IT381 Questions

Short questions

Q: Komponente informacionog sistema su:
A: ljudi, procedure, hardver, softver, mreža I podaci

Q: Kontola pristupa kao bezbednosna usluga dozvoljava:
A: Da ovlašćeni korisnici imaju pristup podacima I računarskim resursima kada sui m potrebni

Q: Zahtevi da samo ovlašćeni korisnici mogu da menjaju podatke naziva se:
A: kontrola pristupa

Q: Ometanje ili spečavanje normalnog korišćenja ili upravljanja komunikacijskim obejtima naziva se?
A: Izmena poruke

Q: Fragmenti koda koji se ubacuju u druge legitimne programe su:
A: Virus

Q: Odobrenje pristupa na određeni način jednom ili viš eobjekata je:
A: Sesija

Q: Matematička funkcija koja se koristi za šifrovanje I dešifovranje naziva se:
A: Kriptograski algoritam ili šifra

Q: Kada cena kriptoanalize premašuje vrednost šifrovanih informacija kažemo da je kritptografski sistem:
A: Siguran

Q: Slabost u sistemu koje omogcavaju napadaču da narusi̇ integritet sistema naziva se?
A: Ranjivost

Q: Sťa opisuje nacĭn na koji subjekat može pristupiti objektu?
A: Pravo pristupa

Q: Zasťa se koristi BLP model?
A: Poverljivost klasifikovanih informacija

Q: Zašta se koristi BIBA model?
A: Pravila za zaštitu integriteta informacija

Q: Kako se dele aktivni napadi?
A: prerušavanje, ponovo pustiti, izmena poruka, odbijanje usluga

Q: Čime se bavi bezbednost informacija?
A: prikupljanjem, protokom i dotokom svih neophodnih podataka

Q: Bezbednosni mehanizmi su projektovani da?
A: detektuju, spreče ili oporave sistem od napada

Q: Bezbednosni ciljevi predstavljaju ciklus Četiri faze?
A: procena, prevencija, detekcija i odgovor

Q: Željeno sigurnosno ponašanje sistema definisano je:
A: Funkcionalnim zahtevima

Q: Osnov za dobijanje poverenja da su zahtevane bezbednosne mere efikasne i da su implementirane ispravno definiše se:
A: Bezbednosnim zahtevima

Q: Napad tokom koga se jedan entitet pretvara da je drugi naziva se?
A: Prerušavanje

Q: Proces uravnotežavanja troškova za zaštitu od rizika i troškova od izlošenosti riziku naziva se?
A: Upravljanje rizikom

Q: Kako se zovu kolone u DAC matrici pristupa?
A: Liste za kontrole pristupa

Q: Koji od sledećiš je napad na raspoloživost?
A: Napad na raspoloživost može da uključuje brisanje podataka ili pad sistema, ali isto tako može sprečiti pristup sistemu smanjenjem ili preopterećenjem komunikacionih kanala za taj sistem.

Q: Koji je od sledećiš napad na integrited mreže?
A: Integritet je povređen kada zaposleni (slučajno ili zlonamerno) briše važne datoteke, kada je računar zaražen računarskim virusom, kada je radnik u mogućnosti da promeni svoju platu na platnom spisku u bazi podataka, kada neko može da baci veliki broj glasova u online anketi, i tako dalje. (izmena)

Q: Koji model je razvijen za komercijalne aplikacije u kojima može nastati sukob interesa?
A: Chinesse Wall model

Q: Osnov za dobijanje poverenja da su zahtevane bezbednosne mere efikasne i da su implementirane ispravno definiše se?
A: Bezbednosnim zahtevima

Q: Kako se naziva algoritam kod koga se otvoreni teksta obrađuje zamenom pozicija karaktera?
A: supstitucija

Q: Kako se naziva algoritam kod koga se otvoreni teksta obrađuje bit po bit (nekad bajt po bajt)?
A: Šifra toka

Q: Pokušaj kripto analize u cilju otkrivanja algoritma šifre, ključa ili otvorenog teksta naziva?
A: Napad

Q: Koji algoritam je do pojave kriptoanalize I napada grubom silom bio najčešće korišćen siguran hash algoritam?

A: MD5

Q: Kako se naziva kriptografska tehnika koja ukazuje na vlasnika ili stvaraoca dokumenta ili označava nečiju saglanost sa sadržajem dokumenta?
A: digitalni potpis

Q: Šta podrazumeva scenario za distribuciju ključeva pomoću centra KDC?
A: Svaki korisnik deli jedinstveni master ključ sa KDC

Q: Zamena međusobnog položaja elemenata otvorenog teksta, tj. Otvoren tekst se ne menja, menja se samo međusobni položaj elemenata otvorenog teksta je?
A: transpozicija

Q: Koji ključ se koristi za vreme trajanja jedne logičke veze a onda se uništava?
A: ključ sesije

Q: nauka koja se bavi izučavanjem i definisanjem metoda za zaštitu informacija i izučavanjem i pronalaženjem metoda za otkrivanje šifrovanih informacija naziva se?
A: Kriptologija

Q: Šta predstavlja algoritam sa svim mogućim otvorenim tekstovima, šifratima I ključevima?
A: Kriptografski sistem (kripto sistem)

Q: Kojim bezbednosnim servisom se obezbeđuje zaštita od oštećenja, pomoću jednog od entiteta uključenih u komunikaciju ili deo komunikacije?
A: Poverljivost

Q: Šta obezbeđuje ESP protocol sigunosti na mrežnom sloju interneta?
A: autentifikaciju, integrated podataka I poverljivost

Q: Kaji algoritam za šifrovanja mora da se podržava implementacija ESP protokola?
A: DES

Q: Koje dve usluge nudi SSL protokol za pisanje za SSL konekciju?
A: Poverljivost I integrated podataka

Q: PGP (Pretty Good Privacy) je bezbednosni progam za?
A: e-poštu

Q: Kako se naziva tehnologija malih bežičnih mreža dimenzionisanih za male udaljenosti koje u gradskim uslovima iznose od nekoliko desetina do nekoliko stotina metara?
A: bežična lokalna mreža – WLAN

Q: Koja mreže rade na većim udaljenostima (udaljenost prijemnika I odašiljača može iznositi I do 50km)?
A: WPAN

Q: Koja dva sloja OSI modela definiše standard za bežične mreže?
A: Fizički (PHY) I sloj podataka (MAC)

Q: Koje tri bezbednosne usluge definiše IEEE802.11 za WLAN
A: Provera identiteta, poverljivost I integrated

Q: Koja dužina ključa za WEP protokol je definisana standardom IEE802.11
A: 104 bita

Q: Koji ključ se koristi za šifrovanje podataka koji se prenose mobilnom mrežom?
A: Generisani ključ Kc

Q: U kom modelu potršać zahteva proizvod ili sulugu od prodavca, tako što postavlja svoh zahtev putem interneta a pdrodavci pregledaju zahteve I daju ponude?
A: Consumer to Business (C2B)

Q: Najčešći updati u sistem elektronskog poslovanja su od:
A: Autorizaovani zaposleni

Q: Kako se naziva sigurnosni servis koji prati I analizira događaj na sistemu ili mreži sa ciljem pružavnja upozorenja da je došlo do pokušaja pristupa resursima Sistema na neovlašćeni način?
A: Detekcija upada

Q: Koji deo Sistema je somišen kako bi se odvukao napadač od pristupa osetljivom sistemu sa značajnim podacima I da administrator može prikupiti informacije o aktivnostima napdatača?
A: Lažni mamac (honeypot)

Q: Kojim bezbednosnim servisom se obezbeđuje zaštita od štoćenja, pomoću jednog od entiteta uključenih u komunikaciju ili deo komunikacije?
A: Poverljivost

Q: Kojim bezbednosni mehanizam se koristi za trasformaciju podataka u obliku koji nije razmiljiv za čitanje:
A: Primena metemtičkih algoritama

Q: Kako se naziva skup protokola koji omogućavaju bezbednost na mrežnom sloju?
A: IP Security

Q: Koja dva tipa upravljanja ključem određuje IPSec arhitektura dokumenta?
A: Transportno I automatsko

Q: Šta je uloga TGS servera u Kerberos protokolu provere identiteta?
A: Isporuka ključeva

Q: Koji protokol je pouzdana treća strana usluge provere identiteta?
A: Kerberos

Q: Kako se naziva otvorena bezbednosna I sigurnosna specifikacija dizajnirana za zaštitu transkacija kreditnim karticama na internetu?
A: SET (Secure Electronic Transaction)

Q: Podatak ili fizički objekat postaje dokaza jedino kada je prikupljen od strane?
A: Ovlašćenog lica

Q: Koja tema bezbednosne politike uključuje definiciju informacione bezbednosti, njene ciljeve I sveukupni cilj I važnost?
A: Principi

Q: Koji element bezbednosti štiti ljude I imovinu unutar celog poslovnog prostora, objekta ili zgrada?
A: Korporativna bezbednost

Q: Koji log fajl sadrži informacije o validnim I ne validnim pokušajima logovanja kao I događaje koji regulišu korišćenje resursa?
A: security log

Q: U kom koraku kompjuterske forenzike se vrši izdvajanje dokaza iz prikupljenog materijala?
A: Ispitivanje

Q: Koja su ograničenja zaštitnih zidova?
A: Zaštitni zid ne može da zaštititi od napada koji zaobilaze (bypass) zaštitni zid. • Zaštitni zid ne štiti potpuno od internih pretnji, kao što je nezadovoljan zaposleni ili zaposleni koji nenamerno sarađuje sa spoljašnjim napadačem. • Nepropisno obezbeđenim bežičnom LAN mrežom može se pristupiti izvan organizacije.

Q: Koji napadi uključuju otkrivanje drugih korisnika, ubacivanje poruka u tranzitu izmedju klijenta I server I ubacivanje informacija na web sajt?
A: Aktivni

Q: Čiji cilj je da dobije pristup sistemu ili da povećava nivo privilegija na sistemu?
A: Uljeza

Q: Koji IDS sistem je softver otvorenog koda, visoko podesiv I prenosan?
A: SNORT

Q: Proces ili uređaj u vezi procesa, koji je projektovan da detektuje, spreči ili da se oporavi od napada na bezbednost naziva se?
A: Mehanizam bezbednosti

Q: Šta obuhvata bezbednost računarskih mreža
A: Dodavanje AH zaglavlja

Q: Koji režim rada pruža zaštitu za ceo IP paket
A: tunelski

Q: Server za izdavanje karata TGS (tiket-grant server) je deo kog protokola?
A: Kerberos

Q: Kada započinje bezbednost Windows Sistema?
A: po završetku instalacije operativnog sistema

Q: Kada započinje bezbednost linux Sistema?
A: U trenutku instalacije operativnog Sistema

Q: Koji oblik provere identiteta, kod bežičnih mreža, koristi kriptografske tehnike?
A: Provera identiteta deljenim kjućem

Q: Kojom komandom se mogu menjati dozvole za svaku datoteku?
A: chmod

Q: Ko je najniži nova OS-a?
A: Jezgro – Kernel

Q: Kome se može dodeliti Linux korisnički nalog?
A: Svima koji raspolažu mogučnost da rade sa datotekama

Q: Na čemu se zasniva linux tradicionalni model bezbednosti?
A: Ljudi ili prcesi sa "root" privilegijama mogu raditi šta god hoće a drugi nalozi su ograničeni

Q: Koja usluga na linux sistemu ograničava mogućnosti brisanja stvari u direktorjiumu?
A: setigid

Q: U kojoj datoteci su definisane grupe?
A: -etc-group

Q: Koji su osnovni bezbednosni blokovi MS windows arhitekture?
A: SRM, LSA, SAM, AD, WinLogon, NetLogon

Q: Kako se naziva reakcija na detektovan događaj koji predstavlja potencijalno narušavanje bezbednosti?
A: Audit odgovor

Q: Kako se naziva informacija uskladištena ili pronošena u digitalnoj formi koja se koristi u sudskom postupku I mogu se koristiti na suđenju?
A: digitalni dokaz

Q: Pojedini napadi koriste obične ljudske mane radi ostvarivanja pristupa koji su inače zabranjeni. Kako se nazivaju takvi napadi?
A: Socijalni inženjering

Q: U kom koraku digitalne forenzike se vrši izrada dokumentacije o nalazima?
A: Izveštaj

Q: U kom koraku digitalne forenzike se vrši izbor alata I opreme za forenzičku istragu?
A: Priprema

Q: U kom koraku kopijuterske forenzike se vrši izdvajanje dokaza iz prikupljenog materijala?
A: Ispitivanje

Q: Između koje tri strane je moguće organizovati elektronsku transakciju?
A: Vlade, kompanija I korisnika

Q: Koji način plaćaja je napopularniji?
A: Plaćanje kreditnim karticama I homebanking

Long questions

Q: Šta je reverzni proksi (eng. Reverse proxy)?
A: Vrsta proksi servera koji priprema resurse u ime klijenta sa jednog ili više servera. Nakon čega se resursi vraćaju klijentu kao da potiču iz samog web servera.

Q: Koje vrste zaštitne barijere (engl. firefall) postoje?
A: Trip tipa mreže zaštitnih zidova: 1) Filtriranje paketa 2) Mrežni prolazi aplikativnog nivoa ili gateways 3) Prolazi na nivou kanala komunikacijskih podataka

Q: Šta je glavna uloga zaštitne barijere (eng. firewall)
A: Zaštitni zidovi se koriste za predstavljanje kontrolnih tačaka bezbednosti na granice privatnih mreža. Mrećna barijejra ispituje sve pakete koji prolaze između private mreže I interneta. Ukoliko paket zadovoljava pravila definisana listama za kontrolu pristupa, mrežna barijera dozvoljava ili zabranjuje protok tih paketa.

Q: Detaljno objasniti napad koji se zove “buffer overflow” napad.
A: Prepunjenost bafera predstavlja najčešći napad pri pokušaju neovlašćenog pristupanja sistemu. Ovlašćeni korisnici biraju ovu vrstu napada kako bi ostvarili veća prava od oniih koji imaju. Napadač koristi grešku u program I šalje više ulaznih podaka nego što program može da podrži, prepunjava ulazno polje sve dok ne dođe do steak. Nakon toga puni stek svojim kodom, koji izvršava neku konkretnu komandu.

Q: Koje vrste ranjivosti postoje?
A: Ranjivost se odnosi na slabosti u sistemu koja omogućava napadaču da naruši integrated tog Sistema. Nastaje kao poslodica lošeg projektovanja ili implementacije aplikacija. Tipovi ranjivosti: - Buffer overflow: niz se smešta u odredište koje je kraće od njegove dužine I program biva prepisan slonamernim kodom – Backdoor turina: koristi se za održavanje programa. Programeri postavljaju backdoor rutine kako bi kasnije, ukoliko je potrebno zaobišli mehanizme kontrole.

Q: Objasniti BIBA model bezbednosti
A: BIBA model bezbednosti je model koji se koristi za pravila za zaštitu bezbednosti informacija. Politika modela zasnovana je na osnovu pravila: - Jednostavnog integriteta, što znači da subjekat može menjati objekat samo ukolliko je nivo subjekta doninantniji nad nivoom objekta – Integriteta ograničavanja, subjekat može čitati objekat ukoliko je nivo integriteta subjekta doninantan nad nivoom integriteta objekta – Svojstva prizivanja, subjekat može tražiti dugri subject ukoliko je nivo integriteta prvog subjekta doninanta nad nivoom integriteta drugog subjekta

Q: Šta je slojevita zaštita I kako se koristi?
A: Predstavlja raslojavanje I preklapanje bezbednosnih mera. Možemo zamisliti da slojeviti zaštitu predstavljaju slojevi luka, sa podacima u jezgru luka. Ljudi su spoljašni sloj luka, a sigurnost mreže, host-zasnovana bezbednost I aplikacije bezbednosti čine unutrašnje slojeve luka. Korišćenje slojevite strategije trebalo bi da ako jedna odbrambena mera ne uspe, postoje I druge mere u odbrani koje će nastaviti da obezbeđuju zaštitu.

Q: Šta je ranjivost I koje vrste ranjivosti postoje?
A: Ranjivost se odnosi na slabosti u sistemu koja omogućava napadaču da naruši integritet tog Sistema. Nastaje kao posledica lošeg projektovanja ili implementacije aplikacija. Buffer overflow – niz se smešta u odredište koje je kraće od njegove dužine I program biva prepisan zlonamernim kodom. Backdoor rutina –

koristi se za održavanje programa. Programeri postavljaju backdoor rutine kako bi kasnije ukoliko je potrebno zaobišli mehanizme kontrole.

Q: Navesti neke od modela kontrole pristupa I objasniti ukratko kako funkcionišu.
A: Modeli kontrole pristupa koje koriste se dele u dve grupe: modele temeljene na mogućnostima I modele temeljene na listama kontrole pristupa (ACL – Access Control List). Tri osnovna metoda za kontrole pristupa:

- Diskrecioni model (DAC – Discretionary Access Control): Neograničena kontrola pristupa zanosvana na identitetu podnosioca zahteva I pravila pristupa, podnosiocu zahteva govori šta mu je dozvoljeno da radi a šta ne
- Mandatorni model (MAC – Mandatory Access Control): Zanovan na upoređivanju bezbednosnih oznaka (ukazuje na osetljive I kritične resurse sistema) sa bezbednosnim dozvolama pristupa (koji sistemi imaju parvo pristupa određenim resursima). Sva prava pristupa su unapred definisana.
- Model grupa I uloga (RBAC – Role based access control): Zasnovan na ulogama korisnika u sistemu I na pravima koje navode čemu korisnik ima pristup. Fleksibilniji od MAC, ali manje fleksibilniji u odnosu na DAC modele.

Q: Za šta se koristi Diffle-Hellman algoritam, objasniti?
A: Cilj algoritma je da omogući korisnicima da sigurno razmenjuju tajni ključ koji zatim mogu da koriste za šifrovanje nakadnih poruka. Algoritam se koristi za zaštićeni prenos ključeva. Efikasnost algoritma zavisi od težine računanja diskretnog logaritma. Ukoliko korisnik A želi da uspotavi vezu sa korisnikom B i koristi tajni ključ za šifrovanje poruke za vezu. Korisnik A može generisati jednokratni privatni ključ XA, izračunati YA i poslati to korisniku B. Korisnik B odgovara generisanjem privatne vrednosti XB, izračunavanjem YB i slanjem YB korisniku A. Oba korisnika sada mogu izračunati ključ.

Q: Objasniti tehnologiju digitalnog koverte (envelope)
A: Koristi se kako bi zaštitili poruke bez potrebe da pošiljalac i primalac imaju isti tajni ključ. Koristi se šifrovanje javnim ključem za zaštitu simetričnog ključa. Osoba A: 1) Priprema poruku 2) Šifruje poruku sa jednokratnim ključem sesije 3) Šifruje ključ sesije pomoću javnog ključa, koji ima i osoba B 4) Prilaže šifrovan ključ sesije poruci i šalje poruku osobi B

Q: Objasniti razliku izmedju IPS i IDS sistema
A: Sistem za detekciju upada (enlg. Intrusion Detection Systems - IDS) i sistem za prevenciju upada (engl. Intrusion Prevention Systems - IPS). Razlika između ova dva sistema je to što se IDS sistemi koriste za detekciju napda i obaveštenje administratora o istom a IPS sistemi za njihovo sprečavanje.

Q: Koje se tehnologije koriste u V irtualnim privatnim mrežama (navesti dva protokola)?
A: Predstavljaju šifrovane tunele koji omogućavaju zaštićeno povezivanje dve fizički odvojene mreže preko interneta. Virtualne privatne mreže su uglavnom jeftinije nego prave privatne mreže, ali se kao i one, oslanjaju na isti sistem šifrovanja i provere identiteta na oba kraja. Internet Protocol Security or IPSec – Layer 2 Tunneling Protocol (L2TP) – Point to Point Tunneling Protocol (PPTP) – Secure Sockets Layer (SSL) and Transport Layer Security (TLS)

Q: Objasniti tehnologiju digitalnog potpisa.
A: Digitalni potpis predstavlja kup podataka u elektronskom obliku koji su pridruženi elektronskim porukama ili dokuemntima i služe za identifikaciju potpisnika. Svrha digitalnog potpisa je da potvdri sadržaj poruke i identitet pošiljaoca poruke.

Q: Šta je digitalna koverta a šta digitalni potpis email dokumenta?

A: Digitalna koverta se koristi kako bi zaštitili poruke bez potrebe da pošiljalac i primalac imaju isti tajni ključ. Koristi se šifrovanje javnim ključem za zaštitu simetričnog ključa. Radi na sledeći način: Osoba A priprema poruku i šifruje je sa jednokratnim ključem sesije. Dalje ključ sesije šifruje pomoću javnog ključa (koji ima i osoba B), prilaže šifrovan ključ sesije poruci i šalje poruku osobi B. Digitalni potpis predstavlja skup elektonskih podataka koji su pridruženi elektronskim porukama i služe za verifikaciju vlasnika poruke, tj. Njegovor identiteta kao i proveru autentičnosti samog sadržaja poruke. Primer detekcije anomalija: - DOS, podrazumeva ogromno povećanje paketa saobraćaja ili pokušaj da se prenatrpa neki sistem – Skeniranje, u trenutku kada napadač pretražuje željenu mrežnu ili neki sistem, šaljući različite pakete u cilju da otkrije krakteristike sistem – Crvi, kada se radi o velikoj propusnosti sistema

Q: Objasniti IPsec protokol
A: Predstavlja skup proširenja IPv4 protokola koji obezbeđuju osnovne sigurnosne aspekte mrežne komunikacije. Glavno svojstvo IPSec protokola je omogućavanje podrške raličitim aplikacijama, mogućnost šifrovanja i provera identiteta celokupnog saobraćaja na IP sloju.

Q: Šta je kerberos protokol i za šta se koristi?
A: Kerberos predstavlja standard za daljinsku proveru identiteta. On predstavlja pouzdanu treću stranu usluge provere identiteta. Zahteva da korisnik dokaže identitet prilikom bilo kog pozivanja, takođe može i od servera zahtevati da svoj identitet dokaže klijentima.

Q: Navesti i objasniti tehnike detekcije upada
A: Detekcija upada zasnovana na mreži koristi detekciju potpisa i detekciju anomalija. Primer detekcije potipsa: - Aplikacioni sloj, uloga slija je da analizira desetak aplikacionih protokola u potrazi za identifikovanjem modela npada – Transportni sloj, analizira TCP i UDP protokole za paketne fragmente, skeniranje portova i sl. – Mrežni sloj, uglavnom analiza IPv4 i ICMP za IP adresom, ilegalnim vrednostima IP zaglavlja i sl. – Kršenje pravila, poput upotrebe neadekvatnih web stranica, korišćenje zabranjenih protokola i sl.

Q: Objasniti proces ojačanja Linux sistema?
A: Administrator sistema može za veoma kratko vreme sprečiti razne vrste napada na sistem primenjujući neke od postupka: - Postavljanje lozinke za pristup BIOS konfiguraciji i zabrana podizanja operativnog sistema sa diskete ili cd roma. – Korišćenje programa za podaizanje operativnog sistema (LILO i GRUB) – Privremeno isključivanje servera sa mreže

Q: Objasniti šta je kompromitovani računar
A: Pojam kompromitovanog računara najčešće se odnosi na napadnuti računar (žrtvu) može obuhvatiti i osumnjičeni izvnorni ili posredni računar. U praksi istrage digitalnih dokaza često neophodno izvšiti forenzičku analizu računara sa koje je izvršen napad, napadnutog računara i nekog od posrednih računara, na primer preko čijeg naloga je napadač ušao u sistem. Pod kompromitovanim računarom danas se podrazumevaju i mobilni telefoni i IOT uređaju (kamere, automobili, medicinski uređaji)

Q: Koje su dve vrste IDS sistema i koje su razlike izmedju njih?
A: IDS zasnovan na hostu (HIDS) – nadgleda aktivnosti hosta i događaje unutar tog hosta, prilikom otkrivanja sumnjivih aktivnosti. IDS zasnovan na mreži (NIDS) – prati mrežni saobraćaj za pojedine segmente mreže ili uređaje i analizira mreže, transport i protokole aplikacija, kako bi identifikovao sumnjive aktivnosti.

Q: Šta je Encapsulating Security Payload – ESP?
A: Encapsulating Security Paypload obezbeđuje usluge poverljivosti sadržaja poruke i ograničeni protok saobraćaja poverljivosti. Pored toga obezbeđuje i sigurnosne usluge provere identiteta, integriteta, neporecivosti i privatnosi podataka.

Q: Objasniti kako funkcioniše SSl bezbednost transportnog sloja?
A: Transport Layer Securty – TLS format zapisa je jednak formatu SSL zapisa. Razlika je u vrednosti polja za verziju. Kod TLS verzije, plje Major Version je 3 a minor Version je 1. TLS koristi HMAC algoritam za autentfikaciju koda (opisa RFC2104) i peudoslučajnu funkciju PRF (pseudo random function) kako bi generisali duži blokovi podataka na osnovu relativno malih poverljivih podataka.

Q: Šta predstavlja Utvrđeni Bastion Host?
A: Zaštitni zid administratora vidi ovaj sistem kao jaku kritičnu tačku u mrežnoj bezbednosti. Služi kao platforma za mrežni prijelaz na aplikacionom sloju ili na nivou kanala komunikacijski podataka. Zajedničke karakteristike:

- Izvršava sigurnu verziju operativnog sistema
- Samo su neophodne usluge instalirane na utvrđenom hostu
- Mogu zahtevati proveru identiteta korisnika pre dozvole pristupa proxy uslugama i proveru identiteta pre dodele pristupa korisnika
- Podržava samo podskup aplikacijskog skupa naredbi
- Omogućava pristup samo na određene host sisteme
- Održava detaljne audit informacije prijavom celokupnog saboraćaja
- Nezavisan od drugih proxy na utvrđenom hostu
- Izvršava se bez pristupa disku

Q: Koje se tehnologije koriste u virtulnim privatnim mrežama?
A: Za odbijanje ovog napada potreban je VPN. VPN koristi šifrovanje i proveru identiteta u donjim slojevima protokola da obezbedi bezbednu vezu kroz inače nesigurnu mrežu, najčešće Internet. Virtuelne privatne mreže su obično jeftinije nego stvarne privatne mreže korišćenjem privatne linije, ali se oslanjaju na isti sistem šifrovanja i provere identiteta na oba kraja. Šifrovanje se može izvršavati pomoću softvera zaštitnog zida ili eventualno pomoću rutera. Najčešći mehanizam protokola koji se koristi za ovu namenu na nivou IP-a je poznat kao IPSec.

Q: Šta je kriptosistem i od čega se sastoji?
A: Kriptografski sistem je sistem koji se koristi za prenosa podataka uz pomoć šifrovanja i dešifrovanja, koji su od značaja za realizaciju bezbednosnog sistema. Obezbeđuje sledeće usluge: - Proveru identiteta – Obezbeđenje integriteta ili celovitosti informacija – Obezbeđenje poverljivosti – Onemogućavanje poricanja porekla podataka

Q: Objasniti kako funkcioniše dinamičko ispitivanje paketa?
A: Stateful inspection firewall proverava informacije paketa, kao i zapise o TCP vezama. Kada program koji koristi TCP kreira sesiju sa udaljenim hostom, on kreira i TCP vezu u kojoj je broj TCP porta za server aplikaciju manji od 1024, što predstavlja poznate port brojeve. Ostali brojevi (brojevi i veći od 1024) imaju privremeni značaj, tj. Značanji su samo u toku trajanja TCp veze. Zaštivni zid za filtriranje paketa dopušta ulazni mrežni saobraćaj na svim portovima za TCP zaobraćaj. Ovo predstavlja ranjivost koja se može iskoristiti od strane neovlašćenih korisnika. Kako bi se problem rešio, firewall kreira imenike izlaznih TCP veza.

Q: Sigurnosni propusti u IEEE 802.11 standardu?
A: WEP protokol se koristu u WLANu baziranom na 802.11. WEP koristi RC4 kriptografski algoritam sa promenljivom dužinom ključa za zaštistu saobraćaja. Bezbednosni problemi kojima se može kompromitovati bezbednost WLAN-a:

- Pasivni napadi na dešifrovani saobraćaj zasnovan na statističkoj analizi
- Aktivni napadi za uvođenje novog saboraćaja

- Aktivni napadi za dešifrovani saobraćaj
- Napadi izgradnje rečnika

Q: Šta je SELinux?
A: SELinux je NSA implementacija obavezne kontrole pristupa za linux. Procenjuje akcije pokušaja subjekata prema objektu. U SELinux-u subjekti su uvek procesi, pošto izvršavaju komande korisnika a kacije se zovu dozvole.

Q: Ojačanje Windows sistema?
A: Ojačanje sistema se odgleda u procesu poboljšanja odbrane, smanjivanjem funkcionalnosti nepoverljivim korisnicima i onemogućavajući manje korišćenja svojstva. Primenjuje se pravilo 80/20 na svojstva. Ako svojstvo ne koristi 80% populacije onda se to svojstvo onemogućava.

Q: Koje su osnovni rizici u elektronskim sistemima plaćanja?
A: Rizici mogu biti ekonmske posledice otkaza ili zloupotrebe Internet tehnologija, posledica prevara, gubljenje vrednih i poverljivih informacija, gubljenje poslova zbog nedostupnosti servisa, neovlašćena upotreba resura, gubljenje poslovnog ugleda i poverenja klijenata, nepotrebni troškovi i sl.

Q: Šta je digitalni dokaz?
A: Digitalni dokaz je informacija uskladištena ili prenošena u digitalnoj formi koja se koristi u sudskom posupuki i može se koristiti na suđenju.

Q: Šta se podrazumeva pod pojmom tradicionalno sakupljanje dokaza?
A: Tradicionalno, forenzičke istrage se sprovode na ostatku podataka, poput hard diska. Prekidom napajanja računara, hard disk ostaje u stanju kom je bio pre samog isključenja. Međutim takvo isključenje može narušiti sadržaj diska, čak dovesti i do gubitka vrednih podataka, jer se isključenjem podaci iz keš memorije neće upisati na disk. Pravilno isključenje računara sprečava narušavanje sadržaja diska, ali opet može doći do gubitka podataka. Isključenjem se može izgubiti zlonamerni kod ili će instaliran program uništiti bilo kakve dokaze o upiadu

Q: Kakva je razlika izmedju tradicionalnog i LIVE sakupljanje dokaza?
A: Pojedini istražitelji odmah isključuju računar, dok drugi počinju sa istragom na uključenom računaru. Tradicionalno, forenzičke istrage se sprovode na ostatku podataka, poput hard diska. Prekidom napajanja računara, hard disk ostaje u stanju u kom je bio pre samog isključenja. Međutim, takvo isključenje može narušiti sadržaj diska, čak dovesti i do gubitka vrednih podataka, jer se isključenjem podaci iz keš memorije neće upisati na disk. Pravilno isključenje računara sprečava narušavanje sadržaja diska, ali opet može doći do gubitka podataka. Isključenjem se može izguviti zlonamerni kod ili će instaliran program uništiti bilo kakve dokaze o napadu. Stoga, sve je veći naglasak na obavljanju analizu na live sistemu. Prvobitno jer mnogi napadi ne ostavljaju trag na hard disku računara, već se informacije nalaze samo u memoriji računara. Drugo, ukoliko se radi o upotrebi kriptografskog skladištenja, postoji mogućnost da je jedini primerak ključa dešifrovanja sačuvan upravo u momoriji računara i isključivanje računara će se izgubiti. Da bi se smanjila mogućnost izmene tekućeg stanja memorije na ispitivanom računaru, poželjno je koristi samo jednu naredbu, koja će kao proces zauzeti što manje memorije u računaru ili alternativno koristiti neki poseban hardverski uređaj.

Q: Navedite nekoliko najčešće primenljivih forenzičkih alata za koje ste čuli:
A: EnCase Guidence Software, Frensic Toolkit, Helix CD, ProDiscover, SMART, The Sleuth KIT / Autopsy, The Coroner’s Toolkit (TCT), Logminer, Brian Carrier’s Sleuth Kit

Practice

Q: Objasniti ulogu Forward, Input, Output chain-a?
A: OUTPUT je za pakete koje emituje host. Njihova destinacija je obi;no drugi host, ali mo\e biti isti host preko loopback interfejsa, tako da svi paketi koji prolaze kroz OUTPUT zapravo nisu u stanju mirovanja. FORWARD je za pakete koji ne emituje ni host niti upu'eni doma'inu. Oni su paketi koje domaćin samo usmerava. INPUT lanac se koristi za kontrolu ponašanja dolaznih veza. Na primer ako korisnik pokuša ssh nad nekim računarom/serverom iptables će pokušati da mapiraju IP adresu I port sa pravilom u ulaznom lancu.

Q: Koja je uloga NAT tabele?
A: Tokom prolaska paketa kroz mrežnu barijeru, NAT skriva IP adrese računara iz private mreže I prevodi ih u adresu mrežne barijere. Nakon toga mrežna barijera, ponovo šalje podatke tog paketa sa svoje adrese, koristeći tabelu prevođenja adresa. NAT tabela mogućava uštedu javnih IP adresa, jer se jedna javna IP adresa, korišćenjem dosta različitih portova, može prevesti u više privatnih IP adresa.

Q: Objasniti ulogu Prerouting I Postrouting chain-a?
A: PREROUTING lanac se koristi za odluke vezane za rutiranje pre slanja bilo kog paketa. POSTROUTING lanac se koristi za donošenje odluka rutiranja nakon slanja nekog paketa.

Q: Koja je uloga MANGLE tabele?
A: Pošto se NAT odnosi na prevođenje adresa ili mangaling, koriste se 2 tabele u okviru iptables za MANGLE I NAT. Paketi iptables-a prvo ulaze u lance MANGLE tabele pa zatim u lance NAT tabele.

Q: Korišćenjem iptables blokirati odlazni saobraćaj prema adresi 192.168.1.11
A: iptables -A OUTPUT -s 192.168.1.1 -p udp -j REJECT

Q: Korišćenjem iptables blokirati dolazni saobraćaj sa adrese 10.0.0.15
A: iptables -A INPUT -s 10.0.0.15 -j REJECT

Q: Korišćenjem iptables blokirati odlazni I dolazni saobraćaj prema/sa mreže 192.168.254.0/24
A: iptables -A output -s 192.168.254.0/24 -j REJECT
Iptables -A INPUT -s 192.168.254.0/24 -j REJECT

Q: Korišćenjem iptables blokirati odlazni forward saobraćaj na interfejsu uth0.
A: iptables -A FORWARD -o eth0 -j DROP

Q: Korišćenjem iptables blokirati odlazni saobraćaj prema mreži 192.168.55.0/30
A: iptables OUTPUT -s 192.168.55.0/30 -j DROP

Q: Korišćenjem iptables blokirati dolazni saobraćaj od mreže 192.168.5.0/26
A: iptables -A INPUT -s 192.168.5.0/26 -p udp -j REJECT

Q: Korišćenjem iptables blokirati sve dolazne tcp I udp pakete na portu 8080 I 3306
A: iptables -A INPUT -p tcp -p udp -m multiport –dports 8080,3306 -j DROP

Q: Korišćenjem iptables dozvoliti dolazne tcp I udp pakete na portu 81 I 3306 I blokirati ostale portove:
A: iptables -A INPUT -p tco -p udp -m multiport ! –doprts 81,3306 -j DROP

Q: KOrišćenjem iptables blokirati sve dolazne konekcije I jedino dozvoliti konekcije na portu 465, 587 I 995
A: iptables -A INPUT -m multiport ! –dports 465,587 I 995 -j DROP

Q: Korišćenjem iptables blokirati sve dolazne konekcije I jedino dozvoliti konekcije na portu 25 I 995.
A: iptables -A INPUT -p tcp -m multiport ! –dports 25, 995 -j DROP

Q: Obrisati pravilo koje zabranjuje dolazni saobraćaj sa adrese 11.11.15.15
A: iptables -D INPUT -s 11.11.15.15 -j DROP

Q: Napisati iptables pravila koja dozvoljavaju jedino odlazni SMTP saobraćaj na svim STMP podrazumevanim portovima, dok je sav ostali saobraćaj blokiran
A:
iptables -A OUTPUT -p tcp -m multiport –dports 25,587,465 -j ACCEPT
block everything else
Iptables -A INPUT -j DROP
Iptables -A OUTPUT -p tcp -m multiport ! – dports 25,587,465 -j DROP

Q: napisati iptables pravila koja dozvoljavaju jedino odlazni POP3 I SMTP saobraćaj, dok je sav ostali saobraćaj blokiran
A:
iptables -I OUTPUT –dport 110 -j ACCEPT
iptables -I OUTPUT –dport 25 -j ACCEPT
iptables -I OUTPUT -j DROP

Q: Korišćenjem iptables blokirati sve dolazne konekcije I jedino dozvoliti konekcije na portu 25 I 587.
A: iptables -A INPUT -p tcp -m multiport ! –dports 25,587 -j DROP

Q: Obrisati pravilo koje zabranjuje dolazni saobraćaj sa adrese 10.10.1.10
A: iptables -D INPUT -s 10.10.1.10 -j DROP

Q: Naisati iptables pravila koja dozvoljavaju jedino odlazni SNMP saobraćaj dok je sav ostali saobraćaj blokiran
A:
iptables -I INPUT -p udp -m udp –dport 161 -j ACCEPT
iptables -I INPUT -p udp -m udp –dport 162 -j ACCEPT

Q: Napisati komandu kojom se brišu sedmo pravilo u inpu ttabeli
A: iptables -D input 7

Q: Korišćenjem iptables dozvoliti odlazne tcp I udp pakete na portu 81 I 8081 I blokirati ostale portove
A:
iptables -I OUTPUT -p tcp –dport 81 -j ACCEPT
iptables -I OUTPUT -p tcp –dport 8081 -j ACCEPT
block everything else
Iptables -A INPUT -j DROP
Iptables -A OUTPUT -p tcp -m multiport ! –dports 81,8081 -j DROP
Iptables -A OUTPUT -p udp -m multiport ! –dports 81,8081 -j DROP

Q: Napisati komandu kojom se briše treće pravilo u input tabli
A: iptables -D input 3

Q: Napisati iptables pravila koja zabranjuje ping na INPUT-u I OUTPUT-u
A: iptables -A INPUT -p icmp -I eth0 -j DROP
Iptables -A OUTPUT -p icmp -o eth0 -j DROP

==========

Q: Objasniti: iptables -A INPUT -S 192.168.71.0/255.255.255.0 -I eth0 -p udp -m udp –dport 135:139 -j DROP
A: Pravilo obuhvata udp pakete sa adresa u datom opsegu, koji se nalaze na interfejsu eth0 I koji koriste samo dati opseg porta. Presta se sa saobraćajem u datom lancu.

Q: Objasniti:
iptables -A INPUT -I eth0 -p tcp –dport 22 -m state –state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp –sport -m state –state ESTABLISHED -j ACCEPT
A: Prvo pravilo prihvata dolazne tcp pakete sa porta desinacije 22 interfejsa eth0 I stanjem ESTABLISHED. Drugo pravilo prihvata odlazne tcp pakete sa izvornog porta 22, interfejsa eth0 I stanjem ESTABLISHED.

Q: iptables -A OUTPUT -o eth0 -p tcp –sport 80 -m stage –state ESTABLISHED -j ACCEPT
A: Prihvata odlazne tcp pakete na eth0 interfejsu I portu 80 sa stanjem ESTABLISHED

Q: Objasniti: iptables -A INPUT -s 161.53.2.70 -p udp -m udp –dport 321 -j ACCEPT
A: Pravilo prihvata udp pakete sa ip adrese 161.53.2.70 koji koriste port 321.

Q: Objasniti: iptables -A INPUT -s !161.53.2.70 -p udp -m udp –dport 321 -j ACCEPT
A: Pravilo prihvata sve dolazne pakete koji nisus a adrese 161.53.71.235 i koji koriste port 321

Q: Objasniti: iptables -A INPUT -s !161.53.71.235 -I eth0 -p tcp -m tcp –dport 25,465 -j DROP
A: Pravilo odbacuje sve dolazne tcp pakete sa eth0 interfejsa na portovima 25 I 465, koji nisus a adrese 161.53.71.235

Q: Objasniti: iptables -A INPUT -i ppp0 -m state –state NEW,INVALID -j DROP
A: Pravilo odbacuje dolazni saobraćaj sa interfejsom ppp0 I stanjima NEW, INVALID.

Q: Objasniti: iptables -A FORWARD -i ppp0 -m stage –stage NEW, INVALID -j DROP
A: Pravilo dobacuje dolazni FORWARD saobraćaj sa interfejsom ppp0 I stanjima NEW, INVALID

Q: Objasniti: iptables -A FORWARD -I eth0 -o eth1 -j ACCEPT
A: Pravilo prihvata dolazni FORWARD saobraćaj na eth0 interfejsu I odlazni na eth1 interfejsu.

Q: Objasniti: iptables -A INVALID -I wan_eth -ptcp –tcp-flags ALL FIN,URG -j DROP
A: Pravilo ignoriše nevalidne/ilegalne tcp zastavice ALL, FIN I URG na wan_etch interfejsu.

Q: Objasniti: iptables -A INPUT -I eth0 -p tcp –sport 22 -m state –state ESTABLISHED -j ACCEPT
A: Prihvata dolazne tcp pakete na eth0 interfejsu I izvnornog porta 22 sa stanjem ESTABLISHED

Q: Objasniti:
iptables -A PREROUTING -I eth0 -p tcp –dport 443 -m state –state NEW -m nth –counter 0 –every 3 –packet 0 -j DNAT –to-destination 192.168.1.101:443

iptables -A PREROUTING -I eth0 -p tcp –dport 443 -m state –state NEW -m nth –counter 0 –every 3 –packet 1 -j DNAT –to-destination 192.168.1.102:443
A: Upućivanje svakog trećeg tcp paketa sa interfejsa eth0 na portu 443 I stanjem NEW na adresu 192.168.1.103:443. Brojač na početku je jednak 0. Upućivanje svakog trećeg tcp paketa sa interfejsa eth0 na portu 443 I stanjem NEW koji dolaze sa adrese 192.168.1.103:443. Brojać je na početku jednak 0.

Q: Kojim ključem se vrši digitalnog šifrovanjei potpisivanje poruke digitalnog potpisa. Opisati postupak?
A: Termin digitalni potpis (digital signature) podrazumeva korišćenje asimetričnog šifrovanja, gde korisnik objavljuje javni priptografski ključ I potpisuje poruke privatnim ključem, po kojem će primenom javljnog ključa, biti potvrđeno da je poruka potpisana konkretno tim privatnim ključem.

Q: Napisati komandu kojom se grupi it381 na linux sistemu dodeljuje parvo čitanja nad fajlom ovdeprocitati bez promene trenutnog vlasnika I grupe.
A: chgrp it381 ovdeprocitati

Q: Napisati komandu kojom se korisniku it381 na linux sistemu oduzima pravko čitanja nad fajlom ovdeprocitati bez ppromene tretnunog vlasnika I grupe:
A: setfacl -m user:it381:-wx ovdeprocitati

Q: Napisati snort pravilo za detekciju PING aktivnosti
A: Alert icmp any any -> any any (msg:“Detekcija pinga“; sid:1000000001;)

Q: Napisati snort pravilo za detekciju dolaznog TCP saobraćaja na portu 25 I 465, koje daje poruku da je došlo do detekcije saobraćaja na datim portovima?
A: alert tcp any any -> any 25 (msg: „Došlo je do detekcije saobraćaja na portu 25“; sid:1000000001;)
alert tcp any any -> any 456 (msg:“Došlo je do detekcije saobraćaja na portu 465“; sid:1000000001;)

Q: Na linux sistemu šta se nalazi u /etc-passwd a šta u /etc/shadow datoteci?
A: Nalozi se kreiraju i njima se upravljaju preko datoteke /etc/passwd. U datoteci /etc/shadow se nalazi stvarna lizinka u šifrovanom formatu za svaki nalog sa dodatnim informacijama o lozinci.

Q: Kojom komandom se brišu sva ACL pravila?
A: setfacl -D e *

Q: Koristeći ACL ukoloniti privilegije za korisnika test na fajlu IT381
A: setfacl -m user:test:--- it381

==========

Q: Napisati sledeća ACL pravila koristeći Cisco Packet Tracer: Dozvoliti samo portove 80,443,8080 prema računaru sa adresom 192.168.2.5 gde su polazne adrese 192.168.3.0/24
A: iptables -t nat -A PREROUTING -s 192.168.3.0/24 -p tcp -m multiport –dports 80,443,8080 -j SNAT –to-source 192.168.2.5

Q: Napisati sledeća ACL pravila koristeći Cisco Packet Tracer: Napisati pravilo da se iz mreže 192.168.3.0/24 može izvršiti ping komanda prema ostalim mrežama, dok je ping saobraćaj prema toj mreži blokiran.
A: iptables -A OUTPUT -s 192.168.3.0/24 -p icmp –icmp-type echo-request -j ACCEPT
Iptables -A INPUT -s 192.168.3.0/24 -p icmp –icmp-type echo-request -j DROP

Q: Napisati sledeća ACL pravila koristeći Cisco Packet Tracer: Dozvola ping-a samo za adresu 192.168.2.5 prema adresi
A: iptables -t nat -A INPUT -s 192.168.2.5 -p icmp –icmp-type echo-request -j SNAT –to-destination 192.168.1.5
Iptables -A INPUT -s 192.168.1.5 -p icmp –icmp-type echo-request -j DROP

Q: Napisati sledeća ACL pravila koristeći Cisco Packet Tracer: Napisati pravila koja dozvoljavaju pristup server na adresi 192.168.3.2. sa adrese 192.168.1.5 I mreže 192.168.2.0/24 na portovima od 1000 do 1030.
A: iptables -t -nat -A PREROUTING -s 192.168.2.0/24 -p tcp -m tcp –dport 1000:1030 -j DNAT –to-destination 192.168.3.2

Q: Napisati sledeća ACL pravila koristeći Cisco Packet Tracer: Napisati pravilo kojim se dozvoljava ping (ICMP) saobraćaj prema server na adresi 192.168.2.2 I to samo sa adrese 192.168.3.2
A: iptables -A INPUT -s 192.168.2.2 -p icmp -icmp-type echo-request -s 192.168.3.2 -j ACCEPT
Iptables -t nat -A INPUT -s 192.168.3.2 -p icmp –icmp-type echo-request -j SNAT –to-destination 192.168.2.2