvole?

a)integritet plaćanja
b)tajnost plaćanja
c)autorizacija plaćanja
d)autentifikacija plaćanja
e)neporecivost plaćanja

119. Koji bezbednosni servis plaćanja sprečavaju ponovno korišćenje i falsifikovanje elektronskih novčanica?

a)bezbednosti smart kartica
b)transakcioni
c)bezbednosti digitalnih čekova
d)bezbednosti platnih kartica
e)bezbednosti digitalnog novca

120. Kako se naziva proces sprečavanja pristupa računarskim sistemima u nekoj zgradi?

a)spoljašnje obezbeđenje
b)IDS sistemi
c)video nadzor
d)sigurnosne zone
e)kontrola pristupa

121. Koji prestup ima najveći faktor rasta u oblasti kompjuterskog kriminala?

a)krađa labtop računara
b)krađa identiteta
c)krađa mobilnih telefona
d)krađa prenosnih memorija
e)neovlašćen pristup

122. Koji je od sledećih je napad na raspoloživost?

a)presretanje
b)presecanje
c)izmena
d)fabrikacija
e)nijedan od navedenih

Koji je od sledećih na napad na integritet mreže?

a)presecanje
b)izmena
c)fabrikacija
d)nijedan od navedenih
e)presretanje

123. Kontrola pristupa kao bezbednosna usluga dozvoljava

a)da je neko ili nešto ono za koga/šta se predstavlja
b)da ovlašćeni korisnici imaju pristup podacima i računarskim resursima kada su im potrebni
c)da korisnik koji pošalje poruku ne može kasnije poreći da je to uradio
d)da se podaci neautorizovano menjaju ili uništavaju
e)objektu proverenog identiteta da pristupi sistemu

124. Ometanje ili sprečavanje normalnog korišćenja ili upravljanja komunikacijskim objektima naziva se?

a)Ponovo pustiti
b)Fabrikovanje
c)Prerušavanje
d)Izmena poruke
e)Odbijanje usluga

125. Fragmenti koda koji se ubacuju u druge legitimne programe su?

a)Logička bomba
b)Klopka
c)Virus
d)Crv
e)Trojanski konj

126. Kada cena kriptoanalize premašuje vrednost šifrovanih informacija kažemo da je kriptografski sistem?

a)provaljen
b)napadnut
c)kompromitovan
d)jak
e)siguran

127. Željeno sigurnosno ponašanje sistema definisano je?

a)Funkcionalnim zahtevima
b)Zajedničkim klasama
c)Zajedničkim kriterijumima
d)Bezbednosnim zahtevima

128. Kako se naziva sigurnosni servis koji prati i analizira događaja na sistemu ili mreži sa ciljem pružanja upozorenja da je došlo pokušaja pristupa resursima sistema na neovlašćen način?

a)Sigurnosni cilj
b)Bezbednosni zahtev
c)Bezbednosni upad
d)Detekcija upada
e)Funkcionalni zahtev

129. Koji deo sistema je osmišljen kako bi odvukao napadača od pristupa osetljivom sistemu sa značajnim podacima i da administrator može prikupili informacije o aktivnostima napadača?

a)Dekoder paketa
b)Lažni "mamac" (honeypot)
c)senzor
d)SNORT
e)podsistem za evidentiranje

130. Kojim bezbednosni mehanizam se koristi za transformaciju podataka u oblik koji nije razumljiv za čitanje?

a)kontrola pristupa
b)uticaj saobraćaja
c)integritet podataka
d)kontrola rutiranja
e)primena matematičkih algoritama

131. Kako se naziva skup protokola koji omogućavaju bezbednost na mrežnom sloju?

a)S/MIME
b)Kerberos
c)IP Security
d)SSL
e)PGP

132. Koja usluga na Linux sistemu ograničava mogućnost brisanja stvari u direktorijumu?

a)setuid
b)setgid
c)stikybit
d)useradd
e)chmod

133. Između koje tri strane je moguće organizovati elektronsku transakciju?

a)vlade, kompanija i korisnika
b)prodavca, kompanija i korisnika
c)vlade, zaposleni i korisnik
d)zaposleni, kompanija i korisnika
e)vlade, kompanija i zaposleni

134. Najčešći upadi u sistem elektronskog poslovanja su od?

a)Neautorizovani zaposleni
b)Teroristi
c)Autorizovani zaposleni
d)Hakeri
e)Spoljni saradnici

II. Esejska pitanja:

1. Nabrojati minimum 3 mehanizma za bezbednost.

Lista bezbedonosnih mehanizama :

- ❖ Šifrovanje
- ❖ Digitalni potpis
- ❖ Kontrola pristupa
- ❖ Integritet podataka
- ❖ Provere identiteta
- ❖ Traffic Padding
- ❖ Kontrola rutiranja
- ❖ Overa

2. Nabrojati bezbednosne usluge:

U bezbedonosne usluge spadaju:

- ❖ Poverljivost – obezbeđivanja pristupa informacijama samo za one korisnike koji su ovlašćeni da tim informacijama pristupe
- ❖ integritet – obezbeđuje tačnost i potpunost informacija
- ❖ raspoloživost – obezbeđuje da ovlašćeni korisnici imaju pristup podacima i računarskim resursima kada su im, i gde su im potrebni
- ❖ provera identiteta – obezbeđuje način da se proveri da je neko ili nešto ono za koga / šta se predstavlja.
- ❖ kontrola pristupa – sprečava zloupotrebu pristupa
- ❖ neporecivost – služi da obezbedi neoboriv dokaz

3. Šta je to Ransomware?

Ransomware je vrsta malvera koji kodira podatke na računaru ili mreži, a zatim zahteva plaćanje otkupa od žrtve kako bi dobila ključ za dešifrovanje podataka. Ova vrsta napada obično blokira pristup žrtvi njenim vlastitim podacima, čime se stvara ozbiljan problem za korisnike ili organizacije.

4. Objasniti prisluškivanje i njuškanje kao primere najčešće primenjivanih vrsta napada i pretnji.

Prisluškivanje (Sniffing): Prisluškivanje je tehnika koja se koristi kako bi se neovlašćeno presrelo i pratilo komunikacioni saobraćaj između uređaja u mreži. Napadač koristi alate koje omogućavaju presretanje i analizu mrežnog saobraćaja, omogućavajući mu da vidi nezaštićene informacije, uključujući korisničke lozinke, privatne podatke ili druge osetljive informacije. Prisluškivanje može ozbiljno ugroziti privatnost i sigurnost, jer omogućava napadaču da pasivno prati komunikaciju bez znanja korisnika ili administratora mreže.

Njuškanje (Eavesdropping): Njuškanje se odnosi na prisluškivanje komunikacije, ali se obično koristi u širem kontekstu van mreža, uključujući i fizičke lokacije gde se može fizički prisluškivati govor, razgovori ili druge vrste komunikacije. Na primer, njuškanje može uključivati prisluškivanje telefonskih razgovora, praćenje razgovora između ljudi ili bilo koju drugu aktivnost koja se neovlašćeno prati sa ciljem prikupljanja informacija. Njuškanje može ozbiljno ugroziti privatnost pojedinaca ili organizacija, posebno ako se koristi u kriminalne svrhe ili u cilju prikupljanja osetljivih informacija.

5. Šta je mehanizam kontrole pristupa?

Kontrola pristupa dozvoljava objektu proverenog identiteta da pristupi sistemu, tj. određuje ko ima pravo da pristupi resursima, i na kakav način. Ovom uslugom treba da se spreči zloupotreba resursa.

6. Objasniti razliku između privatnog i javnog ključa.

Asimetrična kriptografija koristi dva ključa – javni i privati ili tajni. Javni ključ koristi pošiljalac za šifrovanje poruke, dok privatni ključ koristi primalac da bi dešifrovao poruku. Prednost ovog načina šifrovanja je u tome što ne mora da se brine o načinu prenosa ključa.

7. Šta je IPS i koje su njegove funkcije?

IPS (Intrusion Prevention System) je sistem za prevenciju upada koji se koristi u oblasti bezbednosti informacionih sistema. Osnovna funkcija IPS-a je otkrivanje i blokiranje pokušaja neovlašćenog pristupa ili zlonamernih aktivnosti na mreži.

Osnovne funkcije IPS sistema su sledeće:

- ❖ identifikacija neovlašćenih aktivnosti na osnovu potpisa,

- identifikacija neovlašćenih aktivnosti na osnovu detektovanih anomalija,
- vođenje evidencije i/ili slanje upozorenja administratorima zaduženim za sigurnost u realnom vremenu,
- prikupljanje forenzičkih podataka o detektovanim napadima,
- sprečavanje napada.

8. Šta je virtuelna privatna mreža i koja je njena funkcija?

Virtuelna privatna mreža (VPN) je tehnologija koja omogućava sigurno povezivanje udaljenih računara ili mreža preko nesigurnih javnih mreža, poput interneta. Glavna funkcija VPN-a je stvaranje sigurne i enkriptovane veze između korisnika i resursa mreže, čime se osigurava privatnost, integritet podataka i sigurnost komunikacije.

Ključni aspekata funkcije VPN-a

- Enkripcija Saobraćaja
- Sigurno Povezivanje sa Udajmljenim Resursima
- Pristup Kontroli i Autentifikaciji:
- Sigurnost na Javnim Mrežama:
- Daljinsko Povezivanje i Rad na Daljinu

9. Koji su sigurnosni propusti u WEP standardu?

WEP je zastareli standard za sigurnost bežičnih mreža koji je prvobitno dizajniran da obezbedi sigurnost sličnu onoj u žičanim mrežama. Tokom vremena su otkriveniozbiljni sigurnosni propusti u WEP standardu, čineći ga ranjivim na napade. Glavni sigurnosni propusta u WEP standardu:

- Korišćenje Slabih Ključeva
- Problemi u Procesu Generisanja Ključeva
- Nedostatak Autentifikacije
- Bruteforce Napadi
- Nemogućnost Oporavka od Usporenih Ključeva:
- Slabost Integriteta Podataka

10. Objasniti B2B poslovanje i njegov uticaj.

B2B (Business-to-Business) poslovanje se odnosi na poslovne transakcije koje se odvijaju između dve kompanije, odnosno između poslovnih entiteta. Ovaj model poslovanja fokusiran je na pružanje proizvoda i usluga drugim preduzećima umesto direktnom prodajom krajnjim potrošačima. Uticaj B2B poslovanja je značajan jer igra ključnu ulogu u ekonomskom razvoju, omogućava efikasnu razmenu resursa i doprinosi razvoju inovacija u poslovnom sektoru.

11. Objasniti B2C poslovanje i njegov uticaj

B2C (Business-to-Consumer) poslovanje predstavlja model poslovanja gde kompanije direktno prodaju proizvode ili usluge krajnjim potrošačima. Ovaj model se često odvija putem online prodavnica, maloprodajnih lokacija ili drugih kanala koji omogućavaju direktnu interakciju između kompanije i pojedinca.

12. Objasniti C2C poslovanje i njegov uticaj

C2C (Consumer-to-Consumer) poslovanje predstavlja model poslovanja gde pojedinci direktno kupuju i prodaju proizvode ili usluge jedni drugima, obično putem online platformi ili drugih posredničkih sistema. Ovaj model omogućava pojedincima da budu i prodavci i kupci u isto vreme.

13. Objasniti C2B poslovanje i njegov uticaj

C2B (Consumer-to-Business) poslovanje predstavlja model poslovanja gde pojedinci (potrošači) nude proizvode, usluge ili informacije kompanijama, umesto da tradicionalno kompanije nude proizvode ili usluge potrošačima. Ovaj model se često pojavljuje u digitalnom okruženju.

14. Šta je bezbednosna politika jedne organizacije?

Sigurnosna politika je skup pravila, smernica i postupaka koji definišu na koji način informacioni sistem treba učiniti sigurnim. Sigurnosnom politikom definisana su pravila koja se odnose na celokupnu računarsku opremu institucije (hardver i softver), osobe odgovorne za administraciju informacionog sistema, sve zaposlene i korisnike sistema, odnosno osobe koje imaju pravo pristupa, spoljne saradnike (npr. ovlašćene radnike zadužene za održavanje sistema).

15. Navesti osnovne faze napada

- Ispitaj i proceni – Napadač posmatra sistem da bi utvrdio ranjivost
- Eksploatiši i prodri – Napadač pokušava da eksploatiše ranjivost i da prodre u mrežu ili sistem

- ❖ Povećaj privilegije – Kada uspe da uđe u sistem ili mrežu napadač će pokušati da poveća svoja prava
- ❖ Održi pristup – Napadač preduzima korake da prikrije tragove i da olakša buduće napade
- ❖ Odbij uslugu

16. Objasniti BLP model bezbednosti

BLP je razvijen u vojsci SAD radi regulisanja skladištenja i zaštite poverljivih podataka. Sprečavanje neovlašćenog pristupa poverljivim podacima je bio osnovni cilj razvoja ovog modela. Prema ovom modelu, svakom subjektu i svakom objektu je dodeljena bezbednosna klasa. Bezbednosne klase formiraju strogu hijerarhiju, koje se nazivaju bezbednosni nivoi. Bezbednosne klase kontrolišu način na koji subjekat može da pristupa objektu.

17. Šta je kriptoanaliza

Kriptoanaliza je disciplina koja se bavi analizom i dešifrovanjem šifrovanih podataka, tj. pokušava razbiti kriptografske sisteme kako bi otkrila originalne informacije koje su bile zaštićene šifrom. Cilj kriptoanalize je pronaći slabosti u algoritmima šifrovanja, ključevima ili implementacijama koje bi omogućile napadaču da prevaziđe zaštitu i pristupi poverljivim podacima.

18. Šta je hash funkcija i za šta se sve koristi

Hash funkcija generiše jedinsvetni kod za datoteku ili drugi podatak. Dodaje se na kraju poruke, korisnik koji prima poruku sa hash ponovo računa vrednost hash poruke i upoređuje te dve vrednosti. Hash funkcija je funkcija koja na osnovu poruke proizvoljne dužine generiše hash vrednost koja ima fiksnu dužinu, i koja služi kao autentifikator.

Postoje slabe hash funkcije I jake hash funkcije. Slabe hash funkcije zadovoljava prva 5 svojstva; Jaka hash funkcija zadovoljava 6 svojstva

19. Objasniti honeypot tehnologiju

Honeypot je zamka koja je postavljena da otkrije ili spreci pokusaj neovlascenog koriscenja informacionog sisitema. Honey pot ili lazni mamci su računari koji služe kao meta eventualnih napada. Oni služe da zaštite sistem od napada, tako što odvlače napadača, a administrator ima vremena da reaguje I zaštiti sistem ili I prikupi informacije o napadaču. Mamci sadrže informacije koje deluju kao važne I nisu dodatni zaštićeni.

20. Objasniti Authentication Header (AH)

AH obezbeđuje sigurnosne usluge provere identiteta, integriteta i neporecivosti IP paketa, ali ne može obezbediti privatnost. Protokolom je definisano AH zaglavlje koje se smešta između IP zaglavlja i podataka koji slede. Specifičnost AH je u tome što on, za razliku od ostalih TCP/IP protokola, ne enkapsulira podatke protokola kojima pruža uslugu.

21. Šta je SSL protokol, koje verzije postoje i za sta se sve koristi?

SSL je jedan od najkorišćenijih bezbednosnih protokola.Nalazi se između aplikacionog i transportnog sloja. SSL prima podatke, šifruje podatke i usmerava šifrovane podatke na TCP soket. SSL je zasnovan na metodama asimetričnog PKI šifrovanja. SSL služi da identifikuje dve strane povezane računarskom mrežom. SSL se nalazi između aplikacionog I transportnog sloja.

22. Objasniti kako funkcionise dinamičko ispitivanje paketa

Kod dinamičkog ispitivanja paketa proveravaju se informacije paketa i zapisi o TCP vezama. Kada program koji koristi TCP kreira sesije sa udaljenim hostom, on kreira TCP vezu u kojoj je broj TCP port za udaljenu (server) aplikaciju broj manji od 1024, a broj TCP port za lokalnu (klijent) aplikaciju je broj između 1024 i 65535. Brojevi manje od 1024 su "poznati" port brojevi i dodijeljeni su trajno određenim

23. Bezbednost mobilnih mreza

Bezbednost mobilnih mreža je ključna oblast fokusirana na zaštitu podataka i uređaja u okviru mobilnih komunikacija. Ova oblast obuhvata niz mera koje se primenjuju kako bi se osiguralo da korisnici mobilnih uređaja imaju sigurnu i privatnu komunikaciju. Ključni aspekti uključuju enkripciju podataka kako bi se obezbedila poverljivost, autentifikaciju korisnika kako bi se sprečio neovlašćeni pristup, zaštitu od malvera radi očuvanja integriteta sistema, i implementaciju sigurnosnih protokola u mobilnim mrežama.

24. Objasniti lokalni domen naloga i Windows privilegije

Lokalni nalozi postoje na svakom Windows računaru i služe za proveru identiteta korisnika na tom računaru i kontrolu pristupa resursima tog računara. Administriraju se pomoću Computer Management alata. Kada je računar pridružen preko domena, korisnici mogu pristupiti tom računaru korišćenjem domen naloga.Oni se mogu prijaviti korišćenjem lokalnih naloga, ali

lokalni nalozi možda nemaju sve privilegije koje bi želeli. Privilegije su dozvole na nivou sistema dodeljenih korisničkom nalogu.

25. Koje vrste zaštitne barijere (engl. firewall) postoje?

Postoji tri tipa mrežnih zaštitnih zidova:

- ❖ filtriranje paketa
- ❖ mrežni prolazi aplikativnog nivoa
- ❖ prolazi na nivou kanala komunikaciskih podataka.

26. Šta je slojevita zaštita i kako se koristi?

Slojevita zaštita predstavlja koncept bezbednosti koji se oslanja na implementaciju više nivoa sigurnosnih mera kako bi se zaštitili sistemi i podaci. Ovaj pristup je usmeren na stvaranje višestrukih barijera, tako da eventualni napad na jednom nivou ne dovodi do potpunog kompromitovanja sistema.

27. Šta je ranjivost i koja je razlika izmedju ranjivosti i pretnje?

Ranjivost se odnosi na slabosti u sistemu koje omogućava napadaču da naruši integritet tog sistema. Ranjivost može biti softverska, usled konfigurisanja, u sigurnosnoj arhitekturi. Ranjivost može biti rezultat slabog korisničkog imena, greške u programu , virusa ili drugih zlonamernih programa, ubačenog skript koda.

Pretnja je potencijal za kršenje bezbednosti, koji postoji kada imamo okolnost, pogodnost, radnju ili događaj koji bi mogli izazvati kršenje bezbednosti i štetu; to jest, pretnja je moguća opasnost sa namerom da se iskoristi ranjivost sistema.

28. Za šta se koristi Diffle-Hellman algoritam, objasniti?

Diffle-Hellman je algoritam koji služi da omogući korisnicima da sigurno razmenjuju tajni ključ koji se koristi za šifrovanje naknadnih poruka. Ukratko ovaj algoritam se koristi za zaštićeni prenos ključeva.

29. Objasniti tehnologiju digitalnog koverte (envelope).

Digitalna koverta se koristi kako bi zaštitile poruke bez potrebe organizovanja da pošiljalac i primalac imaju isti tajni ključ.Razlog zbog čega se naziva digitalna koverta je što je slična zatvorenoj koverti sa nepotpisanim pismom. Koristi se šifrovanje javnim ključem za zaštitu simetričnog ključa.

30. Objasniti razliku izmedju IPS i IDS sistema.

Glavna razlika je da IPS može proaktivno blokirati napad, a IDS može analizirai i oceniti saobraćaj, ali ga ne može zausaviti. IDS sistemi su fokusirani na to kako se napad izvodi, a IPS na to šta napad radi.

31. Koje se tehnologije koriste u Virtualnim privatnim mrežama (navesti dva protokola)?

U Virtualnim privatnim mrežama (VPN), dva često korišćena protokola su:

IPsec (IP Security): IPsec je set protokola za sigurnu komunikaciju na Internetu. Koristi se za obezbeđivanje privatne komunikacije putem internetske mreže, pružajući autentifikaciju, integritet podataka i šifrovanje.

OpenVPN: OpenVPN je open-source softver koji se koristi za uspostavljanje VPN veza. On koristi kombinaciju SSL/TLS protokola za obezbeđivanje sigurne veze.

32. Objasniti proces ojačanja Linux sistema?

Ojačavanje Linux sistema podrazumeva primenu različitih bezbednosnih mera kako bi se smanjila ranjivost sistema. Ključni koraci u ovom procesu uključuju redovno ažuriranje sistema, upravljanje korisničkim nalozima, konfiguraciju firewall-a, fizičku sigurnost, enkripciju podataka, auditing, ograničavanje servisa, postavljanje sigurnosnih politika, kontrolu pristupa i redovne sigurnosne provere. Ovi koraci doprinose jačanju zaštite sistema od potencijalnih pretnji i neovlašćenog pristupa.

33. Objasniti šta je kompromitovani računar?

Kompromitovani računar je računar koji je pogođen bezbednosnim pretnjama ili napadima i čiji su resursi, podaci ili funkcionalnosti ugroženi ili zloupotrebljeni od strane neovlašćenog korisnika ili zlonamernog softvera. Kompromitovanje računara može rezultirati gubitkom poverljivosti, integriteta ili dostupnosti podataka, kao i mogućnošću da napadač preuzme kontrolu nad sistemom. Ovakvi napadi mogu uključivati različite tehnike, poput virusa,, phishinga, napada sajber-kriminalaca ili drugih pretnji koje mogu dovesti do oštećenja računarskih sistema ili krađe informacija. Kompromitovanje računara često zahteva

implementaciju odgovarajućih bezbednosnih mera kako bi se sprečile ili minimizovale potencijalne posledice.

34. Kakva je razlika izmedju tradicionalnog i LIVE sakupljanje dokaza?

Razlika između tradicionalnog i LIVE sakupljanja dokaza u oblasti digitalne forenzike odnosi se na vreme i način prikupljanja elektronskih dokaza:

Tradicionalno sakupljanje dokaza: Obično se sprovodi nakon što je sistem zatvoren ili isključen. Računar se fizički izdvaja iz mreže ili se onemogućava pristup njegovim resursima. Prikupljanje dokaza se vrši na statičan način, gde se kopija podataka pravi s fizičkog diska ili drugih uređaja koji se zatim analizira. Mogućeje dobiti detaljne informacije o stanju sistema u trenutku zatvaranja, a analiza se može izvršiti bez aktivnog rada na računaru.

LIVE sakupljanje dokaza: Prikupljanje se vrši dok je sistem još uvek aktivan i u upotrebi. Prikupljanje se vrši tokom rada operativnog sistema. Ova metoda omogućava prikupljanje podataka o trenutnom stanju sistema, otvorenim aplikacijama, aktivnim vezama i drugim parametrima. Prednost je mogućnost prikupljanje podataka u realnom vremenu, što je korisno za analizu događaja koji se dešavaju tokom aktivnog korišćenja sistema.

35. Koje vrste ranjivosti postoje?

Ranjivost se odnosi na slabosti u sistemu koje omogućava napadaču da naruši integritet tog sistema. Ranjivost može biti softverska, usled konfigurisanja, u sigurnosnoj arhitekturi. Ranjivost može biti rezultat slabog korisničkog imena, greške u programu , virusa ili drugih zlonamernih programa, ubačenog skript koda.

Ranjivosti sigurnosne arhitekture su:

- ❖ Skriveni kanal,
- ❖ Nepostojanje provere perimetra,
- ❖ Maintenance hok ranjivost
- ❖ Time of check to time of use

36. Šta je Digitalna koverta a Šta digitalni potpis email dokumenta?

Digitalna koverta se koristi kako bi zaštitile poruke bez potrebe organizovanja da pošiljalac i primalac imaju isti tajni ključ.Razlog zbog čega se naziva digitalna koverta je što je slična zatvorenoj koverti sa nepotpisanim pismom. Koristi se šifrovanje javnim ključem za zaštitu simetričnog ključa.

Digitalni potpis se dodaje ili pridružuje elektronskim porukama ili dokumentima i služi kao metod za identifikaciju pošaljioca. Svrha digitalnog potpisa je da potvrdi autentičnost sadržaja poruke tj. dokaz da poruka nije promenjena na putu od pošiljaoca do primaoca, kao i da obezbedi garantovanje identiteta pošiljaoca poruke.

37. Objasniti IDS baziran na mreži

Mrežni IDS prati saobraćaj u odabranim tačkama na mreži ili u skupu povezanih mreža. Na raspolaganju su im baze podataka sa parametrima poznatih napada. Pregleda paket po paket u realnom vremenu i tako pokušava da otkrije na koj način je moglo da da dođe do upada. Ako se pronađe pokapanje sa postojećim modelima aktivnosti u bazi, mrežni IPS sistem salje upozorenje administrator ili pokušava da blokira napad u ranoj fazi. Mrežni IDS može ispitati vrednosti na mrežnom, transportnom ili aplikativnom nivuo.

38. Objasniti IDS zasnovan na hostu

IDS zasnovan na hostu pruža sloj bezbednosnog softvera za ugrožene ili osetljive sisteme, koji prati aktivnosti na sistemu sa ciljem da otkrije sumnjivo ponašanje. On proverava integritet sistema i nadgleda najvažnije sistemske datoteke.

Može da zaustavi napad pre nego dođe do štete, mada je njegova osnovna svrha da otkrije upad, šalje upozorenje i prijavi sumnjive događaje.

Glavna njegova prednost je da se može otkriti i spoljašnji i unutrašnji upad.

39. Obajsniti IPSec protokol

IPsec (Internet Protocol Security) je skup protokola i standarda za obezbeđivanje sigurne komunikacije na Internetu. Ovi protokoli se koriste za pružanje sigurnosnih usluga, uključujući enkripciju, autentifikaciju i zaštitu integriteta podataka na nivou IP sloja. IPsec se često koristi za izgradnju tzv. "virtualnih privatnih mreža" (VPN). Glavne komponente su:

AH (Authentication Header),ESP (Encapsulating Security Payload), IKE (Internet Key Exchange)

40. Šta je kerberos protokol i za šta se koristi?

Kerberos je protokol za proveru identiteta korisnika. Kerberos poseduje bazu, server za proveru identitea i server za izdavanje karata. Kerberos zahteva da koristik dokaže identitet prilikom svakog povezivanja, a može i od servera zahtevati da dokaže svoj identitet klijentima. Koristi se

za prijavljaivanje korisnika samo jednom i posle prijavljivanja korisnici imaju pristup resursima u sistemu za koje su ovlašćeni.

41. Objasniti Linux modele bezbednosti

Linux operativni sistem koristi modele bezbednosti kako bi kontrolisao pristup resursima i obezbedio integritet sistema. Dva glavna modela bezbednosti koja se često koriste u Linux-u su:

- ❖ DAC (Discretionary Access Control) – DAC je model bezbednosti koji omogućava vlasnicima resursa da određuju ko može pristupiti tim resursima i koje privilegije korisnici imaju na njima.
- ❖ MAC (Mandatory Access Control) – MAC je model bezbednosti koji daje centralnu kontrolu nad pravima pristupa, nezavisno od vlasnika resursa.

42. Navesti lokacije zaštitnih zidova

Spoljni zaštitni zid je smešten na ivici lokalne ili mreže firme.
Jedan ili više unutrašnjih zaštitnih zidova štite većinu mreže firme.
Jedan ili više umreženih uređaja u regionu se pominju kao DMZ (demilitarizovana zona) mreže.

43. Objasniti kako funkcioniše bezbednost mobilne trgovine i digitalnog novca

Bezbednost mobilne trgovine i digitalnog novca obuhvata niz mera koje su usmerene ka zaštiti ličnih i finansijskih informacija korisnika. Ključne tačke uključuju:

- ❖ Enkripcija podataka: Zaštititi prenos osetljivih informacija između uređaja i servera enkripcijom, koristeći protokole poput TLS ili SSL.
- ❖ Višestruki faktori autentifikacije: Koristiti dodatne autentifikacione korake.
- ❖ Zaštita od pretnji: Implementirati mehanizme zaštite od malvera, phishinga i drugih pretnji kako bi se očuvala bezbednost mobilnih aplikacija i digitalnih novčanika.
- ❖ Sigurnost plaćanja: Osigurati sigurnost transakcija kroz bezbedne platne gateway-e, tokenizaciju podataka i procese autorizacije plaćanja.
- ❖ Sigurnost mobilnih uređaja: Korisnici trebaju preduzeti korake poput postavljanja lozinki, korišćenja zaključavanja ekrana i redovnog ažuriranja softvera kako bi očuvali bezbednost svojih mobilnih uređaja.
- ❖ Politike privatnosti i regulative: Pridržavati se zakona o privatnosti i regulativa kako bi se zaštitila prava korisnika u vezi s rukovanjem njihovim podacima.
- ❖ Redovno nadgledanje i praćenje: Aktivno nadgledati i analizirati sigurnosne događaje kroz sisteme nadzora i beleženja radi prepoznavanja i odgovora na potencijalne pretnje

44. Objasniti AES algoritam

AES algoritam koristi promenljivu dužinu ključa 128, 192 ili 256 bitova , kao i promenljivu dužinu bloka 128, 192 ili 256 bitova.Najčešće korišćena dužina ključa je 128 bitova. Ovaj algoritam ima simetričnu i paralelnu struktura, kao i pogodnost za moderne procesore.Zasniva se na algoritmu Rijndael.

45. Obajsniti kako se vrši provera verodostojnosti poruke

To se čini digitalnim potpisom.Korisnik koji pošalje poruku ili izmeni neki podatak ne može kasnije poreći da on to nije uradio. Kada je poruka poslata, primalac može da dokaže da je pošiljalac poslao poruku. Isto tako kada je poruka uručena, pošiljalac može da dokaže da je primalac primio poruku.Cilj ove usluge je da obezbedi neoboriv dokaz koji omogućava brzo rešavanje sporova.

46. Objasniti bezbednost transportnog sloja

SSL (Secure Sockets Layer) obezbeđuje mehanizme za identifikaciju dva sagovornika povezana računarskom mrežom i zaštićeni prenos između njih.Zasnovan je na PKI šifrovanju.Ovaj sloj se nalazi između aplikacionog i transportnog sloja.Na predanoj strani,podaci prolaze kroz SSL sloj,zatim se šifruju i usmeravaju na TCP.Na prijemnoj strani SSL čita podatke iz TCP-a,dešifruje ih i preusmerava ka aplikaciji. Ako je server obezbeđen sa SSL slojem, URL za stranicu je https://. Koristi RSA algoritam.

47. Objasniti kako funkcioniše bezbednost elektronskih sistema plaćanja

- ❖ Autentifikacija plaćanja - kupac i prodavac moraju dokazati identitete plaćanja
- ❖ Integritet plaćanja – podatke o transakciji ne može modifikovati neautorizovani korisnik. Podaci sadrže identite kupaca i prodavaca, sadržaj kupovine i iznos.
- ❖ Autorizacija plaćanja – novac se ne može preuzimati sa računa potrošača ili smart kartice bez dozvole.
- ❖ Tajnost plaćanja - pokriva poverljivost transakcionih podataka.