**Q1**

1. Neporicanje kao bezbednosna usluga obezbeđuje?
   1. celovitost podataka
   2. da korisnik koji pošalje poruku ne može kasnije poreći da je to uradio
   3. da ovlašćeni korisnici imaju pristup podacima i računarskim resursima kada su im potrebni
   4. da se podaci neautorizovano ne menjaju ili uništavaju
   5. pristup informacijama samo za one korisnike koji su ovlašćeni da tim informacijama pristupe
2. Bezbednosni ciljevi predstavljaju ciklus četiri faze?
   1. poverljivost, integritet i raspoloživost
   2. procena, prevencija, raspoloživost i odgovor
   3. prevencija, detekcija, celovitost i odgovor
   4. procena, prevencija, detekcija i odgovor
   5. privatnost, sigurnost, poverljivost, raspoloživost
3. Zahtev da samo ovlašćeni korisnici mogu da menjaju podatke naziva se?
   1. Provera identiteta
   2. Raspoloživost
   3. Neporicanje
   4. Kontrola pristupa
   5. Integritet T
4. U kojoj fazi napadač odlučuje koje resurse će napasti?
   1. ispitaj i proceni
   2. odbij uslugu
   3. održi pristup
   4. eksploatiši i prodri
   5. povećaj privilegije
5. Odobrenje pristupa na određeni način jednom ili više objekata je?
   1. funkcija pristupa
   2. sesija
   3. lista prava
   4. dozvola ili pravo pristupa
   5. uloga
6. Kome se dodeljuje sigurnosna oznaka u mehanizmu kontrole pristupa?
   1. dodeljuje se nekom pravu pristupa
   2. dodeljuje se nekom resursu
   3. dodeljuje se nekom procesu
   4. dodeljuje se nekoj ulozi
   5. dodeljuje se nekom subjektu
7. Kako se nazivaju algoritmi kod kojih se originalna poruka šifruje po grupama (blokovima)?
   1. blokovska šifra
   2. supstitucija
   3. transpozicija
   4. šifra toka
   5. jednokratna beležnica
8. Jednosmerna funkcija za autentifikaciju poruke koja ne uključuje korišćenje tajnog ključa za generisanje malog bloka podataka, poznatog je kao ?
   1. kod za autentifikaciju
   2. digitalno potpis T
   3. hash funkcija
   4. šifrovanje
9. Kako se naziva pravno lice koje izdaje elektronske sertifikate u skladu sa odredbama zakona o digitalnom potpisu?
   1. sertifikaciono telo
   2. elektronski sertifikat
   3. digitalni potpis
   4. kvalifikovani elektronski sertifikat
10. Čiji cilj je da dobije pristup sistemu ili da poveća nivo privilegija na sistemu?
    1. uljeza
    2. pošiljaoca
    3. primaoca
    4. legitimnog korisnika T
    5. crva

**Q2**

1. Detekcija uljeza zasniva se na pretpostavci?
   1. da se ponašanje uljeza ne razlikuje od legitimnog korisnika na način koji se može kvantifikovati
   2. da se ponašanje uljeza razlikuje od legitimnog korisnika na način koji se može kvantifikovati
   3. da je ponašanje uljeza definisano modelom ponašanja prethodnih napada
   4. da je ponašanje uljeza predvidljivo
   5. da se ponašanje uljeza može detektovati hardverom
2. Ko beleži svaki audit zapis generisan od strane audit sistema za kolekciju?
   1. menadžer
   2. podsistem za upozoravanje
   3. agent
   4. analizator
   5. Operater
3. Utvrđeni (bastion) host je sistem identifikovani od strane zaštitnog zida administratora kao?
   1. slaba kritična tačka
   2. „uska grla” između unutrašnjih i spoljnih mreža
   3. jaka kritična tačka
   4. prolazna tačka
   5. tačka za audit
4. Šta obezbeđuje AH protokol sigurnosti na mrežnom sloju Interneta?
   1. poverljivost
   2. autentifikaciju i integritet podatak T
   3. kontrolu identiteta
   4. autentifikaciju, integritet podataka i poverljivost
   5. autentifikaciju i kontrolu identiteta
5. Koja dva tipa upravljanja ključem određuje IPSec arhitektura dokumenta?
   1. transportno i automatsko T
   2. tunelski i automatsko
   3. fizičko i tunelski
   4. fizičko i transportno – treba automatsko
6. IPSec je skup protokola koji omogućava bezbednost na?
   1. Gateway
   2. Transportnom sloju
   3. Zaštitnom zidu
   4. Mrežnom sloju
   5. Aplikativnom sloju
7. Na kom algoritmu šifrovanja je zasnovan SSL protokol?
   1. SHA
   2. Simetričnom
   3. DSS
   4. Asimetričnom
   5. MAC

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

* 1. S/MIME
  2. TLS
  3. SSL
  4. Kerberos
  5. IP/IPSec

1. Koji je bezbednosni protokol u IEEE802.11 bežičnim lokalnim mrežama?
   1. IPsec
   2. Bluetooth
   3. WEP
   4. WPA2
   5. WPA
2. Koja dužina ključa za WEP protokol je definisana standardom IEE 802.11?
   1. 40 bita
   2. 128 bita T
   3. 56 bita
   4. 152 bita
   5. 104 bita

**Q3**

1. Protokol IEEE802.11i pored bežičnog klijenta i pristupne tačke AP definiše?
   1. WEP, EAP ključ
   2. server za proveru identiteta
   3. passkey, ključ sesije
   4. dinamičko definisanje ključa šifrovanja
   5. upareni glavni i privremeni ključ
2. Šta na Unix sistemu nije predstavljeno kao datoteka?
   1. objekti i grupe
   2. grupe i akcije
   3. korisnici i grupe
   4. korisnici i objekti
   5. korisnici i akcije
3. Šta obuhvata ranjivost Linux standardnih distribucija?
   1. prekoračenje bafera, problemi sinhronizacije (race), DoS napad, ranjivost Web aplikacija, napad rootkit
   2. korisnik ili proces sa root privilegijama
   3. prostor Linux jezgra i prostor svih ostalih servisa
   4. prekoračenje bafera, DoS, neograničena kontrola pristupa
   5. DoS napad, ranjivost Web aplikacija, kontrola pristupa zasnovana na ulogama
4. U kojoj datoteci su definisane grupe?
   1. /etc/shadow
   2. /etc/secure
   3. /etc/passwd
   4. /etc/root
   5. /etc/group
5. Koji model elektronske trgovine je danas dominantan na internetu?
   1. Consumer to Consumer (C2C)
   2. Consumer to Business (C2B)
   3. Business to Employee (B2E)
   4. Business to Consumer (B2C)
   5. Business to Business (B2B)
6. U kom modelu je on-line aukcija jedna od mogućnosti on-line kupovine?
   1. Business to Business (B2B)
   2. Consumer to Consumer (C2C) t
   3. Consumer to Business (C2B)
   4. Business to Consumer (B2C)
7. Kako se naziva plastična kartica sa ugrađenim mikroprocesorom i memorijom?
   1. digitalni ček
   2. elektronski ček
   3. elektronski novac
   4. elektronska kreditna kartica
   5. smart kartica
8. Pojedini napadi koriste obične ljudske mane radi ostvarivanja pritupa koji su inače zabranjeni. Kako se nazivaju takvi napadi?
   1. IDS sistem
   2. spoljašnje obezbeđenje
   3. socijalni napadi
   4. biometrija
   5. CHAP identifikator
9. Kako se naziva lista formatiranih zapisa događaja?
   1. audit arhiver
   2. bezbednosni audit tragovi
   3. audit zapis
   4. audit provajder
   5. audit analizer
10. Koji log fajl sadrže informacije o validnim i ne validnim pokušajima logovanja kao i događaje koji regulišu korišćenje resursa?
    1. security log
    2. appliction log
    3. mrežni log
    4. system log

**Q4**

**1. Koje vrste ranjivosti postoje?**

U kompjuterskoj bezbednosti, termin ranjivost se odnosi na slabosti u sistemu koje omogućava napadaču da naruši integritet tog sistema. Ranjivost može biti rezultat slabog korisničkog imena, greške u programu (eng. software bugs), virusa ili drugih zlonamernih programa, ubačenog skript koda.

Softverska ranjivost:

Ranjivosti  usled konfigurisanja

Ranjivosti u sigurnsosnoj arhitekturi

Linux ranjivosti standardnih distribucija

1. **Objasniti AES algoritam**

AES algoritam može da koristiti promenljivu dužinu ključa (128, 192 ili 256 bitova), kao i promenljivu dužinu bloka (128, 192 ili 256 bitova). Najčešće implementirana dužina ključa je 128 bitova. AES standard postoji u dve varijante: 128-bitni blok sa 128-bitnim ključem i 128-bitni blok sa 256-bitnim ključem. Prednosti ovog algoritma su simetrična i paralelna struktura, realizacija na modernim procesorima, specijalizovanom hardveru ili u pametnim karticama. Vrlo je važno napomenuti da je pojava slabih ključeva kod ovog algoritma nemoguća

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

Cilj algoritma je da omogući korisnicima da sigurno razmenjuju tajni ključ koji zatim mogu da koriste za šifrovanje poruka. Efikasnost algoritma zavisi od težine računanja diskretnog logaritma. Sigurnost algoritma leži u činjenici da dok je lako izračunati eksponent po modulu prostog broja, to je vrlo teško izračunati diskretni logaritam.

**4. Sta je Digitalna koverta a sta digitalni potpis email dokumenta?**

Digitalna koverta se koristi kako bi zaštitila poruke bez potrebe da pošiljalac i primalac imaju isti tajni ključ. To je ekvivalent zatvorenoj koverti sa nepotpisanim pismom. Koristi se šifrovanje javnim ključem za zaštitu simetričnog ključa.

Digitalni potpis je elektronska sigurnosna oznaka koja se može dodati datotekama. Ona omogućava proveru identiteta izdavača datoteke, kao i proveru je li datoteka menjana otkako je digitalno potpisana. Ako datoteka nema valjani digitalni potpis, ne možete biti sigurni da li potiče iz navedenog izvora, i da li je neko zlonamerno menjao.

1. **Objasniti IDS zasnovan na hostu**

IDS zasnovan na hostu (engl. Host-based IDS ) prati aktivnosti na sistemu na razne načine sa ciljem da otkrije sumnjivo ponašanje. IDS/IPS sistema proverava integritet sistema, nadgleda status najvažnijih sistemskih datoteka. IDS može biti u mogućnosti da zaustavi napad pre nego je učinjena šteta, mada je njegova osnovna svrha da otkrije upad, prijavi sumnjive događaje i šalje upozorenje (engl. alerts ). Glavna prednost IDS zasnovanog na hostu je da može otkriti i spoljašnji i unutrašnji upad, što nije moguće sa IDS zasnovanom na mreži ili mrežnom barijerom (engl. firewall).

**6. Obajsniti kako se vrši provera verodostojnosti poruke**

Vernost ili autentičnost originalnog sadržaja (autentifikacija poruke) poruka je bezbednosni mehanizam koji se koristi za proveru integriteta poruka tj., da primljena poruka ne sadrži modifikacije, dodate delove, ili da su neki delovi izbrisani. Po definiciji, kompletna autentičnost poruke se odnosi na:

• Autentičnost sadržaja

• Autora-pošiljaoca poruke

Bilo da je reč o autentifikaciji sadržaja ili pak autora poruke, mehanizam za autentifikaciju se sastoji od dve elementarne komponente:

• na nižem nivou nalazi se algoritam predstavljen funkcijama koje generišu i analiziraju autentifikacione podatke ili autentifikator

• na višem nivou nalazi se protokol za autentifikaciju, kojim se definiše upotreba, tj. obrada autentifikatora kako bi primalac bio u stanju da proveri autentičnost.

**7. Sta je kerberos protokol i za sta se koristi?**

Kerberos je jedan od najpoznatijih protokola za proveru identiteta korisnika. Ime je dobio po Kerberu, zato što centar za distribuciju ključeva, poput mitskog bića, ima tri „glave“: bazu, server za proveru identiteta i server za izdavanje karata. Jedna od najznačajnijih prednosti protokola Kerberos jeste takozvano prijavljivanje tipa „prijavi-se-samo-jednom“ (engl. Single Sign On), koje korisnicima omogućava da se samo jednom prijave na sistem i da nakon toga, u skladu sa svojim ovlašćenjima, imaju pristup svim resursima u sistemu (ili mreži).

**8. Objasniti bezbednost transportnog sloja**

Pretraživač i server startuju SSL protokol kako bi proverili spremnost za prenos. Nakon toga, autentifikuje se server i generiše simetrični ključ. U ovim koracima se koristi RSA tehnologija javnih ključeva. Kada se uspostavi sinhronizacija sa serverom, svi podaci koji se šalju preko TCP konekcije između pretraživača i servera, šifrovani su pomoću simetričnog ključa sesije. TLS format zapisa je jednak formatu SSL zapisa, razlika je samo u vrednosti polja za verziju.

**9. Navesti lokacije zaštitnih zidova**

Zaštitni zid je postavljen da obezbedi zaštitnu barijeru između spoljašnjeg, potencijalno nepoverljivog izvora saobraćaja i interne mreže. Spoljni zaštitni zid je smešten na ivici lokalne ili mreže preduzeća. Jedan ili više internih zaštitnih zidova štite većinu mreže preduzeća.

**10. Objasniti kako funkcioniše bezbednost elektronskih sistema plaćanja**

Elektronska trgovina se realizuje uz pomoć skupa tehnologija i procedura koje automatizuju poslovne transakcije putem elektronskih sredstava. Postoje online i offline elektronski sistemi plaćanja.

U offline sistemu, kupac i prodavac su online u toku novčane transakcije, ali nemaju elektronsku konekciju sa svojim bankama. U ovom scenariju kupac nema mogućnost da zahteva autorizaciju od svoje banke i proveri mogućnost plaćanja. Zbog toga su online sistemi bezbedniji, ali zahtevaju više komunikacionih resursa.

Glavni promoteri PCI DSS (Payment Card Industry Data Security Standard) standarda su Visa i Master Card International.

Bezbednosni problemi tradicinalnih sistema plaćanja su falsifikovanje novca i potpisa, i višestruko izdavanje čekova.

Osnovni bezbednosni zahtevi elektronskih sistema plaćanja su:

• Autentifikacija plaćanja

• Integritet plaćanja

• Autorizacija plaćanja

• Tajnost plaćanja

**Q5 pr**

* **Objasniti ulogu Forward, Input, Output chain-a?**

INPUT chain se koristi za sve pakete koji uđu u sistem.

OUTPUT chain je za svaki paket koji napušta sistem. A

FORWARD chain je za pakete koji se prosleđuju (preusmeravaju) kroz sistem.

* **Koja je uloga FILTER tabele?**

Tabela FILTER koristi se za filtriranje paketa. Tablica filtera u iptables ima tri chain-a (skupa pravila) Input ,Forward i Output.

* **Korišćenjem iptables blokirati dolazni saobraćaj sa adrese 10.15.1.1.**

iptables -A INPUT -s 10.15.1.1 -j DROP

* **Korišćenjem iptables blokirati odlazni i dolazni saobraćaj prema/sa mreže 192.168.11.0/24.**

iptables -I INPUT -s 192.168.11.0 --dport 24 -j DROP

iptables -I OUTPUT -d 192.168.11.0 --dport 24 -j DROP

* **Korišćenjem iptables dozvoliti dolazne tcp i udp pakete na portu 81 i 3306, i blokirati ostale portove.**

iptables -I INPUT 1 -m udp -p tcp -j DROP

iptables -I INPUT 1 -m udp -p tcp --dport 81 -j ACCEPT

iptables -I INPUT 1 -m udp -p tcp --dport 3306 -j ACCEPT

* **Korišćenjem iptables blokirati sve dolazne konekcije, i jedino dozvoliti konekcije na portu 465, 587 i 995.**

iptables -A INPUT -p tcp -m tcp -m multiport ! --dports 465,587,995 -j DROP

* **Obrisati pravilo koje zabranjuje dolazni saobraćaj sa adrese 10.20.11.0/24.**
* **Napisati iptables pravila koja dozvoljavaju jedino odlazni POP3 i SMTP saobraćaj, dok je sav ostali saobraćaj blokiran.**
* **Napisati iptables pravila koja jedino dozvoljavaju ping na INPUT-u i OUTPUT-u.**
* **Napisati komandu kojom se brišu deveto pravilo u imput tabeli .**

**Q6**

* **iptables -A INPUT -s 89.216.56.0/255.255.255.0 -i eth0 -p udp -m udp --dport 135:139 –j ACCEPT**

Komanda oznacava dodavanje novog pravila u lancu pravila cija izvorisna adresa nije raslicita od one navedene, sa interfejsa eth0, preko udp porta gd3 je odredisni port izmedju 137 i 139

* **iptables -A INPUT -s !161.53.9.70 -p udp -m udp --dport 123 -j DROP**

**Komanda oznacava odbijanje ovog pravila u lancu cija izvorsna adresa nije razlicita od one navedene, preko udp porta gde je odredisni port 123**

* **iptables -A INPUT -s 161.11.77.235 -i eth0 -p tcp -m tcp --dport 25, 465 -j ACCEPT**

komanda oznacava dodavanje novog pravila u lancu pravila cija izvorisna adresa nije raslicita od one navedene, sa interfejsa eth0, preko udp porta gd3 je odredisni port izmedju 137 i 13

* **iptables -A INPUT -i ppp0 -m state -- state NEW, ESTABLISHED -j ACCEPT**

to je dodavanje novog pravila na inteferjsu ppp0, gde se dozvoljava propustanje paketa sa  stanjem novi i uspostavljen

* **iptables -A FORWARD -i ppp0 -m state -- state NEW, RELETED -j DROP**

to je dodavanje novog pravila na inteferjsu ppp0, gde se zabranjuje(paketi se uništavaju) propuštanje paketa sa stanjem novi i povezani sa već postojećom konekcijom(FTP, ICMP..)

**Q7**

* **Kojim ključem se vrši digitalno šifrovanje i potpisivanje poruke. Opisati postupak?**

PKCS#1 je standard šifrovanja podataka korišćenjem RSA asimetričnog algoritma najčešće se koristi za digitalne koverte i digitalne potpise.Kod I digitalnog potpisa, sadržaj koji treba da se potpiše prvo se redukuje (na primer, MD5 ili SHA-1), a zatim se šifruje primenom, na primer, RSA algoritma, koristeći privatni ključ potpisnika poruke. Šifrovani otisak poruke predstavlja digitalni potpis date poruke i postaje njen pridruženi deo. Kada ovakva poruka stigne do primaoca kojem je namenjena, izvršava se postupak verifikacije digitalnog potpisa. Ovaj postupak se sastoji od dešifrovanja izvoda dobijene poruke primenom RSA algoritma, uz upotrebu javnog ključa pošiljaoca poruke.

* **Napisti komandu za generisianje ključeva na linux sistemu za GPG.**

gpg – full-gen-key

* **Napsiati snort pravila za detekciju dolaznog TCP sobraćaja na odredišnim portovima 22 i 80, koje daje poruku da je došlo do detekcije saobraćaja na datim portovima i blokira saobraćaj sa odredišnih adresa?**
* **Na linux sistemu šta se nalazi u /etc/passwd a šta u /etc/shadow datoteci?**

*/etc/passwd* - je baza podataka koja sadrži sve korisničke naloge Linux sistema.

*/etc/shadow* - U datoteci/etc/shadow se nalazi stvarna lozinka u šifrovanom formatu za svaki nalog sa dodatnim informacijama o lozinci. Svako polje je odvojeno od susednog polja simbolom (:). Datoteka /etc/shadow sadrži jedan red za svakog korisnika koji je naveden u datoteci /etc/ passwd. /etc/pasword

* **Koristeći ACL ukloniti sve privilegije za korisnika it381 na fajlu IT381?**

setfacl -x u:it3881\_korisnik:-r home/ IT381/private/

**BLANKETI B**

**Q1**

1. Koji način plaćanja je najpopularniji?
   1. plaćanje samo debitnim karticama
   2. plaćanje debitnim karticama i homebanking
   3. plaćanje debitnim i kreditnim karticama
   4. homebanking
   5. plaćanje kreditnim karticama i homebanking
2. Kako se naziva skup bezbednosnih protokola i formata koji omogućava korisnicima da plaćaju kreditnom karticom na otvorenoj mreži, na siguran način?
   1. digitalni sertifikat
   2. Payment gateway
   3. sertifikaciono telo
   4. SET (Secure Electronic Transaction)
   5. privatnost plaćanja
3. Kako se naziva osoba ili organizacija koja prodaje robu ili usluge koje mogu da se plate karticom?
   1. Payment gateway
   2. dobavljač
   3. vlasnik kartice
   4. izdavač
   5. trgovac
4. Koja tema bezbednosne politike uključuje kontrolu pristupa i zahtevano prijavljivanje na sistem?
   1. softver
   2. principi
   3. operativni sistemi
   4. sigurnost komunikacije
   5. zaštita podataka
5. Šta predstavlja algoritam sa svim mogućim otvorenim tekstovima, šifratima i ključevima?
   1. dešifrovanje
   2. kriptografski algoritam
   3. kriptografski sistem
   4. šifrovanje
6. Zamena međusobnog položaja elemenata otvorenog teksta, tj. otvoren tekst se ne menja, menja se samo međusobni položaj elemenata otvorenog teksta je?
   1. transpozicija
   2. jednokratna beležnica
   3. šifra toka
   4. blokovska šifra
   5. supstitucija
7. Ko određuje kojim sistemima je dozvoljeno da komuniciraju međusobno i jednokratan obezbeđuje ključ sesije za komunikaciju?
   1. javni ključ
   2. modul bezbednosnih usluga
   3. stalni ključ
   4. centar za distribuciju ključeva (KDC)
   5. master ključ
8. Koji algoritam je izabran kao standardni MAC alat za IPS, TLS i SET protokole?
   1. HMAC
   2. SHA
   3. MD5
   4. DSS

**Q2**

1. Pomoću koje komponente ili procesa korisnik upravlja IDS sistemom?
   1. analizator
   2. agent
   3. operater
   4. menadžer
   5. podsistem za upozoravanje
2. Bilo koja akcija koja kompromituje bezbednost jednog sistema naziva se?
   1. Napad na bezbednost
   2. Mehanizam bezbednosti
   3. Bezbednost na mrežnom sloju
   4. Bezbednosni servisi
   5. Bezbednosni protokol
3. Koji zaštitni zid kontroliše saobraćaj izmedju ličnog računara ili radne stanice sa jedne strane, i Interneta ili mreže preduzeća sa druge strane?
   1. zaštitni zid zasnovan na host
   2. lični zaštitni zid
   3. ruter
   4. utvrdjeni zaštitni zid
   5. SOCKS
4. Koja su dva osnovna režima rada IPsec protokola?
   1. integritet, poverljivost
   2. tunelski i kontrola pristupa
   3. autentifikacija, integritet
   4. transportni, tunelski
   5. transportni i kontrola rutiranja
5. Koji režim rada pruža zaštitu za ceo IP paket?
   1. tunelski i transportni
   2. transportni
   3. tunelski
   4. autentifikacija paketa
   5. autentifikacija zaglavlja
6. PGP (Pretty Good Privacy) je bezbednosni program za?
   1. zaštitu paketa koji se prenosi
   2. izračunavanje izvoda paketa
   3. šifrovanje saobraćaja na transportnom sloju
   4. daljinsku autentifikaciju servera
   5. e-poštu
7. Koji priotokol je pouzdana treća strana usluge provere identiteta?
   1. Kerberos
   2. S/MIME
   3. SSL
   4. IP/IPSec
   5. TLS
8. Koji ključ se koristi za šifrovanje podataka koji se prenose mobilnom mrežom?
   1. Korenski ključa Ki
   2. Slučajni broj RAND
   3. Definisan ključ algoritma A8
   4. Definisan ključ algoritma A3
   5. Generisani ključa Kc
9. Kojom komandom se menja vlasništvo na Linux sistemu?
   1. stikybit
   2. setuid
   3. useradd
   4. chmod
   5. setgid

**Q3**

1. Koja komanda ako se postavi na izvršnu binarnu datoteku uzrokuje da se program "izvršava kao" da ga je pokrenuo njegov vlasnik?
   1. chmod
   2. stikybit
   3. setuid
   4. useradd
   5. setgid
2. Kojom komandom se mogu menjati dozvole za svaku datoteku?
   1. chmod
   2. setuid
   3. useradd
   4. stikybit
   5. setgid
3. Ko je najniži nivo OS-a ?
   1. LSA (Local Security Authority)
   2. Jezgro – kernel
   3. Object Manager
   4. SRM (Security Reference Monitor)
   5. SD (Security Descriptor)
4. Koja komponenata obavlja proveru pristupa, generiše audit log zapise, i upravlja pravima korisnika, koji se nazivaju i privilegije?
   1. SRM (Security Reference Monitor
   2. WinLogon, NetLogon
   3. SAM (Security Account Manager)
   4. LSA (Local Security Authority)
   5. SD (Security Descriptor)
   6. AD (Active Directory)
5. Koja tema bezbednosne politike uključuje kontrolu pristupa i zahtevano prijavljivanje na sistem?
   1. softver
   2. principi
   3. operativni sistemi
   4. sigurnost komunikacije
   5. zaštita podataka

**Q4**

1. **Objasniti BLP model**

BLP model se zasniva se na trenutnom stanju sistema (b, M, f, H), definisan kao:

Trenutni set pristupa b: trostruki niz u obliku (subjekat, objekat, pristup-mod);

• Matrica pristupa M: struktura je navedena ranije.

• Nivo funkcije f: dodjeljuje sigurnosni nivo svakom subjektu i objektu.

• Hijerarhija H: upravljačko stablo čiji čvorovi su objekti u sistemu. Nivo bezbednosti objekta mora da dominira nivoom bezbednosti svojih roditelja.

**3. Objasniti ulogu Honeypot.**

U računarskoj terminologiji, honeypot je zamka koja je postavljena da otkrije, odvrati ili na neki drugi način spreči pokušaje neovlašćenog korišćenja informacionih sistema. Može se sastojati od računara, podataka, sajta koji izgleda kao deo mreže, ali je, u suštini, izolovan, zaštićen, nadziran, a deluje tako kao da sadrži informacije ili resurse koji mogu biti interesantni i značajni za napadače.

’’Lažni mamci’’ su računari koji su određeni za metu eventualnih napada.

1. **Objasniti IDS baziran na mreži**

Mrežni IDS ( Network-Based IDS - NIDS ) prati saobraćaj u odabranim tačkama na mreži ili skupu međusobno povezanih mreža. Mrežni IDS sistemi raspolažu bazom podataka sa različitim parametrima poznatih napada. NIDS pregleda paket po paket saobraćaja u realnom vremenu, ili blizu realnom vremenu, u pokušaju da otkriju model upada. Tipični NIDS sistem uključuje brojne senzora za praćenje paketa saobraćaja. Senzori mogu da budu raspoređeni na jedan od dva načina: online i pasivno.

**6. Obajsniti IPSec protokol**

Predstavlja skup proširenja protokola IPv4 koji obezbeđuje osnovne sigurnosne aspekte mrežne komunikacije. Pošto se integriše sa IP protokolom, IPSec implementira sigurnosne mehanizme mrežne komunikacije na mrežnom sloju, odnosno na internet sloju skupa protokola TCP/IP. IPSec se može koristiti bez obzira na način implementacije fizičkog sloja i sloja veze. Komunikacioni uređaji na putu između dva entiteta ne moraju podržavati IPSec.

**8. Objasniti Linux modele bezbednosti**

Linux tradicionalni model bezbednosti može se sažeti prilično kratko: ljudi ili procesi sa "root" privilegijama mogu raditi šta god hoće; drugi nalozi (engl. accounts ) su ograničeni. Prema tome, cilj napadača je da dobije root privilegije. Kada se to dogodi, napadač može izbrisati ili urediti dnevnike (engl. logs ); sakriti svoje procese, datoteke i direktorijume. Korisnici čitaju, pišu i izvršavaju objekte, na osnovu dozvola objekata (engl. objects permissions ). Svaki objekat ima tri skupa dozvola: korisnik-vlasnik objekta, grupni vlasnik, i "drugi" (svi ostali). Ove dozvole sprovodi Linux kernel-a, "mozak" operativnog sistema

**9. Navesti lokacije zaštitnih zidova**

Zaštitni zid je postavljen da obezbedi zaštitnu barijeru između spoljašnjeg, potencijalno nepoverljivog izvora saobraćaja i interne mreže. Spoljni zaštitni zid je smešten na ivici lokalne ili mreže preduzeća. Jedan ili više internih zaštitnih zidova štite većinu mreže preduzeća. Između ova dva tipa zaštitnih zidova jedan ili više umreženih uređaja u regionu se pominju kao DMZ (demilitarizovana zona) mreže.

**10. Objasniti kako funkcioniše bezbednost mobilne trgovine i digitalnog novca**

Mreže mobilne telefonije su ćelijske, koriste bazne stanice BS (engl. Base Station) za pokrivanje specifične geografske površine. Bazne stanice kontroliše kontroler BSC (engl. Base Station Controler ) i centar MSC (engl. Mobile SwitchingCenter). U mobilnoj mreži ne postoji permanenta konekcija sa mobilnim terminalom MS (engl. Mobile Station ), tako da MS dobija LAI (engl. Location Area Identifier ) svaki put kada promeni zonu pokrivanja jednog kontrolera BSC (engl. location update ). Kada se uputi poziv jednom korisniku, MSC šalje pagging poruke svim BS u čijim LA je MS registrovan.

Digitalni novac predstavlja novi instrument plaćanja elektronske trgovine. Kada potrošač sa tradicionalnim novcem plati račun, serijski broj novčanica se ne zapisuje. Digitalne novčanice takođe poseduju serijske brojeve. Anonimnost kupca i nemogućnost praćenja transakcije se može ostvariti poverenjem u trećeg učesnika, mrežu servera valuta koji razmenjuju novčanice za novčanice bez identiteta, nakon provere validnosti i provere duplog trošenja.

**Q5**

* **Objasniti ulogu Output, Prerouting, Postrouting chain-a?**

Output – odnosi se na kontrolu paketa koji odlaze tj. Ka nekoj ip adresi ili mreži

Prerouting – izmena odredista paketa pri dolasku za razliku od FORWARD koji sa filtrira pakete

Postrouting – izmena odredista paketa neposredno pre odlaska iz mreze

* **Koja je uloga MANGLE tabele?**

Mangle tabela je pre svega namenjena izmeni zaglavlja IP paketa. Moguce je menjati gotovo sve aspekte tj sve tipove zaglavlja IP paketa.

* **Korišćenjem iptables dozvoliti jedino dolazni saobraćaj sa adrese 10.2.3.11**

Iptables –P INPUT DROP

Iptables –P OUTPUT DROP

Iptables –A INPUT –s 10.2.3.11 –j ACCEPT

* **Korišćenjem iptables blokirati odlazni i dolazni saobraćaj prema/sa mreže 192.168.9.0/24.**

Iptables –A INPUT –s 192.168.9.0/24 –j DROP

Iptables –A OUTPUT -d 192.168.9.0/24 –j DROP

* **Korišćenjem iptables dozvoliti dolazne tcp i udp pakete na portu 8080 i 3306, i saobraćaj na ostalim portovima.**

Iptables –A INPUT –p tcp --dports 8080,3306 –j ACCEPT

Iptables –A INPUT –p udp --dports 8080,3306 –j ACCEPT

* **Korišćenjem iptables blokirati sve dolazne konekcije, i jedino dozvoliti konekcije na portu 465, 587 i 995.**

Iptables –A INPUT DROP

Iptables –A INPUT --dports 465,587,995 –j ACCEPT

* **Obrisati pravilo koje zabranjuje dolazni saobraćaj sa adrese 10.18.1.0/24.**

iptables –D INPUT –s 10.18.1.0/24 –j DROP

* **Napisati iptables pravila koja dozvoljavaju jedino odlazni POP3 i SMTP saobraćaj, dok je sav ostali saobraćaj blokiran.**
* Iptables –A INPUT DROP
* Iptables –A OUTPUT DROP
* Iptables –A OUTPUT --sport 110 –j ACCEPT
* Iptables –A OUTPUT --sport 465 –j ACCEPT
* **Napisati iptables pravila koja jedino dozvoljavaju ping na INPUT-u i OUTPUT-u.**

Iptables –A INPUT –p icmp --icmp-type echo-request –j ACCEPT

Iptables –A OUTPUT –p icmp --icmp-type echo-request –j ACCEPT

* **Napisati komandu kojom se brišu sedmo pravilo u imput tabeli .**

Iptables –D INPUT 7

**Q6**

* **iptables -A INPUT -s !89.216.56.0/255.255.255.0 -i eth0 -p udp -m udp --dport 137:139 –j ACCEPT**

Dodaj pravilo na lanac pravila koje prihvata pakete ciji je izvorsni IP razlicit od zadate mreze tj. Koji ne potice iz date mreze sa interfejsa eth0 I koji koristi udp protocol gde mu je odredisni protocol u rasponu od 137 do 139

* **iptables -A INPUT -s !161.53.2.70 -p udp -m udp --dport 123 -j DROP**

Dodaje pravilo na lanac pravila - odbacuje dolazne pakete bez ciji je izvorisni ip razlicit od datog, koji koristi udp protocol I ciji je odredisni port 123

* **iptables -A INPUT -s 161.11.77.235 -i eth0 -p tcp -m tcp --dport 25, 465 -j ACCEPT**

dodaje pravilo na lanac pravila. Prihvata dolazece pakete ciji je izvorisni ip zadat 161.11.77.235, izvorisni interfejs slanja eth0, protocol koji koristi je tcp a odredisni portovi su 25,465

* **iptables -A INPUT -i ppp0 -m state -- state NEW, ESTABLISHED -j ACCEPT**

dodaje pravilo na lanac pravila. Prihvata dolazece pakete ciji je izvorni interfejs ppp0 I cije je stanje konekcije NOVO ili USPOSTAVLJENO

* **iptables -A FORWARD -i ppp0 -m state -- state NEW, RELETED -j ACCEPT**

dodaje pravilo na lanac pravila za preusmeravanje. Preusmerava pakete ciji je izvorisni interfejs ppp0 a stanje konekcije NOVO ili obrisano

**Q7**

* **Kojim ključevima se vrši digitalno šifrovanje i potpisivanje poruke. Opisati postupak?**

Postize se koriscenjem javnog I tajnog kljuca. Svaka strana ima svoj tajni I javni kljuc, javni kljucevi se razmenjuju I koriste se za sifrovanje dok se za desifrovanje koriste privatni kljucevi. Na ovaj nacin funckionise uopsteni digitalni potpis, RSA I slicni algoritmi koji koriste digitalno potpisivanje.

* **Napisti komandu za generisianje GPG ključeva na linux sistemu za korinsika IT381 i komandu za izvoz ključeva u asii foramtu za korisnika IT381.**

sudo gpg --full-gen-key (prethodno se logovati kao korisnik IT381)

gpg --export –a IT381

* **Napisati snort pravila za detekciju odlaznog TCP sobraćaja na odredišnim portovima 22 i 90, koje daje poruku da je došlo do detekcije saobraćaja na datim portovima i blokira saobraćaj ka odredišnim adresama?**

Alert tcp 22,90 -> !any any(msg: “Doslo je do detekcije”;)

* **Na linux sistemu šta se nalazi u /etc/passwd a šta u /etc/shadow datoteci?**

U passwd datoteci nalaze se podaci korisnika na sistemu koji se koriste recimo prilikom logovanja. Svaki od tih korisnika ima svoji home direktorijum svoj ID I generalno informacije koje bi bile od koristi administrator. Shadow datoteka cuva u stvari hesirane sifre korisnickih naloga na sistemu

* **Koristeći ACL ukloniti sve privilegije za korisnika it381 na fajlu IT382**?

Setfacl -x u:it381:rwx /IT382

**BLANKET C**

**Q1**

1. Pre upotrebe elektronske opreme za obradu podataka, važne informacije su najčešće čuvane u?
   1. magacinu
   2. sefu
   3. banci
   4. registrima
2. Raspoloživost kao bezbednosna usluga obezbedjuje?
   1. da ovlaćæeni korisnici imaju pristup podacima i računarskim resursima kada su im potrebni
   2. da se podaci neautorizovano ne menjaju ili uništavaju
   3. da korisnik koji pošalje poruku ne može kasnije poreći da je to uradio celovitost podataka
   4. pristup informacijama samo za one korisnike koji su ovlašćeni da tim informacijama pristupe
3. Integritet kao bezbednosna usluga obezbedju?
   1. pristup informacijama samo za one korisnike koji su ovlaši da tim informacijama pristupe
   2. da se podaci neautorizovano ne menjaju ili uništavaju
   3. da ovlašæeni korisnici imaju pristup podacima i računarskim resursima kada su im potrebni
   4. da korisnik koji pošalje poruku ne može kasnije poreći da je to uradio celovitost podataka
4. Napad tokom koga se jedan entitet pretvara da je drugi naziva se?
   1. Ponovo pustiti
   2. Fabrikovanje
   3. Izmena poruke
   4. Odbijanje usluga
   5. Prerušavanje
5. Šta opisuje način na koji subjekat može pristupiti objektu?
   1. uloga
   2. pravo pristupa
   3. objekat
   4. subjekat
   5. model
6. Matematička funkcija koja se koristi za šifrovanje i dešifrovanje naziva se?
   1. kriptografski algoritam ili šifra
   2. otvoren tekst
   3. ključ
   4. šifrat
7. Otkrivanje ključa nekriptoanalitičkim metodama naziva:
   1. snaga kriptosistema
   2. napad
   3. šifrovanje
   4. sigurnost kriptosistema
   5. kompromitovanje
8. Koji bezbednosni mehanizam se koristi za proveru integriteta poruka?
   1. digitalni potpis
   2. kontrola pristupa
   3. šifrovanje
   4. autentifikacija poruke

**Q2**

1. Koji IDS sistem je zasnovan na računarima koji su određeni za metu eventualnih napada?
   1. IDS zasnovan na hostu
   2. SNORT
   3. Lažni “mamci”
   4. IDS zasnovan na mreži
   5. Audit zapisa
2. Kojim bezbednosnim servisom se obezbedjuje zaštita od oštećenja, pomoću jednog od entiteta uključenih u komunikaciji ili deo komunikacije?
   1. autentifikacija
   2. neodbacivanje
   3. kontrola pristupa
   4. integritet podataka
   5. poverljivost
3. Koji zaštitni zid kontroliše saobraćaj izmedju ličnog računara ili radne stanice sa jedne strane, i Interneta ili mreže preduzeća sa druge strane?
   1. zaštitni zid zasnovan na host
   2. lični zaštitni zid
   3. ruter
   4. utvrdjeni zaštitni zid
   5. SOCKS
4. Koje tri funkcionalne oblasti obuhvata IPSec protokol?
   1. proveru identiteta, povjerljivost i digitalni potpis
   2. kontrolu rutiranja, povjerljivost i upravljanje ključevima
   3. autentifikacija, integritet i upravljanje ključevima
   4. proveru identiteta, povjerljivost i upravljanje ključevima
   5. algoritam za šifrovanje, digitalni potpies i upravljanje ključevima
5. Oakley protokol razmene ključa zasnovan je na?
   1. HMAC kodu
   2. digitalnom potpisu
   3. asimetričnom algoritmu šifrovanja
   4. Hash kodu
   5. Diffie-Hellman algoritmu
6. Koji protokoli osiguravaju transportni sloj?
   1. SSL, TLS
   2. Kerberos, S/MIME
   3. UDP
   4. IP/IPSec
   5. TCP
7. Koji napadi uključuju otkrivanje drugih korisnika, ubacivanje poruka u tranzitu izmedju klijenta i servera i ubacivanje informacija na web sajt?
   1. Reprodukovanje
   2. DoS
   3. Upad
   4. Aktivni
   5. Pasivni
8. Kako se naziva tehnologija malih bežičnih mreža dimenzionisanih za male udaljenosti koje u gradskim uslovima iznose od nekoliko desetina do nekoliko stotina metara?
   1. Bluetooth
   2. WWAN
   3. RFID
   4. bezična lokalna mreža - WLAN
   5. WPAN
9. Kod koje bežične mreže razlikujemo "ad hoc" i "infrastrukturne" veze?
   1. WWAN
   2. WPAN
   3. WLAN
   4. Bluetooth
   5. RFID

**Q3**

1. Kako se naziva direktna veza dva računara ili drugih uređaja koji imaju ugrađene module za WLAN komunikaciju?
   1. RFID
   2. WPAN
   3. ad hoc
   4. GSM
   5. infrastrukturna
2. Ko može da menja dozvole objekta?
   1. svi korisnici
   2. Kernel
   3. grupa
   4. vlasnik
   5. subjekat
3. Koji bezbednosni model je implementiran u SELinux a zasniva se na Bell-LaPadula (BLP) modelu?
   1. bezbednost na više nivoa
   2. Type Enforcement
   3. RBAC
   4. DAC
   5. MAC
4. Koji bezbednosni servis obezbeđuje da se novac ne može preuzimati sa računa potrošača ili smart kartice bez eksplicitne dozvole?
   1. integritet plaćanja
   2. tajnost plaćanja
   3. autorizacija plaćanja
   4. autentifikacija plaćanja
   5. neporecivost plaćanja
5. Koji bezbednosni servis plaćanja sprečavaju ponovno korišćenje i falsifikovanje elektronskih novčanica?
   1. bezbednosti smart kartica
   2. transakcioni
   3. bezbednosti digitalnih čekova
   4. bezbednosti platnih kartica
   5. bezbednosti digitalnog novca
6. Kako se naziva informacija uskadištena ili prenošena u digitalnoj formi koja se koristi u sudskom postupku i mogu se koristiti na suđenju?
   1. pravni dokaz
   2. informatički dokaz
   3. proveren dokaz
   4. digitalni dokaz
7. Kako se naziva proces sprečavanja pristupa računarskim sistemima u nekoj zgradi?
   1. spoljašnje obezbeđenje
   2. IDS sistemi
   3. video nadzor
   4. sigurnosne zone
   5. kontrola pristupa
8. Koji prestup ima najveći faktor rasta u oblasti kompjuterskog kriminala?
   1. krađa labtop računara
   2. krađa identiteta
   3. krađa mobilnih telefona
   4. krađa prenosnih memorija
   5. neovlašćen pristup

**Q4**

1. Navesti osnovne faze napada

Ispitaj I proceni

Ekspoatiši I prodri

Povećaj privilegije

Održi pristup

3. Šta je kriptoanaliza?

Kriptoanaliza je nauka koja bez ključa određuje otvoren tekst na osnovu šifrata.

Pokušaj kriptoanalize u cilju otkrivanja algoritma šifre, ključa ili otvorenog teksta naziva se ''napad''. Otkrivanje ključa nekriptoanalitičkim metodama naziva se ''kompromitovanje''.

4. Sta je hash funkcija i za sta se sve koristi?

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

1. Objasniti Authentication Header (AH)

AH obezbeđuje sigurnosne usluge provere identiteta, integriteta i neporecivosti IP paketa, ali ne može obezbediti privatnost.

7. Sta je SSL protokol, koje verzije postoje i za sta se sve koristi?

SSL je jedan od najkorišćenijih bezbednosnih protokola. SSL sloj se nalazi između aplikacionog i transportnog sloja. SSL prima podatke, šifruje podatke i usmerava šifrovane podatke na TCP soket.

8. Objasniti kako funkcionise dinamičko ispitivanje paketa

1. Bezbednost mobilnih mreza
2. 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. Postoje više od 45 privilegija na Windows OS, od kojih se neke smatraju opasnim

Q5

* Objasniti razliku između DROP i RETURN vrednosti u IPTABLES zaštitnom zidu?

DROP odbacuje sav promet bez javljanja greške i završava prolaz, I ne čuva log

RETURN pravi log pokušaja.

* Koja je uloga FILTER tabele?
* Korišćenjem iptables blokirati odlazni saobraćaj za adresu 10.1.1.15 i to pravili postaviti na trećem mestu u lancu.

iptables -A INPUT -s 10.0.0.15 -j DROP

* Korišćenjem iptables blokirati odlazni saobraćaj prema mreži 192.168.254.0/30.

iptables -A OUTPUT -d 192.168.254.0/30 -j DROP

* Korišćenjem iptables dozvoliti dolazne tcp i udp pakete na portu 22 i 3306, i blokirati ostale portove i presotali dolazni saobraćaj.
* Izmeniti pravilo iptables –I INPUT 4 –p tcp –dport 3306 –j ACCEPT tako da dozvoaljava saobraćaj na portu 3306 samo sa adrese 89.216.56.81

iptables –I INPUT 4 –p tcp -s 89.216.56.81 –dport 3306 –j ACCEPT

* Obrisati pravilo koje zabranjuje dolazni saobraćaj sa adrese 10.15.15.15.

iptables -D INPUT -s 10.15.15.15 -j DROP

* Napisati iptables pravila koja dozvoljavaju jedino odlazni POP3 i SMTP saobraćaj, dok je sav ostali saobraćaj blokiran.
* Napisati iptables pravila koja zabranjuje ping na FORWARD-u.

iptables -A FORWARD -p icmp --icmp-type echo-request -j DROP

* Napisati komandu kojom se briše sedmo pravilo u output tabeli .

iptables -D INPUT 7

**Q6**

* iptables -A INPUT -s 89.168.91.0/255.255.255.0 -i eth0 -p udp -m udp --dport 135:139 –j ACCEPT
* iptables -A FORWARD -s 161.53.2.70 -p udp -m udp --dport 321 -j ACCEPT

Prihvatiti dolazni saobracaj sa adrese 161.53.2.71 gde je udp protokol i gde je podudaranje udp protokola za odredisni port 321

* iptables -R INPUT 1 -p tcp -s 192.168.0.0/24 --dport 80 -j ACCEPT
* iptables -A OUTPUT -i ppp0 -m state -- state NEW,INVALID -j DROP

Dodaje se pravilo na kraj lanca za OUTPUT, ulazni interfejs je ppp0 nakon čega poredimo stanje koje je NEW ili INVALID i skače na DROP koji odbacuje takve pakete.

* iptables -A FORWARD -i ppp0 -m state -- state NEW,INVALID -j DROP

Q7

* Kojim ključem se vrši digitalno šifrovanje i potpisivanje poruke. Opisati postupak?

Pri potpisivanju poruka, generise se hash poruka sa fiksnom duzinom. Nakon toga se vrsi enkripcija privatnim kljucem osobe koja poruku potpisuje. Tako potpisana poruka zajedno sa enkriptovanom hash vrednoscu se salje primaocu koji ce svojim javnim kljucem desifrovati potpis.

* Korišćenjem ACL-a, napsiati komandu kojom se korisniku it381 na linux sistemu oduzima pravo čitanja nad fajlom ovdeprocitati, bez promene trenutnog vlasnika i grupe.?

chmod -r it381 ovdeprocitati

* Napsiati snort pravilo za detekciju dolaznog UDP sobraćaja na portu 465 i 587, koje daje poruku da je došlo do detekcije saobraćaja na datim portovima?

alert udp any any <- any 465,578 (msg: “Doslo je do detekcije saobracaja na datim portovima”)

* Na linux sistemu šta se nalazi u /etc/passwd a šta u /etc/shadow datoteci?

etc/passwd se koristi pracenje svih postojecih korisnika na linux sistemu dok shadow sadrzi

hesirane lozinke za korisnike

* Koristeći ACL ukloniti pravo čitanja za korisnika it381 na fajlu IT381?

setfacl –r u:it381 IT381

Q4

**7**. Sta je SSL protokol, koje verzije postoje i za sta se sve koristi?

SSL je jedan od najkorišćenijih bezbednosnih protokola. SSL sloj se nalazi između aplikacionog i transportnog sloja. SSL prima podatke, šifruje podatke i usmerava šifrovane podatke na TCP soket.

SSL je zasnovan ja metodama asimetričnog PKI sifrovanja. SSL služi da identifikuje dve strane povezane računarskom mrežom.

SSL se nalazi između aplikacionog I transportnog sloja. SSL I TLS se koristeza autentifikaciju I sifrovanje podataka za pristup pošti IMAP.

**8**. 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*

10. 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.

13. Objasniti razliku izmedju IPS i IDS sistema.

Glavna razlika je da IPS može 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.

17.Objasniti proces ojačanja Linux sistema?

Ojačanje Linux sistema se može postići na sledeći način:

-Postavljanje lozinke za pristup bios-u I zabrana podizanja sistema sa cd-a

-isključivanje server sa mreže

1. 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.*

1. Bezbednost mobilnih mreza

Korišćenje mobilnih uređaja doživljava veliku ekspanziju u zadnjih petnaestak godina. U računarskim mrežama u kojima se za prenos podataka koriste žičani i optički medijumi, postoji određeni nivo inherentne fizičke sigurnosti u odnosu na Wi-Fi mreže. Analogno tome, fiksna telefonija je sigurnija od mobilne. Zbog toga je bilo potrebno u GSM sistemu osigurati zavidan nivo sigurnosti mobilnih uređaja, odnosno prenosa govora i podataka, pogotovo nakon propusta koji su bili uočeni u starijim mobilnim tehnologijama. U novijim tehnologijama, kao što su GPRS, UMTS ispravljeni su ti nedostaci.

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

Postoji tri tipa mrežnih zaštitinih zidova:

-filtriranje paketa

-mrežni prolazi (gateways) aplikativnog nivoa

- prolazi na nivou kanala komunikacijskih podataka

2. Šta je slojevita zaštita i kako se koristi?

Da bi u potpunosti zaštitili podatke tokom njihovog trajanja, svaka komponenta sistema za obradu informacija mora da ima sopstveni mehanizam zaštite. Raslojavanje i preklapanje bezbednosnih mera se naziva slojevita zaštita. Korišćenjem strategije slojevite zaštite, trebalo bi da, ako jedna odbrambena mera ne uspe, postoje i druge mere u odbrani koje će nastaviti da obezbeđuju zaštitu. Naime, možemo zamisliti da slojevitu zaštitu predstavljaju slojevi luka, sa podacima u jezgru luka. Korisnik sistema koji prolazi kroz slojeve zaštite mora zadovoljiti sve mehanizme koji zadržavaju napadača ili minimiziraju njegovu mogućnost pristupa kritičnim resursima. Slojevita zaštita ilustrovana je na primeru četiri prstena.

Q5

1. Korišćenjem iptables dozvoliti odlazni saobraćaj ka adresi 192.168.32.10.

Iptables –A OUTPUT –s192.168.32.10 –j ACCEPT

* Korišćenjem iptables dozvoliti jedino dolazni saobraćaj sa adrese 10.2.3.11

Iptables –P INPUT DROP

Iptables –P OUTPUT DROP

Iptables –A INPUT –s 10.2.3.11 –j ACCEPT

* Korišćenjem iptables blokirati odlazni i dolazni saobraćaj prema/sa mreže 192.168.9.0/24.

Iptables –A INPUT –s 192.168.9.0/24 –j DROP

Iptables –A OUTPUT -d 192.168.9.0/24 –j DROP

* Korišćenjem iptables dozvoliti dolazne tcp i udp pakete na portu 8080 i 3306, i saobraćaj na ostalim portovima.

Iptables –A INPUT –p tcp --dports 8080,3306 –j ACCEPT

Iptables –A INPUT –p udp --dports 8080,3306 –j ACCEPT

* Korišćenjem iptables blokirati sve dolazne konekcije, i jedino dozvoliti konekcije na portu 465, 587 i 995.

Iptables –A INPUT DROP

Iptables –A INPUT --dports 465,587,995 –j ACCEPT

* Napisati iptables pravila koja dozvoljavaju jedino odlazni POP3 i SMTP saobraćaj, dok je sav ostali saobraćaj blokiran.

Iptables –A INPUT DROP

Iptables –A OUTPUT DROP

Iptables –A OUTPUT --sport 110 –j ACCEPT

Iptables –A OUTPUT --sport 465 –j ACCEPT

Port 25 – this is the default SMTP non-encrypted port;

Port 2525 – this port is opened on all SiteGround servers in case port 25 is filtered (by your ISP for example) and you want to send non-encrypted emails with SMTP;

Port 465 – this is the port used if you want to send messages using SMTP securely.

By default, the IMAP protocol works on two ports:

Port 143 – this is the default IMAP non-encrypted port;

Port 993 – this is the port you need to use if you want to connect using IMAP securely.

By default, the POP3 protocol works on two ports:

Port 110 – this is the default POP3 non-encrypted port;

Port 995 – this is the port you need to use if you want to connect using POP3 securely.

* Korišćenjem iptables blokirati dolazni saobraćaj sa adrese 10.15.1.1.

iptables -A INPUT -s 10.15.1.1 -j DROP

* Korišćenjem iptables blokirati odlazni i dolazni saobraćaj prema/sa mreže 192.168.11.0/24.

iptables -I INPUT -s 192.168.11.0 --dport 24 -j DROP

iptables -I OUTPUT -d 192.168.11.0 --dport 24 -j DROP

* Korišćenjem iptables dozvoliti dolazne tcp i udp pakete na portu 81 i 3306, i blokirati ostale portove.

iptables -I INPUT 1 -m udp -p tcp -j DROP

iptables -I INPUT 1 -m udp -p tcp --dport 81 -j ACCEPT

iptables -I INPUT 1 -m udp -p tcp --dport 3306 -j ACCEPT

* Korišćenjem iptables blokirati sve dolazne konekcije, i jedino dozvoliti konekcije na portu 465, 587 i 995.

iptables -A INPUT -p tcp -m tcp -m multiport ! --dports 465,587,995 -j DROP

* Korišćenjem iptables blokirati odlazni saobraćaj za adresu 10.1.1.15 i to pravili postaviti na trećem mestu u lancu.

iptables -A INPUT -s 10.0.0.15 -j DROP

iptables –I INPUT 3 –s 10.0.0.15 –j DROP (\*\*\*\*)

* Korišćenjem iptables blokirati odlazni saobraćaj prema mreži 192.168.254.0/30.

-

iptables -A OUTPUT -d 192.168.254.0/30 -j DROP

* Izmeniti pravilo iptables –I INPUT 4 –p tcp –dport 3306 –j ACCEPT tako da dozvoaljava saobraćaj na portu 3306 samo sa adrese 89.216.56.81

iptables –I INPUT 4 –p tcp -s 89.216.56.81 –dport 3306 –j ACCEPT

* Obrisati pravilo koje zabranjuje dolazni saobraćaj sa adrese 10.18.1.0/24.

iptables –D INPUT –s 10.18.1.0/24 –j DROP

* Obrisati pravilo koje zabranjuje dolazni saobraćaj sa adrese 10.15.15.15.

iptables -D INPUT -s 10.15.15.15 -j DROP

* Napisati komandu kojom se brišu sedmo pravilo u imput tabeli .

Iptables –D INPUT 7

* Napisati komandu kojom se briše sedmo pravilo u output tabeli .

iptables -D INPUT 7

**i**. Obrisati sva pravila iz INPUT lanca.

Iptables –D INPUT

* Napisati iptables pravila koja zabranjuje ping na FORWARD-u.

iptables -A FORWARD -p icmp --icmp-type echo-request -j DROP

* Napisati iptables pravila koja jedino dozvoljavaju ping na INPUT-u i OUTPUT-u.

Iptables –A INPUT –p icmp --icmp-type echo-request –j ACCEPT

Iptables –A OUTPUT –p icmp --icmp-type echo-request –j ACCEPT

2021. \*\*\*\*

**c**. Korišćenjem iptables dozvoliti odlazni saobraćaj ka adresi 192.168.32.10. \*\*\*\*

Iptables –A OUTPUT –s192.168.32.10–j ACCEPT

**d**. Korišćenjem iptables odbaciti dolazne i odlazne ICMP zahteve bez odgovora.

**e**. Korišćenjem iptables blokirati dolazni saobraćaj od mreže 192.168.1.0/24. \*\*\*\*

Iptables –A INPUT –s 192.168.1.0/24 –j DROP

**f.** Napisati pravilo kojim se blokira dolazni tcp saobraćaj sa IP adrese 174.213.0.1 i to preko interfejsa koji nije eth0 i porta 53.

**g**. Napisati pravilo kojim se preusmerava SSH sa porta 5000 na port 22.

**h**. Odbaciti sve pakete koji ne dolaze sa IP adrese 192.168.1.3 i dolaze na port 25.

iptables -A INPUT -s ! 192.168.1.3 –i ! eth0 -p udp -m udp --dport 25 –j DROP

# Q6

**Q6. [20] Objasniti sledeća iptables pravila:**

# 2021.

1. iptables -A INPUT -s ! 192.168.1.32 –i ! eth0 -p udp -m udp --dport 135 –j DROP

**Komanda oznacava odbijanje ovog pravila u lancu cija izvorsna adresa nije razlicita od one navedene, preko udp porta gde je odredisni port 135**

1. iptables –A INPUT –i eth0 –p tcp –dport 143 –m state –state NEW, ESTABLISHED –j ACCEPT
2. iptables –A INPUT –m mac –mac-source 00:0F:EA:91:04:08 –j DROP

Odbascuje sve pakete u mac adrese 00:0F:EA:91:04:08

1. iptables -A INVALID -i wan\_eth -p tcp --tcp-flags SYN, FIN, ACK SYN -j DROP
2. iptables -A INPUT –s 10.10.10.10 -p tcp --dport 3306 -j REJECT

Odbija dolazni saobracaj sa adrese 10.10.10.10, koristeci port 3306

# 2020.

(13.2.2020)

* iptables -A INPUT -s !89.216.56.0/255.255.255.0 -i eth0 -p udp -m udp --dport 137:139 –j ACCEPT

Dodaj pravilo na lanac pravila koje prihvata pakete ciji je izvorsni IP razlicit od zadate mreze tj. Koji ne potice iz date mreze sa interfejsa eth0 I koji koristi udp protocol gde mu je odredisni protocol u rasponu od 137 do 139

* iptables -A INPUT -s !161.53.2.70 -p udp -m udp --dport 123 -j DROP

Dodaje pravilo na lanac pravila - odbacuje dolazne pakete bez ciji je izvorisni ip razlicit od datog, koji koristi udp protocol I ciji je odredisni port 123

* iptables -A INPUT -s 161.11.77.235 -i eth0 -p tcp -m tcp --dport 25, 465 -j ACCEPT

dodaje pravilo na lanac pravila. Prihvata dolazece pakete ciji je izvorisni ip zadat 161.11.77.235, izvorisni interfejs slanja eth0, protocol koji koristi je tcp a odredisni portovi su 25,465

* iptables -A INPUT -i ppp0 -m state -- state NEW, ESTABLISHED -j ACCEPT

dodaje pravilo na lanac pravila. Prihvata dolazece pakete ciji je izvorni interfejs ppp0 I cije je stanje konekcije NOVO ili USPOSTAVLJENO

* iptables -A FORWARD -i ppp0 -m state -- state NEW, RELETED -j ACCEPT

dodaje pravilo na lanac pravila za preusmeravanje. Preusmerava pakete ciji je izvorisni interfejs ppp0 a stanje konekcije NOVO ili obrisano

(14.6.2020.)

* iptables -A INPUT -s 89.216.56.0/255.255.255.0 -i eth0 -p udp -m udp --dport 135:139 –j ACCEPT

Komanda oznacava dodavanje novog pravila u lancu pravila cija izvorisna

adresa nije raslicita od one navedene, sa interfejsa eth0, preko udp porta

gd3 je odredisni port izmedju 137 i 139

* iptables -A INPUT -s !161.53.9.70 -p udp -m udp --dport 123 -j DROP

**Komanda oznacava odbijanje ovog pravila u lancu cija izvorsna adresa nije razlicita od one navedene, preko udp porta gde je odredisni port 123**

* iptables -A INPUT -s 161.11.77.235 -i eth0 -p tcp -m tcp --dport 25, 465 -j ACCEPT

komanda oznacava dodavanje novog pravila u lancu pravila cija izvorisna

adresa nije raslicita od one navedene, sa interfejsa eth0, preko udp porta

gd3 je odredisni port izmedju 137 i 13

* iptables -A INPUT -i ppp0 -m state -- state NEW, ESTABLISHED -j ACCEPT

to je dodavanje novog pravila na inteferjsu ppp0, gde se dozvoljava propustanje paketa sa  stanjem novi i uspostavljen

* iptables -A FORWARD -i ppp0 -m state -- state NEW, RELETED -j DROP

to je dodavanje novog pravila na inteferjsu ppp0, gde se zabranjuje(paketi se uništavaju) propuštanje paketa sa stanjem novi i povezani sa već postojećom konekcijom(FTP, ICMP..)

# 2018.

(4.7.2018.)

* iptables -A INPUT -s 89.168.91.0/255.255.255.0 -i eth0 -p udp -m udp --dport 135:139 –j ACCEPT
* iptables -A FORWARD -s 161.53.2.70 -p udp -m udp --dport 321 -j ACCEPT

Prihvatiti dolazni saobracaj sa adrese 161.53.2.71 gde je udp protokol i gde je podudaranje

udp protokola za odredisni port 321

* iptables -R INPUT 1 -p tcp -s 192.168.0.0/24 --dport 80 -j ACCEPT
* iptables -A OUTPUT -i ppp0 -m state -- state NEW,INVALID -j DROP

Dodaje se pravilo na kraj lanca za OUTPUT, ulazni interfejs je ppp0 nakon čega poredimo stanje koje je NEW ili INVALID i skače na DROP koji odbacuje takve pakete.

* iptables -A FORWARD -i ppp0 -m state -- state NEW,INVALID -j DROP

2021.

1. iptables -A INPUT -s ! 192.168.1.32 –i ! eth0 -p udp -m udp --dport 135 –j DROP

**Komanda oznacava odbijanje ovog pravila u lancu cija izvorsna adresa nije razlicita od one navedene, preko udp porta gde je odredisni port 135**

1. iptables –A INPUT –i eth0 –p tcp –dport 143 –m state –state NEW, ESTABLISHED –j ACCEPT
2. iptables –A INPUT –m mac –mac-source 00:0F:EA:91:04:08 –j DROP

Odbascuje sve pakete u mac adrese 00:0F:EA:91:04:08

1. iptables -A INVALID -i wan\_eth -p tcp --tcp-flags SYN, FIN, ACK SYN -j DROP
2. iptables -A INPUT –s 10.10.10.10 -p tcp --dport 3306 -j REJECT

Odbija dolazni saobracaj od strane 10.10.10.10, koristeci port 3306

# Q7

**Q7. [20] Odgovoriti na sledeća pitanja:**

**a**. Kojom komandom u Kali Linuxu možemo kreirati grupu, a kojom dodati korisnika u tu grupu?

groupadd mygroup

sudo usermod –a –G mygroup katarina

**b**. Kojom komandom možemo generisati novi par GPG ključeva?

gpg – full-gen-key

* Napisti komandu za generisianje ključeva na linux sistemu za GPG.

gpg – full-gen-key

**c**. Kojom komandom se može importovati GPG ključ koji se nalazi u tmp direktorijumu i pod nazivom perinključ?

gpg –verify/tmp/katarininkljuc

b) Napsiati komandu kojom se korisniku *it381* na linux sistemu dodeljuje pravo čitanja nad fajlom *ovdeprocitati*, bez promene trenutnog vlasnika i grupe.?

**d**. Kojom GPG komandom se može potpisati fajl pod nazivom potpisanifajl?

gpg –sign –recipent katarina –encrypt potpisanifajl

**e**. Šta je i čemu služi Snort?

Snort je besplatan programski paket koji služi za praćenje I otkrivanje neovlašćenih aktivnosti.

Snort može u realnom vremenu da sakuplja pakete u realnom vremenu, analizira protocol I sadržaj pretrage, može detektovati niz napada I proba zasnovanih na skupu pravila koje kofiguriše administrator sistema.

* Kojim ključem se vrši digitalno šifrovanje i potpisivanje poruke. Opisati postupak?

PKCS#1 je standard šifrovanja podataka korišćenjem RSA asimetričnog

algoritma i najčešće se koristi za digitalne koverte i digitalne potpise.Kod

I digitalnog potpisa, sadržaj koji treba da se potpiše prvo se redukuje (na primer, MD5 ili SHA-1), a zatim se šifruje primenom, na primer, RSA algoritma, koristeći privatni

ključ potpisnika poruke.

Šifrovani otisak poruke predstavlja digitalni potpis date poruke i postaje njen pridruženi

deo. Kada ovakva poruka stigne do primaoca kojem je namenjena, izvršava se postupak

verifikacije digitalnog potpisa. Ovaj postupak se sastoji od dešifrovanja izvoda dobijene

poruke primenom RSA algoritma, uz upotrebu javnog ključa pošiljaoca poruke.

Pri potpisivanju poruka, generise se hash poruka sa fiksnom duzinom. Nakon toga se vrsi enkripcija privatnim kljucem osobe koja poruku potpisuje. Tako potpisana poruka zajedno sa enkriptovanom hash vrednoscu se salje primaocu koji ce svojim javn

im kljucem desifrovati potpis.

Postize se koriscenjem javnog I tajnog kljuca. Svaka strana ima svoj tajni I javni kljuc, javni kljucevi se razmenjuju I koriste se za sifrovanje dok se za desifrovanje koriste privatni kljucevi. Na ovaj nacin funckionise uopsteni digitalni potpis, RSA I slicni algoritmi koji koriste digitalno potpisivanje.

* Napisti komandu za generisianje GPG ključeva na linux sistemu za korinsika IT381 i komandu za izvoz ključeva u asii foramtu za korisnika IT381.

Komanda za generisanje GPG kljuceva:

Potrebno je da korisnik bude prijavljen: su – IT381

sudo gpg --full-gen-key

Komada za izvoz kljuceva:

gpg –export –a IT381

* Napisati snort pravila za detekciju odlaznog TCP sobraćaja na odredišnim portovima 22 i 90, koje daje poruku da je došlo do detekcije saobraćaja na datim portovima i blokira saobraćaj ka odredišnim adresama?

Alert tcp 22,90 -> !any any(msg: “Doslo je do detekcije”;)

Alert tcp any any -> any 22 90 (msg: “Greska”;) \*\*\*\*

* Napsiati snort pravila za detekciju dolaznog TCP sobraćaja na odredišnim portovima 22 i 80, koje daje poruku da je došlo do detekcije saobraćaja na datim portovima i blokira saobraćaj sa odredišnih adresa?
* Napsiati snort pravilo za detekciju dolaznog UDP sobraćaja na portu 465 i 587, koje daje poruku da je došlo do detekcije saobraćaja na datim portovima?

alert udp any any <- any 465,578 (msg: “Doslo je do detekcije saobracaja na datim portovima”)

c) Napsiati snort pravilo za detekciju ICMP paketa.?

* Na linux sistemu šta se nalazi u /etc/passwd a šta u /etc/shadow datoteci?

etc/passwd se koristi pracenje svih postojecih korisnika na linux sistemu dok shadow sadrzi

hesirane lozinke za korisnike.

*/etc/passwd* - je baza podataka koja sadrži sve korisničke naloge Linux sistema.

*/etc/shadow* - U datoteci/etc/shadow se nalazi stvarna lozinka u šifrovanom formatu za svaki nalog sa dodatnim informacijama o lozinci. Svako polje je odvojeno od susednog polja simbolom (:). Datoteka /etc/shadow sadrži jedan red za svakog korisnika koji je naveden u datoteci /etc/ passwd. /etc/pasword

U passwd datoteci nalaze se podaci korisnika na sistemu koji se koriste recimo prilikom logovanja. Svaki od tih korisnika ima svoji home direktorijum svoj ID I generalno informacije koje bi bile od koristi administrator

Shadow datoteka cuva u stvari hesirane sifre korisnickih naloga na sistemu

* Koristeći ACL ukloniti sve privilegije za korisnika it381 na fajlu IT381?

setfacl -x u:it3881\_korisnik:-r home/ IT381/private/

* Korišćenjem ACL-a, napsiati komandu kojom se korisniku it381 na linux sistemu oduzima pravo čitanja nad fajlom ovdeprocitati, bez promene trenutnog vlasnika i grupe.?

chmod -r it381 ovdeprocitati

* Koristeći ACL ukloniti pravo čitanja za korisnika it381 na fajlu IT381?

setfacl –r u:it381 IT381

* Koristeći ACL ukloniti sve privilegije za korisnika it381 na fajlu IT382?

Setfacl -x u:it381:rwx /IT382

-x uklanja

Read write execute

13.2.2020. \*\*\*\*

* Kojim ključevima se vrši digitalno šifrovanje i potpisivanje poruke. Opisati postupak?

Postize se koriscenjem javnog I tajnog kljuca. Svaka strana ima svoj tajni I javni kljuc, javni kljucevi se razmenjuju I koriste se za sifrovanje dok se za desifrovanje koriste privatni kljucevi. Na ovaj nacin funckionise uopsteni digitalni potpis, RSA I slicni algoritmi koji koriste digitalno potpisivanje.

* Napisti komandu za generisianje GPG ključeva na linux sistemu za korinsika IT381 i komandu za izvoz ključeva u asii foramtu za korisnika IT381.

sudo gpg --full-gen-key (prethodno se logovati kao korisnik IT381)

gpg --export –a IT381

* Napisati snort pravila za detekciju odlaznog TCP sobraćaja na odredišnim portovima 22 i 90, koje daje poruku da je došlo do detekcije saobraćaja na datim portovima i blokira saobraćaj ka odredišnim adresama?

Alert tcp 22,90 -> !any any(msg: “Doslo je do detekcije”;)

* Na linux sistemu šta se nalazi u /etc/passwd a šta u /etc/shadow datoteci?
* Koristeći ACL ukloniti sve privilegije za korisnika it381 na fajlu IT382?

Setfacl -x u:it381:rwx /IT382

# Q1

1. Komponente informacionog sistema su?
   1. hardver, softver, procedure, mreža, podaci, trojanci
   2. procedure, hardver, crvi, mreža, podaci, hakeri
   3. ljudi, procedure, hardver, softver, mreža, podaci
   4. procedure, ljudi, hardver, zlonamerni kod, internet, podaci
   5. podaci, softver, virusi, hardver, ljudi, procedure
2. Kontrola pristupa kao bezbednosna usluga dozvoljava
   1. da je neko ili nešto ono za koga/šta se predstavlja
   2. da ovlašćeni korisnici imaju pristup podacima i računarskim resursima kada su im potrebni
   3. da korisnik koji pošalje poruku ne može kasnije poreći da je to uradio
   4. da se podaci neautorizovano menjaju ili uništavaju
   5. objektu proverenog identiteta da pristupi sistemu
3. Zahtev da samo ovlašćeni korisnici mogu da menjaju podatke naziva se?
   1. Provera identiteta
   2. Raspoloživost
   3. Neporicanje
   4. Kontrola pristupa
   5. Integritet
4. Fragmenti koda koji se ubacuju u druge legitimne programe su?
   1. Logička bomba
   2. Klopka
   3. Virus
   4. Crv
   5. Trojanski konj
5. Odobrenje pristupa na određeni način jednom ili više objekata je?
   1. funkcija pristupa
   2. sesija
   3. lista prava
   4. dozvola ili pravo pristupa
   5. uloga
6. Matematička funkcija koja se koristi za šifrovanje i dešifrovanje naziva se?
   1. kriptografski algoritam ili šifra
   2. otvoren tekst
   3. ključ
   4. šifrat
7. Kada cena kriptoanalize premašuje vrednost šifrovanih informacija kažemo da je kriptografski sistem?
   1. provaljen
   2. napadnut
   3. kompromitovan
   4. jak
   5. siguran
8. Željeno sigurnosno ponašanje sistema definisano je?
   1. Funkcionalnim zahtevima
   2. Zajedničkim klasama
   3. Zajedničkim kriterijumima
   4. Bezbednosnim zahtevima
9. Osnov za dobijanje poverenja da su zahtevane bezbednosne mere efikasne i da su implementirane ispravno definiše se?
   1. Zajedničkim kriterijumima
   2. Funkcionalnim zahtevima
   3. Bezbednosnim zahtevima
   4. Zajedničkim klasama
10. Neporicanje kao bezbednosna usluga obezbeđuje?
    1. celovitost podataka
    2. **da korisnik koji pošalje poruku ne može kasnije poreći da je to uradio**
    3. da ovlašćeni korisnici imaju pristup podacima i računarskim resursima kada su im potrebni
    4. da se podaci neautorizovano ne menjaju ili uništavaju
    5. pristup informacijama samo za one korisnike koji su ovlašćeni da tim informacijama pristupe
11. Bezbednosni ciljevi predstavljaju ciklus četiri faze?
    1. poverljivost, integritet i raspoloživost
    2. procena, prevencija, raspoloživost i odgovor
    3. prevencija, detekcija, celovitost i odgovor
    4. **procena, prevencija, detekcija i odgovor**
    5. privatnost, sigurnost, poverljivost, raspoloživost
12. Zahtev da samo ovlašćeni korisnici mogu da menjaju podatke naziva se?
    1. Provera identiteta
    2. Raspoloživost
    3. Neporicanje
    4. Kontrola pristupa
    5. **Integritet**
13. U kojoj fazi napadač odlučuje koje resurse će napasti?
    1. **ispitaj i proceni**
    2. odbij uslugu
    3. održi pristup
    4. eksploatiši i prodri
    5. povećaj privilegije
14. Odobrenje pristupa na određeni način jednom ili više objekata je?
    1. funkcija pristupa
    2. sesija
    3. lista prava
    4. **dozvola ili pravo pristupa**
    5. uloga
15. Kome se dodeljuje sigurnosna oznaka u mehanizmu kontrole pristupa?
    1. dodeljuje se nekom pravu pristupa
    2. **dodeljuje se nekom resursu**
    3. dodeljuje se nekom procesu
    4. dodeljuje se nekoj ulozi
    5. dodeljuje se nekom subjektu
16. Kako se nazivaju algoritmi kod kojih se originalna poruka šifruje po grupama (blokovima)?
    1. **blokovska šifra**
    2. supstitucija
    3. transpozicija
    4. šifra toka
    5. jednokratna beležnica
17. Jednosmerna funkcija za autentifikaciju poruke koja ne uključuje korišćenje tajnog ključa za generisanje malog bloka podataka, poznatog je kao ?
    1. kod za autentifikaciju
    2. **digitalno potpis**
    3. hash funkcija
    4. šifrovanje
18. Kako se naziva pravno lice koje izdaje elektronske sertifikate u skladu sa odredbama zakona o digitalnom potpisu?
    1. **sertifikaciono telo**
    2. elektronski sertifikat
    3. digitalni potpis
    4. kvalifikovani elektronski sertifikat
19. Čiji cilj je da dobije pristup sistemu ili da poveća nivo privilegija na sistemu?
    1. uljeza
    2. pošiljaoca
    3. primaoca
    4. **legitimnog korisnika**
    5. crva
20. Neporicanje kao bezbednosna usluga obezbeđuje?
    1. celovitost podataka
    2. **da korisnik koji pošalje poruku ne može kasnije poreći da je to uradio**
    3. da ovlašćeni korisnici imaju pristup podacima i računarskim resursima kada su im potrebni
    4. da se podaci neautorizovano ne menjaju ili uništavaju
    5. pristup informacijama samo za one korisnike koji su ovlašćeni da tim informacijama pristupe
21. Bezbednosni ciljevi predstavljaju ciklus četiri faze?
    1. poverljivost, integritet i raspoloživost
    2. procena, prevencija, raspoloživost i odgovor
    3. prevencija, detekcija, celovitost i odgovor
    4. **procena, prevencija, detekcija i odgovor**
    5. privatnost, sigurnost, poverljivost, raspoloživost
22. Zahtev da samo ovlašćeni korisnici mogu da menjaju podatke naziva se?
    1. Provera identiteta
    2. Raspoloživost
    3. Neporicanje
    4. Kontrola pristupa
    5. **Integritet**
23. U kojoj fazi napadač odlučuje koje resurse će napasti?
    1. **ispitaj i proceni**
    2. odbij uslugu
    3. održi pristup
    4. eksploatiši i prodri
    5. povećaj privilegije
24. Odobrenje pristupa na određeni način jednom ili više objekata je?
    1. funkcija pristupa
    2. sesija
    3. lista prava
    4. **dozvola ili pravo pristupa**
    5. uloga
25. Kome se dodeljuje sigurnosna oznaka u mehanizmu kontrole pristupa?
    1. dodeljuje se nekom pravu pristupa
    2. **dodeljuje se nekom resursu**
    3. dodeljuje se nekom procesu
    4. dodeljuje se nekoj ulozi
    5. dodeljuje se nekom subjektu
26. Kako se nazivaju algoritmi kod kojih se originalna poruka šifruje po grupama (blokovima)?
    1. **blokovska šifra**
    2. supstitucija
    3. transpozicija
    4. šifra toka
    5. jednokratna beležnica
27. Jednosmerna funkcija za autentifikaciju poruke koja ne uključuje korišćenje tajnog ključa za generisanje malog bloka podataka, poznatog je kao ?
    1. kod za autentifikaciju
    2. **digitalno potpis**
    3. hash funkcija
    4. šifrovanje
28. Kako se naziva pravno lice koje izdaje elektronske sertifikate u skladu sa odredbama zakona o digitalnom potpisu?
    1. **sertifikaciono telo**
    2. elektronski sertifikat
    3. digitalni potpis
    4. kvalifikovani elektronski sertifikat
29. Čiji cilj je da dobije pristup sistemu ili da poveća nivo privilegija na sistemu?
    1. uljeza
    2. pošiljaoca
    3. primaoca
    4. **legitimnog korisnika**
    5. crva
30. Pre upotrebe elektronske opreme za obradu podataka, važne informacije su najčešće čuvane u?
    1. magacinu
    2. sefu
    3. banci
    4. registrima
31. Raspoloživost kao bezbednosna usluga obezbedjuje?
    1. da ovlaćæeni korisnici imaju pristup podacima i računarskim resursima kada su im potrebni
    2. da se podaci neautorizovano ne menjaju ili uništavaju
    3. da korisnik koji pošalje poruku ne može kasnije poreći da je to uradio celovitost podataka
    4. pristup informacijama samo za one korisnike koji su ovlašćeni da tim informacijama pristupe
32. Integritet kao bezbednosna usluga obezbedju?
    1. pristup informacijama samo za one korisnike koji su ovlaši da tim informacijama pristupe
    2. da se podaci neautorizovano ne menjaju ili uništavaju
    3. da ovlašæeni korisnici imaju pristup podacima i računarskim resursima kada su im potrebni
    4. da korisnik koji pošalje poruku ne može kasnije poreći da je to uradio celovitost podataka
33. Bezbednosni ciljevi predstavljaju ciklus četiri faze?
    1. poverljivost, integritet i raspoloživost
    2. procena, prevencija, raspoloživost i odgovor
    3. prevencija, detekcija, celovitost i odgovor
    4. procena, prevencija, detekcija i odgovor
    5. privatnost, sigurnost, poverljivost, raspoloživost
34. Napad tokom koga se jedan entitet pretvara da je drugi naziva se?
    1. Ponovo pustiti
    2. Fabrikovanje
    3. Izmena poruke
    4. Odbijanje usluga
    5. Prerušavanje
35. Šta opisuje način na koji subjekat može pristupiti objektu?
    1. uloga
    2. pravo pristupa
    3. objekat
    4. subjekat
    5. model
36. Matematička funkcija koja se koristi za šifrovanje i dešifrovanje naziva se?
    1. kriptografski algoritam ili šifra
    2. otvoren tekst
    3. ključ
    4. šifrat
37. Otkrivanje ključa nekriptoanalitičkim metodama naziva:
    1. snaga kriptosistema
    2. napad
    3. šifrovanje
    4. sigurnost kriptosistema
    5. kompromitovanje
38. Koji bezbednosni mehanizam se koristi za proveru integriteta poruka?
    1. digitalni potpis
    2. kontrola pristupa
    3. šifrovanje
    4. autentifikacija poruk
39. Jednosmerna funkcija za autentifikaciju poruke koja ne uključuje korišćenje tajnog ključa za generisanje malog bloka podataka, poznatog je kao ?
    1. kod za autentifikaciju
    2. digitalno potpis
    3. hash funkcija
    4. šifrovanje

# Q2 I q3

1. Neporicanje kao bezbednosna usluga obezbeđuje?
   1. celovitost podataka
   2. **da korisnik koji pošalje poruku ne može kasnije poreći da je to uradio**
   3. da ovlašćeni korisnici imaju pristup podacima i računarskim resursima kada su im potrebni
   4. da se podaci neautorizovano ne menjaju ili uništavaju
   5. pristup informacijama samo za one korisnike koji su ovlašćeni da tim informacijama pristupe
2. Bezbednosni ciljevi predstavljaju ciklus četiri faze?
   1. poverljivost, integritet i raspoloživost
   2. procena, prevencija, raspoloživost i odgovor
   3. prevencija, detekcija, celovitost i odgovor
   4. **procena, prevencija, detekcija i odgovor**
   5. privatnost, sigurnost, poverljivost, raspoloživost
3. Zahtev da samo ovlašćeni korisnici mogu da menjaju podatke naziva se?
   1. Provera identiteta
   2. Raspoloživost
   3. Neporicanje
   4. Kontrola pristupa
   5. **Integritet**
4. U kojoj fazi napadač odlučuje koje resurse će napasti?
   1. **ispitaj i proceni**
   2. odbij uslugu
   3. održi pristup
   4. eksploatiši i prodri
   5. povećaj privilegije
5. Odobrenje pristupa na određeni način jednom ili više objekata je?
   1. funkcija pristupa
   2. sesija
   3. lista prava
   4. **dozvola ili pravo pristupa**
   5. uloga
6. Kome se dodeljuje sigurnosna oznaka u mehanizmu kontrole pristupa?
   1. dodeljuje se nekom pravu pristupa
   2. **dodeljuje se nekom resursu**
   3. dodeljuje se nekom procesu
   4. dodeljuje se nekoj ulozi
   5. dodeljuje se nekom subjektu
7. Kako se nazivaju algoritmi kod kojih se originalna poruka šifruje po grupama (blokovima)?
   1. **blokovska šifra**
   2. supstitucija
   3. transpozicija
   4. šifra toka
   5. jednokratna beležnica
8. Jednosmerna funkcija za autentifikaciju poruke koja ne uključuje korišćenje tajnog ključa za generisanje malog bloka podataka, poznatog je kao ?
   1. kod za autentifikaciju
   2. **digitalno potpis**
   3. hash funkcija
   4. šifrovanje
9. Kako se naziva pravno lice koje izdaje elektronske sertifikate u skladu sa odredbama zakona o digitalnom potpisu?
   1. **sertifikaciono telo**
   2. elektronski sertifikat
   3. digitalni potpis
   4. kvalifikovani elektronski sertifikat
10. Čiji cilj je da dobije pristup sistemu ili da poveća nivo privilegija na sistemu?
    1. uljeza
    2. pošiljaoca
    3. primaoca
    4. **legitimnog korisnika**
    5. crva
11. Neporicanje kao bezbednosna usluga obezbeđuje?
    1. celovitost podataka
    2. **da korisnik koji pošalje poruku ne može kasnije poreći da je to uradio**
    3. da ovlašćeni korisnici imaju pristup podacima i računarskim resursima kada su im potrebni
    4. da se podaci neautorizovano ne menjaju ili uništavaju
    5. pristup informacijama samo za one korisnike koji su ovlašćeni da tim informacijama pristupe
12. Bezbednosni ciljevi predstavljaju ciklus četiri faze?
    1. poverljivost, integritet i raspoloživost
    2. procena, prevencija, raspoloživost i odgovor
    3. prevencija, detekcija, celovitost i odgovor
    4. **procena, prevencija, detekcija i odgovor**
    5. privatnost, sigurnost, poverljivost, raspoloživost
13. Zahtev da samo ovlašćeni korisnici mogu da menjaju podatke naziva se?
    1. Provera identiteta
    2. Raspoloživost
    3. Neporicanje
    4. Kontrola pristupa
    5. **Integritet**
14. U kojoj fazi napadač odlučuje koje resurse će napasti?
    1. **ispitaj i proceni**
    2. odbij uslugu
    3. održi pristup
    4. eksploatiši i prodri
    5. povećaj privilegije
15. Odobrenje pristupa na određeni način jednom ili više objekata je?
    1. funkcija pristupa
    2. sesija
    3. lista prava
    4. **dozvola ili pravo pristupa**
    5. uloga
16. Kome se dodeljuje sigurnosna oznaka u mehanizmu kontrole pristupa?
    1. dodeljuje se nekom pravu pristupa
    2. **dodeljuje se nekom resursu**
    3. dodeljuje se nekom procesu
    4. dodeljuje se nekoj ulozi
    5. dodeljuje se nekom subjektu
17. Kako se nazivaju algoritmi kod kojih se originalna poruka šifruje po grupama (blokovima)?
    1. **blokovska šifra**
    2. supstitucija
    3. transpozicija
    4. šifra toka
    5. jednokratna beležnica
18. Jednosmerna funkcija za autentifikaciju poruke koja ne uključuje korišćenje tajnog ključa za generisanje malog bloka podataka, poznatog je kao ?
    1. kod za autentifikaciju
    2. **digitalno potpis**
    3. hash funkcija
    4. šifrovanje
19. Kako se naziva pravno lice koje izdaje elektronske sertifikate u skladu sa odredbama zakona o digitalnom potpisu?
    1. **sertifikaciono telo**
    2. elektronski sertifikat
    3. digitalni potpis
    4. kvalifikovani elektronski sertifikat
20. Čiji cilj je da dobije pristup sistemu ili da poveća nivo privilegija na sistemu?
    1. uljeza
    2. pošiljaoca
    3. primaoca
    4. **legitimnog korisnika**
    5. crva
21. Pre upotrebe elektronske opreme za obradu podataka, važne informacije su najčešće čuvane u?
    1. magacinu
    2. sefu
    3. banci
    4. registrima
22. Raspoloživost kao bezbednosna usluga obezbedjuje?
    1. da ovlaćæeni korisnici imaju pristup podacima i računarskim resursima kada su im potrebni
    2. da se podaci neautorizovano ne menjaju ili uništavaju
    3. da korisnik koji pošalje poruku ne može kasnije poreći da je to uradio celovitost podataka
    4. pristup informacijama samo za one korisnike koji su ovlašćeni da tim informacijama pristupe
23. Integritet kao bezbednosna usluga obezbedju?
    1. pristup informacijama samo za one korisnike koji su ovlaši da tim informacijama pristupe
    2. da se podaci neautorizovano ne menjaju ili uništavaju
    3. da ovlašæeni korisnici imaju pristup podacima i računarskim resursima kada su im potrebni
    4. da korisnik koji pošalje poruku ne može kasnije poreći da je to uradio celovitost podataka
24. Bezbednosni ciljevi predstavljaju ciklus četiri faze?
    1. poverljivost, integritet i raspoloživost
    2. procena, prevencija, raspoloživost i odgovor
    3. prevencija, detekcija, celovitost i odgovor
    4. procena, prevencija, detekcija i odgovor
    5. privatnost, sigurnost, poverljivost, raspoloživost
25. Napad tokom koga se jedan entitet pretvara da je drugi naziva se?
    1. Ponovo pustiti
    2. Fabrikovanje
    3. Izmena poruke
    4. Odbijanje usluga
    5. Prerušavanje
26. Šta opisuje način na koji subjekat može pristupiti objektu?
    1. uloga
    2. pravo pristupa
    3. objekat
    4. subjekat
    5. model
27. Matematička funkcija koja se koristi za šifrovanje i dešifrovanje naziva se?
    1. kriptografski algoritam ili šifra
    2. otvoren tekst
    3. ključ
    4. šifrat
28. Otkrivanje ključa nekriptoanalitičkim metodama naziva:
    1. snaga kriptosistema
    2. napad
    3. šifrovanje
    4. sigurnost kriptosistema
    5. kompromitovanje
29. Koji bezbednosni mehanizam se koristi za proveru integriteta poruka?
    1. digitalni potpis
    2. kontrola pristupa
    3. šifrovanje
    4. autentifikacija poruk
30. Jednosmerna funkcija za autentifikaciju poruke koja ne uključuje korišćenje tajnog ključa za generisanje malog bloka podataka, poznatog je kao ?
    1. kod za autentifikaciju
    2. digitalno potpis
    3. hash funkcija
    4. šifrovanje

**Q2. [10]** Odgovoriti na sledeća pitanja:

1. Detekcija uljeza zasniva se na pretpostavci?
   1. da se ponašanje uljeza ne razlikuje od legitimnog korisnika na način koji se može kvantifikovati
   2. **da se ponašanje uljeza razlikuje od legitimnog korisnika na način koji se može kvantifikovati**
   3. da je ponašanje uljeza definisano modelom ponašanja prethodnih napada
   4. da je ponašanje uljeza predvidljivo
   5. da se ponašanje uljeza može detektovati hardverom
2. Ko beleži svaki audit zapis generisan od strane audit sistema za kolekciju?
   1. menadžer
   2. podsistem za upozoravanje
   3. agent
   4. **analizator**
   5. Operater
3. Utvrđeni (bastion) host je sistem identifikovani od strane zaštitnog zida administratora kao?
   1. slaba kritična tačka
   2. „uska grla” između unutrašnjih i spoljnih mreža
   3. **jaka kritična tačka**
   4. prolazna tačka
   5. tačka za audit
4. Šta obezbeđuje AH protokol sigurnosti na mrežnom sloju Interneta?
   1. poverljivost
   2. **autentifikaciju i integritet podatak**
   3. kontrolu identiteta
   4. autentifikaciju, integritet podataka i poverljivost
   5. autentifikaciju i kontrolu identiteta
5. Koja dva tipa upravljanja ključem određuje IPSec arhitektura dokumenta?
   1. **transportno i automatsko**
   2. tunelski i automatsko
   3. fizičko i tunelski
   4. fizičko i transportno
6. IPSec je skup protokola koji omogućava bezbednost na?
   1. Gateway
   2. Transportnom sloju
   3. Zaštitnom zidu
   4. **Mrežnom sloju**
   5. Aplikativnom sloju
7. Na kom algoritmu šifrovanja je zasnovan SSL protokol?
   1. SHA
   2. Simetričnom
   3. DSS
   4. **Asimetričnom**
   5. MAC

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

* 1. S/MIME
  2. TLS
  3. SSL
  4. **Kerberos**
  5. IP/IPSec

1. Koji je bezbednosni protokol u IEEE802.11 bežičnim lokalnim mrežama?
   1. IPsec
   2. Bluetooth
   3. **WEP**
   4. WPA2
   5. WPA
2. Koja dužina ključa za WEP protokol je definisana standardom IEE 802.11?
   1. 40 bita
   2. **128 bita**
   3. 56 bita
   4. 152 bita
   5. 104 bita

**Q3. [10]** Odgovoriti na sledeća pitanja:

1. Protokol IEEE802.11i pored bežičnog klijenta i pristupne tačke AP definiše?
   1. WEP, EAP ključ
   2. **server za proveru identiteta**
   3. passkey, ključ sesije
   4. dinamičko definisanje ključa šifrovanja
   5. upareni glavni i privremeni ključ
2. Šta na Unix sistemu nije predstavljeno kao datoteka?
   1. objekti i grupe
   2. grupe i akcije
   3. **korisnici i grupe**
   4. korisnici i objekti
   5. korisnici i akcije
3. Šta obuhvata ranjivost Linux standardnih distribucija?
   1. **prekoračenje bafera, problemi sinhronizacije (race), DoS napad, ranjivost Web aplikacija, napad rootkit**
   2. korisnik ili proces sa root privilegijama
   3. prostor Linux jezgra i prostor svih ostalih servisa
   4. prekoračenje bafera, DoS, neograničena kontrola pristupa
   5. DoS napad, ranjivost Web aplikacija, kontrola pristupa zasnovana na ulogama
4. U kojoj datoteci su definisane grupe?
   1. /etc/shadow
   2. /etc/secure
   3. /etc/passwd
   4. /etc/root
   5. **/etc/group**
5. Koji model elektronske trgovine je danas dominantan na internetu?
   1. Consumer to Consumer (C2C)
   2. Consumer to Business (C2B)
   3. Business to Employee (B2E)
   4. Business to Consumer (B2C)
   5. **Business to Business (B2B)**
6. U kom modelu je on-line aukcija jedna od mogućnosti on-line kupovine?
   1. Business to Business (B2B)
   2. Consumer to Consumer (C2C)
   3. **Consumer to Business (C2B)**
   4. Business to Consumer (B2C)
7. Kako se naziva plastična kartica sa ugrađenim mikroprocesorom i memorijom?
   1. digitalni ček
   2. elektronski ček
   3. elektronski novac
   4. elektronska kreditna kartica
   5. **smart kartica**
8. Pojedini napadi koriste obične ljudske mane radi ostvarivanja pritupa koji su inače zabranjeni. Kako se nazivaju takvi napadi?
   1. IDS sistem
   2. spoljašnje obezbeđenje
   3. **socijalni napadi**
   4. biometrija
   5. CHAP identifikator
9. Kako se naziva lista formatiranih zapisa događaja?
   1. audit arhiver
   2. **bezbednosni audit tragovi**
   3. audit zapis
   4. audit provajder
   5. audit analizer
10. Koji log fajl sadrže informacije o validnim i ne validnim pokušajima logovanja kao i događaje koji regulišu korišćenje resursa?
    1. **security log**
    2. appliction log
    3. mrežni log
    4. system log

30.1.2020.

**Q2. [10]** Odgovoriti na sledeća pitanja:

1. Detekcija uljeza zasniva se na pretpostavci?
   1. da se ponašanje uljeza ne razlikuje od legitimnog korisnika na način koji se može kvantifikovati
   2. **da se ponašanje uljeza razlikuje od legitimnog korisnika na način koji se može kvantifikovati**
   3. da je ponašanje uljeza definisano modelom ponašanja prethodnih napada
   4. da je ponašanje uljeza predvidljivo
   5. da se ponašanje uljeza može detektovati hardverom
2. Ko beleži svaki audit zapis generisan od strane audit sistema za kolekciju?
   1. menadžer
   2. podsistem za upozoravanje
   3. agent
   4. **analizator**
   5. Operater
3. Utvrđeni (bastion) host je sistem identifikovani od strane zaštitnog zida administratora kao?
   1. slaba kritična tačka
   2. „uska grla” između unutrašnjih i spoljnih mreža
   3. **jaka kritična tačka**
   4. prolazna tačka
   5. tačka za audit
4. Šta obezbeđuje AH protokol sigurnosti na mrežnom sloju Interneta?
   1. poverljivost
   2. **autentifikaciju i integritet podatak**
   3. kontrolu identiteta
   4. autentifikaciju, integritet podataka i poverljivost
   5. autentifikaciju i kontrolu identiteta
5. IPSec je skup protokola koji omogućava bezbednost na?
   1. Gateway
   2. Transportnom sloju
   3. Zaštitnom zidu
   4. **Mrežnom sloju**
   5. Aplikativnom sloju
6. Na kom algoritmu šifrovanja je zasnovan SSL protokol?
   1. SHA
   2. Simetričnom
   3. DSS
   4. **Asimetričnom**
   5. MAC

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

* 1. S/MIME
  2. TLS
  3. SSL
  4. **Kerberos**
  5. IP/IPSec

1. Koji je bezbednosni protokol u IEEE802.11 bežičnim lokalnim mrežama?
   1. IPsec
   2. Bluetooth
   3. **WEP**
   4. WPA2
   5. WPA
2. Koja dužina ključa za WEP protokol je definisana standardom IEE 802.11?
   1. 40 bita
   2. **128 bita**
   3. 56 bita
   4. 152 bita
   5. 104 bita

**Q3. [10]** Odgovoriti na sledeća pitanja:

1. Protokol IEEE802.11i pored bežičnog klijenta i pristupne tačke AP definiše?
   1. WEP, EAP ključ
   2. **server za proveru identiteta**
   3. passkey, ključ sesije
   4. dinamičko definisanje ključa šifrovanja
   5. upareni glavni i privremeni ključ
2. Šta na Unix sistemu nije predstavljeno kao datoteka?
   1. objekti i grupe
   2. grupe i akcije
   3. **korisnici i grupe**
   4. korisnici i objekti
   5. korisnici i akcije
3. Šta obuhvata ranjivost Linux standardnih distribucija?
   1. **prekoračenje bafera, problemi sinhronizacije (race), DoS napad, ranjivost Web aplikacija, napad rootkit**
   2. korisnik ili proces sa root privilegijama
   3. prostor Linux jezgra i prostor svih ostalih servisa
   4. prekoračenje bafera, DoS, neograničena kontrola pristupa
   5. DoS napad, ranjivost Web aplikacija, kontrola pristupa zasnovana na ulogama
4. U kojoj datoteci su definisane grupe?
   1. /etc/shadow
   2. /etc/secure
   3. /etc/passwd
   4. /etc/root
   5. **/etc/group**
5. Koji model elektronske trgovine je danas dominantan na internetu?
   1. Consumer to Consumer (C2C)
   2. Consumer to Business (C2B)
   3. Business to Employee (B2E)
   4. Business to Consumer (B2C)
   5. **Business to Business (B2B)**
6. U kom modelu je on-line aukcija jedna od mogućnosti on-line kupovine?
   1. Business to Business (B2B)
   2. Consumer to Consumer (C2C)
   3. **Consumer to Business (C2B**)
   4. Business to Consumer (B2C)
7. Kako se naziva plastična kartica sa ugrađenim mikroprocesorom i memorijom?
   1. digitalni ček
   2. elektronski ček
   3. elektronski novac
   4. elektronska kreditna kartica
   5. **smart kartica**
8. Pojedini napadi koriste obične ljudske mane radi ostvarivanja pritupa koji su inače zabranjeni. Kako se nazivaju takvi napadi?
   1. IDS sistem
   2. spoljašnje obezbeđenje
   3. **socijalni napadi**
   4. biometrija
   5. CHAP identifikator
9. Kako se naziva lista formatiranih zapisa događaja?
   1. audit arhiver
   2. **bezbednosni audit tragovi**
   3. audit zapis
   4. audit provajder
   5. audit analizer
10. Koji log fajl sadrže informacije o validnim i ne validnim pokušajima logovanja kao i događaje koji regulišu korišćenje resursa?
    1. **security log**
    2. appliction log
    3. mrežni log
    4. system log

2018.

4.7.2018.

1. Detekcija uljeza zasniva se na pretpostavci?
   1. da se ponašanje uljeza ne razlikuje od legitimnog korisnika na način koji se može kvantifikovati
   2. da se ponašanje uljeza razlikuje od legitimnog korisnika na način koji se može kvantifikovati
   3. da je ponašanje uljeza definisano modelom ponašanja prethodnih napada
   4. da je ponašanje uljeza predvidljivo
   5. da se ponašanje uljeza može detktovati hardverom
2. Koji IDS sistem je zasnovan na računarima koji su određeni za metu eventualnih napada?
   1. IDS zasnovan na hostu
   2. SNORT
   3. Lažni “mamci”
   4. IDS zasnovan na mreži
   5. Audit zapisa
3. Koji zaštitni zid kontroliše saobraćaj izmedju ličnog računara ili radne stanice sa jedne strane, i Interneta ili mreže preduzeća sa druge strane?
   1. zaštitni zid zasnovan na host
   2. lični zaštitni zid
   3. ruter
   4. utvrdjeni zaštitni zid
   5. SOCKS
4. Koje tri funkcionalne oblasti obuhvata IPSec protokol?
   1. proveru identiteta, povjerljivost i digitalni potpis
   2. kontrolu rutiranja, povjerljivost i upravljanje ključevima
   3. autentifikacija, integritet i upravljanje ključevima
   4. proveru identiteta, povjerljivost i upravljanje ključevima
   5. algoritam za šifrovanje, digitalni potpies i upravljanje ključevima
5. Oakley protokol razmene ključa zasnovan je na?
   1. HMAC kodu
   2. digitalnom potpisu
   3. asimetričnom algoritmu šifrovanja
   4. Hash kodu
   5. Diffie-Hellman algoritmu
6. Koji protokoli osiguravaju transportni sloj?
   1. SSL, TLS
   2. Kerberos, S/MIME
   3. UDP
   4. IP/IPSec
   5. TCP
7. Koji napadi uključuju otkrivanje drugih korisnika, ubacivanje poruka u tranzitu izmedju klijenta i servera i ubacivanje informacija na web sajt?
   1. Reprodukovanje
   2. DoS
   3. Upad
   4. Aktivni
   5. Pasivni
8. Kako se naziva tehnologija malih bežičnih mreža dimenzionisanih za male udaljenosti koje u gradskim uslovima iznose od nekoliko desetina do nekoliko stotina metara?
   1. Bluetooth
   2. WWAN
   3. RFID
   4. bezična lokalna mreža - WLAN
   5. WPAN
9. Kod koje bežične mreže razlikujemo "ad hoc" i "infrastrukturne" veze?
   1. WWAN
   2. WPAN
   3. WLAN
   4. Bluetooth
   5. RFID

**Q3. [10]** Odgovoriti na sledeća pitanja:

1. Kako se naziva direktna veza dva računara ili drugih uređaja koji imaju ugrađene module za WLAN komunikaciju?
   1. RFID
   2. WPAN
   3. ad hoc
   4. GSM
   5. infrastrukturna
2. Ko može da menja dozvole objekta?
   1. svi korisnici
   2. Kernel
   3. grupa
   4. vlasnik
   5. subjekat
3. Šta obuhvata ranjivost Linux standardnih distribucija?
   1. prekoračenje bafera, problemi sinhronizacije (race), DoS napad, ranjivost Web aplikacija, napad rootkit
   2. korisnik ili proces sa root privilegijama
   3. prostor Linux jezgra i prostor svih ostalih servisa
   4. prekoračenje bafera, DoS, neograničena kontrola pristupa
   5. DoS napad, ranjivost Web aplikacija, kontrola pristupa zasnovana na ulogama
4. Koji bezbednosni model je implementiran u SELinux a zasniva se na Bell-LaPadula (BLP) modelu?
   1. bezbednost na više nivoa
   2. Type Enforcement
   3. RBAC
   4. DAC
   5. MAC
5. Kako se naziva plastična kartica sa ugrađenim mikroprocesorom i memorijom?
   1. digitalni ček
   2. elektronski ček
   3. elektronski novac
   4. elektronska kreditna kartica
   5. smart kartica
6. Koji bezbednosni servis obezbeđuje da se novac ne može preuzimati sa računa potrošača ili smart kartice bez eksplicitne dozvole?
   1. integritet plaćanja
   2. tajnost plaćanja
   3. autorizacija plaćanja
   4. autentifikacija plaćanja
   5. neporecivost plaćanja
7. Koji bezbednosni servis plaćanja sprečavaju ponovno korišćenje i falsifikovanje elektronskih novčanica?
   1. bezbednosti smart kartica
   2. transakcioni
   3. bezbednosti digitalnih čekova
   4. bezbednosti platnih kartica
   5. bezbednosti digitalnog novca
8. Kako se naziva informacija uskadištena ili prenošena u digitalnoj formi koja se koristi u sudskom postupku i mogu se koristiti na suđenju?
   1. pravni dokaz
   2. informatički dokaz
   3. proveren dokaz
   4. digitalni dokaz
9. Kako se naziva proces sprečavanja pristupa računarskim sistemima u nekoj zgradi?
   1. spoljašnje obezbeđenje
   2. IDS sistemi
   3. video nadzor
   4. sigurnosne zone
   5. kontrola pristupa
10. Koji prestup ima najveći faktor rasta u oblasti kompjuterskog kriminala?
    1. krađa labtop računara
    2. krađa identiteta
    3. krađa mobilnih telefona
    4. krađa prenosnih memorija
    5. neovlašćen pristup

21.6.2018

**Q1. [10]** Odgovoriti na sledeća pitanja:

1. Slabost u sistemu koje omogcavaju napadaču da naruši integritet sistema naziva se?

a) procena rizika

* 1. izloženost sistema
  2. upravljanje rizikom
  3. osetljivost sistema
  4. ranjivost

1. Šta opisuje način na koji subjekat može pristupiti objektu?
   1. objekat
   2. subjekat
   3. pravo pristupa
   4. model
   5. uloga

1. Za šta se koristi BIBA model?
   1. tok informacija nagore
   2. pravila za zaštitu integriteta informacija
   3. za sprečavanje mešanja bezbednosnih funkcija
   4. liste kontrole pristupa i liste sposobnosti
   5. poverljivost klasifikovanih informacija

1. Koji je od sledećih je napad na raspoloživost?
   1. presretanje
   2. presecanje
   3. izmena
   4. fabrikacija
   5. nijedan od navedenih

1. Koji je od sledećih na napad na integritet mreže?
   1. presecanje
   2. izmena
   3. fabrikacija
   4. nijedan od navedenih
   5. presretanje

1. Koji model je razvijen za komercijalne aplikacije u kojima može nastati sukob interesa?
   1. Model toka informacija
   2. BLP model
   3. Biba model
   4. Clark-Wilson model
   5. Chinesse Wall model

1. Kako se naziva algoritam kod koga se otvoreni teksta obrađuje zamenom pozicija karaktera?
   1. blokovska šifra
   2. supstitucija
   3. transpozicija

|  |
| --- |
|  |

* 1. jednokratna beležnica fra toka

. Pokušaj kriptoa nalize u cilju otkrivanja algoritma šifre, ključa ili otvorenog teksta naziva? a) sigurnost kriptosistema

* 1. šifrovanje
  2. kompromitovanje
  3. snaga kriptosistema
  4. napad

**Q2. [10]** Odgovoriti na sledeća pitanja:

1. Koji algoritam je do pojave kriptoanalize i napada grubom silom bio najčešće korišćen siguran hash algoritam?
   1. RSA
   2. DSS
   3. MD5
   4. SHA

1. Šta podrazumeva scenario za distribuciju ključeva pomoću centra KDC?
   1. svaki korisnik deli jedinstveni javni ključ sa KDC
   2. svaki korisnik deli jedinstveni privatni ključ sa KDC
   3. svaki korisnik deli jedinstveni master ključ sa KDC
   4. svaki korisnik deli ključ sesije sa KDC

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

a) šifrovanje

* 1. kriptografski sistem
  2. dešifrovanje
  3. kriptografski algoritam