1. Zaokruzi istinite tvrdnje o elektronskom perimiteru (EP):

a) Kolektori podataka SIEMalata se ne postavljaju na EP

b) Kolektori podatka SIEM alata se postavljaju na sve mobilne elemente EP

**c) Uradjaji za detekciju I prevenciju upada(IDS/IPS) se mogu postaviti na EP**

**d) Uredjaji tipa network tap(tj, duplikatori tokova podataka mogu biti postavljeni na EP)**

**e) Firewall moze biti postavljen na EP**

f) Kolektori podataka SIEM alata se postavljaju samo na EP-*siem se postavlja svuda ne samo na ep*

2. Zaokruziti istinite iskaze o indikatorima kompromisa(Indicator of Compromise - IOC)

~~a)IOC se primenjuje samo u kontekstu antimalver resenja~~

**b) TCP/UDP port moze biti deo IOC**

**c) Fajl hes moze biti deo IOC**

**d) IP adresa moze biti deo IOC**

**e) Faze zivotnog veka IOC su : nezreo(immature), zero(mature) I retired(penzionisan)**

3. Zaokruziti usluge koje pruzaju SIEM alati

~~a) Pracenje radnika u transformatorskoj stanici preko RFID tagova~~

~~b) Aktivna zastita od zlonamernog softvera~~

**c) Dashboard, tj vizuelizacija agregiranih podataka**

**d) Prikupljanje skladistenje podataka iz nadzora distribuiranih informacionih sistema**

**e) Upotreba sadrzanih podataka kao dokazni material u slucajevima krivicnih dela**

**f) Staticka obrada podataka**

**g) Agregacija I korelacija podataka**

4. U kontekstu autentifikacije elektronskih identiteta

~~a) je nemoguca visefaktorska autentifikacija na Internetu~~ *\*?*

~~b) bankomat je dobar primer visefakotorske autentifikacije preko necega sto primamo~~

~~c) uvek se primenjuje biometrijski hardver~~ *–\* identifikacuju fizickih lica ali ne ovo*

**d) upotreba lozinke I mobilnog telefona omogucava visefaktorsku autentifikaciju**

~~e) upotreba lozinke uvek obezbedjuje dovoljan nivo bezbednosti~~

5. Zaokruzi tacno dve funkcionalnosti koje ne pruzaju moderna anti malware resenja:

a) Povezivanje sa jezgrom operativnog sistema

b) Staticka analiza mreznog saobracaja

c) Premestanje sumnjivih datoteka u karantin

d) Ciscenje zarazenog racunara zlonamernog softvera

e) Distribuirana detekcija botneta

f) Skeniranje email priloga

6. Zaokruzi istinite iskaze o botnetima:

a) Nema upravljanja,botovi su potpuno autonomni

b) Clanovi mreze zarazenih racunara se zovu botovi ili zombiji

c) Botovi mogu da koriste HTTPS ili DNS za komunikaciju sa drugim elementimabotneta

d) Upravljanje botnetom moze biti centralizovano ili distribuirano

e) Upravljanje se iskljucivo implementira preko epidemic protokola

7. Zaokruzi tacne iskaze o statickoj analizi izvornog koda:

**a) Kljucni ulaz je izvorni kod softvera**

**b) Poznata I pod imenom white box testing**

**c) Neki od poznatih alata za staticku analizu su u vlasnistvu kompanije IBM I Microsotf**

**d) Deo staticke analize je manuelna analiza izvornog koda**

**e) Postoje alati koji mogu automatizovati process analize**.

8. Obfuskacija izvornog koda

**a) se implemetira preko promene redosleda instrukcija I transpozicije koda**

~~b) podrazumeva cuvanje korisnickih imena u konfiguracionim XML datotekama~~

c~~) se implementira preko ACL-ova~~

**d) omogucava sakrivanje izvornog koda koji je potrebno objaviti na vebu npr.JAVASCRIPT**

**e) je relevantna u kontekstu binarnih fajlova pisanih u programskim jezicima Java I C#**

f**) se implementira preko tehnika tipa dodavanje redudantnog koda, odnosno promena imena promenljivih I klasa**

~~g) nije relevantna u kontekstu binarnih fajlova ciji je kod bio pisan u programskim jezicima Java I C#~~

9. Navesti bar dva tipa firewall-a

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

10. Navesti definiciju I tipove perimetra:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

11. Navesti tri tipa potencijalnih zloupotreba mobilnih elemenata informacionog Sistema:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

12. Zaokruziti istinite tvrdnje TCP/IP protocol steku I bezbednosti podataka:

~~a) Kodiranje I dekodiranje podataka sa AES/RSA algoritmima se vrsi fizickom sloju~~

~~b) Kodiranje podataka se vrsi u transportnom sloju~~

~~c) Dekodiranje podataka se vrsi u aplikativnom , kodiranje u mreznom sloju~~

**d) Provera digitalnih potpisa se vrsi u aplikativnom sloju**

**e) Kodiranje I dekodiranje podataka je moguce u mreznom sloju**

13. Zaokruziti funkcionalnosti koje vecina modernih IDS/IPS uredjaja podrzava:

~~a) Pracenje aktivnosti Sistema I korisnika u fizickom prostoru – \*~~*u elektronskom je*

b~~) Provera konfiguracije racunara I prijava oznatih slabosti preko fiksne telefonije~~

**c) Prepoznavanje poznatih tipova napada u racunarskim mrezama –\*na osnovu potpisa radi**

**d) Detekcija anomalija u mreznim tokovima podataka statistickom analizom**

~~e) Instalacija I odrzavanje zamki za napadace (tzv. honeypot)~~

14. Zaokruzi osnovne funkcije aplikativnih proksija:

a) ~~Pracenje aktivnosti Sistema I korisnika u fizickom prostoru~~

**b) Analiza zaglavlja (eng. header) I donosenje odluka o prosledjivanju ili odbacivanju paketa**

~~c) Analiza malvera~~

**d) Filtriranje komandi u aplikativnom sloju (npr. HTTPS PUT)**

~~e) Detekcija anomalija statistickom analizom~~

f~~) Rad sa audit logovima I detekcija anomalija primenom masinskog ucenja~~

~~g) Detekcija I predlozi korekcija gresaka u konfiguraciji Sistema~~

15. Zaokruzi istinite iskaze o IPsecu-u

**a) Implementira autentifikaciju u 3. OSI sloju (mrezni)**

~~b) Implementira autentifikaciju u 7.OSI sloju~~

**c) Omogucava kodiranje podataka u mreznom sloju TCP/IP protokolu steka**

~~d) Omogucava neporecivost poruka u mreznom sloju TCP/IP protokolu steka~~

~~e) Implementira se u aplikativnom 7. OSI sloju~~

~~f) Implementira kontrolu pristupa u 2. OSI sloju~~

16. Zaokruzi tacne iskaze o aspektima privatnosti

a) Subjekat je vlasnik osetljivih ili visoko osetljivih informacija

b) Auditing je aspekat privatnosti

c) Objekat privatnosti je osetljiv ili visoko osetljiva informacija

d) Kontrolisano otkrivanje je kljucni aspekat privatnosti

e) Autorizacija je aspekat privatnosti

17. Zaokruziti tacne iskaze o privatnosti u okviru elektroenergetskih Sistema (EES):

a) Softverski sistemi EES ne skaldiste nikakve licne podatke korisnika

b) Nacin rukovanja licnim podacima odredjuje srednji menadzment na nedeljnim stanicama

c) Neki podsistemi EES skladiste licne podatke korisnika

d)Rukovanje licnim podacima se uskladjuje sa svim relativnim zakonima npr Zakon o inf bezbed

18. Zaokruzi tvrdnje koje su istinite o patentima I autorskom pravu:

a) Patent traje beskonacno

b) Patent stiti naucno tehnoloske I inzinjerske rezultate

c) Patent stiti intelektualnu svojinu

d) Autorsko pravo stiti intelektualnu svojinu

e) Autorsko pravo traje beskonacno

19. Zaokruziti istinite iskaze o kontekstu klauzule o zabrani konkurencije

a) Trajno omogucavaju prelazak zaposlenog kod direktnih konkurenata

b) Ako se aktivira, onda bivsi poslodavac placa novcanu naknadu(ranije) ugovorene visine

c) Onemogucuje pravnim licima ulazak na pojedinacna trzista

d) Ako se aktivira, onda bivsi poslodavac placa novcanu naknadu u visini zakonske min plate u drzavi

e) Nema trajanje duze od 10 godina

f) Nema trajanje duze od 2 godine

20. Bezbednosna politika formira odgovore na sledeca pitanja:

a) Koji su prioriteti elemenata Sistema

b) Koji su sastavni elementi Sistema

c) Koje su ocekivane pretnje

d) Kako oporaviti system nakon incidenta

e) Koliko je limit ulaganja u bezbednosne mere

21. Zaokruziti imena institucija u Republici Srbiji cija je onsnovna delatnost vezana za inf bezbednost

a) Univerzitet u Beogradu

b) Zavod za izradu novcanika I kovanog novca

c) MUP-OV CERT

d) Nacionalni CERT

e) Tuzilastvo za visoko-tehnoloski criminal

f) Ministarstvo odbrane

21. Zaokruziti tacne iskaze u kontekstu pretnji I komunikacionih medijuma

~~a) Pretnje tipa presretanje, modifikacija I fabrika uopste nisu releventne u kontesktu Sistema koji koriste opticke kablove~~

**b) Pretnja tipa ispad su relevantne u konttekstu svih tipova prenosnih medijuma (parice, optika bezicno)**

**c) Pretnje tipa presretanje je tehnicki lakse u implementirati u bezicnim mrezama u odnosu na optiku**

**d) Pretnje tipa fabrikacija su moguce u Ethernet mrezama ukoliko postoji barem jedan kompromitovan host**

~~e) Pretnja tipa presretanje se trivijalno implementira u kontekstu optickih vlakana sa ili bez fizickog pristupa~~

22. Zaokruziti usluge koje pruzaju moderni operativni sistemi za medjusobnu zastitu adresnih prostora procesa:

~~a) Bazni registar razdvaja memoriju OS od memorije procesa~~

**b) Deljenje podataka I koda u tzv. Stranice(paging)**

~~c) Hardverska ograda izmedju podataka I instrukcija~~

~~d) Hardversko trgovanje memorijskih lokacija za citanje I pisanje odnosno izvrsavanje~~

**e) Deljenje memorije procesa u segmente**

23. Zaokruziti istinite iskaze o listama za kontrolu pristupa

~~a) Omogucava zastitu integriteta fajl Sistema u slucaju elementarnih nepogoda~~

~~b) Omogucava deljenje memorijskih blokova podataka u stranice~~

**c) Koristi se u kontekstu kontrole fizickog pristupa, npr. Fizicko lice na spisku gostiju ima pravo ulaska u zasticeni fizicki proctor**

~~d) Ne koristi se u kontekstu kontrole fizickog pristupa~~

~~e) Onemogucava staticku obradu podatka~~

**f) Lakse se odrzava od MAC modelaautorizacije u velikim sistemima**

~~g) Teze se odrzavaju od MAC modela autorizacije u velikim sistemima~~

24. Zaokruzi istinite iskaze o merama bezbednosti za cuvanje lozinki na lkalnom racunaru:

~~a) Koristi se Kerberos za lokalno skladistenje lozinki~~

~~b) Lozinke se kodiraju I dekodiraju sa AES algoritmom~~

~~c) Lozinke se kodiraju I dekodiraju sa RSA algoritmom~~

**d) Lozinke se mogu cuvati lokalno, ali kodirane jednosmernim funkcijama sa primenom tzv SALT VREDNOSTI**

25. Zaokruziti istinite iskaze o merama bezbednosti za zastitu fajl Sistema:

**a) OS omogucava zastitu integriteta fajl Sistema preko ACL-ova I atuomatskog bekapa**

~~b) EFS je system kodiranja delova ili celog fajl Sistema na LinuxOS~~

**c) EFS je system kodiranja delova ili celog fajl Sistema na Windows OS**

~~d) OS omogucava pristup sistemskim fajlovima svim korisnicima~~

**e) OS onemogucava pristup sistemskim fajlovima korisnicima bez administrativnih prava**

26. Zaokruziti istinite iskaze o baseline konfiguraciji u kontekstu upravljanja konfiguracijama:

~~a) Kreira se u dizajn fazi \*~~*system koji je operativan treba*

**b) Kreira se odmah nakon implementacije I pustanja Sistema “u pogon”**

**c) Sadrzi verzije binarnih I konfiguracionih fajlova, odnosno dokumentacije I ostalih artefakata Sistema**

**d) Korisna je u kontekstu nalazenja odstupanja od osnovne konfiguracije Sistema**

~~e) Kreira se racno mesec dana nakon pustanja Sistema “u pogon”~~

27. Zaokruzi tacne iskaze o dinamickoj analizi u kontekstu razvoja bezbednog softvera:

~~a) Poznata I pod imenom white box testing~~

~~b) Kljucni ulaz je izvor koda softvera~~

**c) Kljucni ulaz je proces u izvrsavanju u ulazni podaci za potrebe testa**

~~d) Deo deterministicke analize je manuelna analiza izvornog koda~~

**e) Neki od poznatih alata za dinamicku analizu su u vlasnistvu kompanije IBM I Microsoft**

28. Zaokruzi tacne iskaze o interaktivnoj analizi aplikativnih procesa:

**a) Podrazumeva ubacivanje tzv. Sondi za pracenje procesa koji se testira**

~~b) Kljucni ulaz je izvorni kod softvera~~

**c) Kljucni ulazi su binarni fajlovi potrebni za pokretanje procesa I ulaz procesa za potrebe testa**

~~d) Ne postoje alati koji mogu automatizovati process analize~~

~~e) Deo interaktivne analize je manuelna analizaizvornog koda~~

30. Zaokruzi dva tacna odgovora o tipu namerne greske koji je doveo do bezbednosnog propusta Heartbleed u OpenSSL Biblioteci:

**a) Neadekvatna validacija ulaza**

~~b) Buffer overflow~~ \*overread je

**c) Otkrivanje kriticnih informacija**

~~d) SQL injection~~

~~e) Buffer superadmin~~

31. Zaokruzi tacne iskaze o otkrivanju kriticnih informacija u kontekstu razvojabezbednosnog softvera:

~~a) Definise se kao podtip neadekvatne validacije ulaza~~

~~b)Buffer overflow spade u ovu grupu~~

~~c) SQL Injection spade u ovu grupu~~

d**) Moguce je preko “Zakodiranja” informacija u izvornom kodu**

**e) Cuvanje korisnickih imena I lozinki u konfiguracionim XML datotekama spade u ovu grupu**

32. Neadekvatna validacija ulaza(NVU):

**a) je relevantna u procesu razvoja firmvera I ostalog softvera za rutere**

~~b) nije relevantna u procesu razvoja firmvera I ostalog softvera za rutere~~

~~c) je podvrsta buffera overflow-a~~

**d) nije podvrsta SQL Injection napada**

~~e) je grupa slabosti koja najcesce nastaje nenamernom greskom u kompajleru~~

**f) je grupa slabosti koja najcesce nastaje nenamernom greskom u programera**

33. Zaokruziti razloge otezanog sprovodjenja zakona u sudskim procesima na polju sajber kriminala

a) Kompleksnost I nerazumenvanje kriminalnog akta

b) Nepostojanje fizickih dokaza

c) Zrtve cesto ne zele da objave relevantne informacije zbog zastite ugleda I iz finansijskih razloga

d) Otezano odredjivanje visine stete

e) Pocinioci su cesto maloletnici

34. Zaokruziti tacne tvrdnje o odnosu bezbednosnih zona I elektronskog/fizickog perimetra

a) Zona nema perimeter

b) Zona nema nikakve veze sa elektronskim perimetrom

c) Jedini perimeter je na granici informacionog Sistema

d) Ceo informacioni system mora biti u jednoj zoni

e) Fizicki perimeter se retko poklapa sa elektronskim perimetrom

f) Elektronski perimeter se vecim delom nalazi na obodu zone

35. Zaokruziti dva tacna iskaza o KASPERSKY I Syemantec:

~~a) Kaspersky je slovacka kompanija~~

~~b) Symantec je Ruska kompanija~~

**c) Obe kompanije se bave istrazivanje u polju informacione bezbednosti**

~~d) Osnovna delatnost ovih kompanija je razvoj anti malware resenja od njihovog osnivanja~~

**e) Kaspersky je osnovan u Rusiji**

~~f) Obe kompanije su osnovane u evropi~~

SBES 1/2 – Modifikacija je:

~~A. Neutorizovan pristup podacima ili servisima~~

B. Nedostupnost,neupotrebljivost ili unistenje podataka i servisa

**C. Neautorizovana izmena podataka ili servisa**

D. Neautorizovano generisanje dodatnih podataka ili servisa koji nebi postojali u normalnim situacijama

SBES 1/3 – Poredjati faze napada tj upisati redni broj ispred svake od dole navedenih faza:

Enumeracija 2

Perzistencija 4 \*perzistencija znaci zadrzavanje

Izvidjanje 1

Napad 3

SBES 1/5 – Napad u kontekstu sigurnosti i bezbednosti je:

**A. Koriscenje tudjeg identiteta**

**B. Koriscenje slabosti nekog sistema za postizanje nekog cilja**

**C. Neautorizovana izmena podataka ili servisa**

**D. Sve navedeno**

SBES 1/6 – Skeniranje dostupnih bezicnih mreza (tzv. war civing) se radi tokom sledece faze:

**A. Izvidjanje**

B. Perzistencija

C. Enumeracija

D. Ispad

SBES 1/6 – Zaokruziti akcije koje hakeri preduzimaju u fazi napada:

A. Kreiranje spiska bezicnih mreza

**B. Slanje e-mail poruke sa “zarazenim” prilogom**

**C. Izdavanje komande botovima preko C&C servera**

D. Izdavanje komande C&C server sa svih botova

**E. Instalacija rootkit-a**

SBES 2/1 – Zaokruzite eksterne mere fizicke bezbednosti:

**A. Sigurnosna vrata i kapije**

B. Skrivene instalacije

C. Zastita od poplava

**D. Cist prozor oko predmeta zastite**

**E. Adekvatna eksterna rasveta**

SBES 2/2 – Navesti (barem) tri mere fizicke zastite radnog mesta i radne stanice (tj racunara):

Zastita radnog mesta i radne stanice:

* zastita od kradje
* zabrana upotrebe nalepnica
* zabrana razbacivanja papira po random mestu
* biometrijski senzori i jake lozinke
* zakljucavanje sesije cim korisnik cim se korisnik udalji
* osetljive dokumente cuvati zakljucane u sefu.

SBES 2/3 – Zaokruziti prve tri najznacajnije fizicke zastitne mere za zastitu tajnih dokumenata:

**A. Cuvanje dokumenata u sefu**

B. Zastita od poplava

C. Cuvanje dokumenata u fijoci radnog mesta

**D. Senzori za detekciju pristupa (alarm)**

E. Oruzani cuvari

**F. Zakljucana bezbednosna vrata**

G. Neprozirni prozori

**SBES 2/4 – Zaokruziti tri najznacajnije fizicke zastitne mere protiv elementarnih nepogoda:**

A. Neprobojna vrata i prozori

**B. Zastita od poplava**

C. Podela postrojenja u veci broj izolovanih zona D. Senzori za deteklciju nezeljenih dogadjaja

**E. Postavljanje serverskih soba i razvijenog napajanja na vise spratove**

**F. Kreiranje kontrolnih i data cenatara na odgovarajucim geografskim lokacijama**

SBES 2/5 – Poredjati sledece mere (fizicke) bezbednosti u serverskim sobama po prioritetu

**(tj koje treba prvo primeniti) ----------------- odgovor nije siguran??:**

Multifaktorska autentifikacija i stroga kontrola pristupa 2

Skrivanje instalacije (npr. mrezni kablovi) 3

Jedna zakljucana vrata 1

Video nadzor 4

**3 – BEZBEDAN LJUDSKI ELEMENT**

**SBES 3/1 – Zaokruziti odgovore koji ne sadrze pretnje iz grupe socijanog inzinjeringa:**

A. Shoulder surfing

B. Spear phising

**C. Nepozenjne reklame (tj. spam)**

1. Impersonacija
2. **Hakovanje bankomata**

**SBES 3/2 – Poredjati sledece komunikacione kanale po ucestalosti njihove primene u socijalnom inzinjeringu:**

|  |  |
| --- | --- |
| Analogna i digitalna telefonija | 3 |
| Instant messager aplikacije | 2 |
| Email | 1 |
| Papirno pismo | 4 |

**SBES 3/3 – Navesti bar tri mere provere buducih zaposlenih (pre zaposlenja):**

* provera tvrdnji iz CV-a
* provera izdavaoca reference
* provera fizickog i psihickog stanja
* provera prethodnih pozicija na kome je buduci zaposleni radio

**SBES 3/4 - Sta je potrebno uraditi nakon davanja otkaza zaposlenom:**

A. Obrisati ga/je iz telefonskog imenika

**B. Obrisati pripadajuce korisnicke naloge iz internih poslovnih sistema**

**C. Obavestiti partnerske kompanije**

**D. Promeniti administratorske lozinka**

**SBES 3/5 – Navesti bar tri tehnike scijalnog inzinjeringa:**

* Soulder surfing
* Prisluskivanje
* Phishing
* Spear phishing
* Impersonacija

**SBES 3/6 – Zaokruziti tri posebno osetljive faze nadzora rada zaposlenih na osetljivim radnim mestima sa kojih imaju pristup kriticnim delovima informacionih sistema.**

A. Odmah nakon davanja otkaza zaposlenom

B. 3 meseca nakon zaposlenja

C. 6 meseci nakon zaposlenja

**D. Smanjenje plate**

**E. Primena disciplinske mere, npr. promena titule na dole**

**F. U fazi kada su najavljena otpustanja u IT sektoru**

**4 – BEZBEDNI KOMUNIKACIONI KANALI**

**SBES 4/1 – Zaokruziti istinite tvrdnje o elektronskom perimentru.**

**A. Firewall moze biti postavljen na EP**

**B. Uredjaji tipa network tap mogu biti postavljeni na EP**

C. Uredjaji za detekciju i prevenciju ispada (IDS/IPS) se postavljaju samo na EP

D. Kolektori podataka SIEM alata se postavljaju samo na EP

E. Kolektori podataka SIEM alata se ne postavljaju na EP

**F. Kolektori podataka SIEM alata se postavljaju na mobilne elemente EP**

**SBES 4/2 – navesti tri tipa potencijalni zloupotreba mobilnih elemenata informacionog sistema:**

* zaraza malware-om van kompanija i ubacivanje u zasticene zone tj enclave
* kradja
* neautrizovano dizanje sistema npr. preko USB-a

**SBES 4/3 – Zaokruziti istinite iskaze o aplikativnim proxy-jima:**

A. Pracenje aktivnosti sistema i korisnika

**B. Analizira zaglavlja paketa (eng. header)**

**C. Analizira podatke u paketima**

**D. Omogucava filtriranje komandi u aplikativnom sloju**

E. Detekcija anomalija statickom analizom

F. Rad sa audit logovima i detekcija anomalija

G. Detekcija i predlozi korekcija gresaka u konfiguraciji sistema

**SBES 4/4 – Zaokruziti istinite iskaze o IPsec-u:**

**A. Implementira autentifikaciju na 3. OSI sloju**

B. Implementira autentifikaciju na 7. OSI sloju

**C. Omogucava kodiranje podataka u mreznom sloju TCP/IP protokol steka**

D. Omogucava neporecivost u mreznom sloju TCP/IP protokol steka

E. Implementira se aplikativnom tj 7. OSI sloju

**5 - KRIPTOGRAFIJA**

**SBES 5/1 – Zaokruziti karakteristike hash funkcija:**

1. **Jednosmernost**
2. **Slaba otpornost na koliziju**
3. **Jaka otpornost na koliziju**
4. Lako dekodiranje od strane bilo kog ucesnika u distribuiranom sistemu

**SBES 5/2 – Koje operacije koriste AES i DES simetricni algoritmi nad ulaznim podacima:**

1. **Permutacija**
2. Faktorizacija velikih brojeva
3. Rad sa elipticnim krivama
4. **Substitucija**
5. **Logicki operatori (AND, OR, XOR, itd…)**

**SBES 5/3 – Opisati nacin rada, karakteristike i dva mesta prakticne primene jednosmernih (kriptografskih) funkcija:**

Jednosmerna funkcija je kriptografski postupak pretavranja poruke proizvoljne duzine u poruku fiksne duzine.Po definiciji ne postoji inverzna funkija tj nije moguce naci originalnu poruku na osnovu izlaza.

**Karakteristike jednosmernih funkcija:**

* nepostojanje inversne funkcije
* deterministicnost  za isti ulaz uvek cemo dobiti identican izlaz
* uniformnost  ravnomerno mapiranje ulaza na prosto izlaza
* jaka optpnost na koliziju
* slaba otpornost na koliziju

**Jednosmerne funkcije si primenjuju:** za proveru ispravnosti poslatih sadrzaja, za skaldistenjesifri, kao deo digitalnog potipisa i u hash tabeleme tj struktura podataka za brzu pretragu.

**SBES 5/4 – Zaokruziti istinite tvrdnje o kriptografiji i kriptoanalizi:**

A. Cilj kriptografije je unapredjivanje postojecih i razvoj novih algoritama

B. Cilj kriptoanalize je unapredjivanje postojecih i razvoj novih algoritama

C. Kriptografija je zasnovana na faktorizaciji velikih brojeva

**D. Kriptoanaliza izucava tehnike nalazenja originalne poruke bez poznavanja kljuca**

E. U kriptografiji duzina kljuca zavisi od duzine kodirane poruke

**SBES 5/5 – Zaokruziti tacne tvrdnje o AES simetricnom algoritmu.**

**A. Koristi operaciju permutacija**

B. Ne koristi operaciju permutacija

C. Zasnovan na faktorizaciji velikih brojeva

**D. Tip algoritma block chaper**

E. Duzina kljuca zavisi od duzine kodirane poruke

**F. Slozenost je maksimalno 14 iteracija sa 256-bitnim kljucem**

**SBES 5/6 – Objasniti princip rada ECB moda kod simetricnih algoritama:**

ECB je mod rada block chipper vrte simetricnih algoritama gde algoritam deli poruku na jednake blokove duzine n (i ako treba dopunjava poslednji do duzine n). Enkriocija i dekripcija se radi na taj nacin da se operacije izvrsavaju na svakom bloku posebno tj blokovi su nezavisni jedni od drugih. Prednost ovog moda je brzina i mogucnost paraleliacije, dok je mana da mogu postojati isti blokovi i otkrivanjem jednog bloka, automatski otkrivamo i sve ostale iste blokove.

**SBES 5/7 – Koje operacije izvrsava SHA256 kriptografski algoritam nad ulaznim podacima.**

1. **Permutacija**
2. Faktorizacija velikih brojeva
3. Rad sa elipticnim krivama
4. **Substitucija**
5. **Logicki operatori (AND, OR, XOR, itd…)**

**SBES 5/8 – Na koja pitanja treba da odgovori upravljanje bezbednim mehanizmima**

**A. Kako se distribuiraju tajni kljucevi?**

**B. Koliki je zivotni vek kljuceva?**

**C. Kako se povlace razbijeni kljucevi?**

D. Ko ce snimiti javni kljuc na USB disk?

**E. Kako realizovati delegaciju prava pristupa?**

F. Kako se otvara bezbedan komunikacioni kanal?

**6 – BEZBEDNOST RACUNARSKIH SISTEMA**

**SBES 6/1 – Autorizacija je:**

**A. Dodela prava pristupa**

B. Otvaranje bezbednog komunikacionog kanala

C. Pojam koji se cesto mesa sa kontrolom pristupa (podacima i/ili) servisima

**SBES 6/2 – Zaokruziti usluge koje pruzaju SIEM alati:**

**A. Prikupljanje i skladistenje monitoring podataka**

**B. Agregacija i korelacija podataka**

**C. Staticka obrada podataka**

1. **Dashboard**
2. Aktivna zastita od zlonamernog softvera
3. **Dokazani material u slcajevima krivicnih dela**

**SBES 6/3 – Zaokruziti usluge koje pruzaju najmoderniji operativni sistemi za medjusobnu zastitu adresnih prostora procesa:**

A. Bazni registar

**B. Deljenje memorijskih blokova podataka u stranice**

C. Ograda izmedju podataka i instrukcija

D. Tagovanje memorisjkih lokacija

E. Staticka obrada podataka

1. Dashboard
2. **Deljenje memorije procesa na segmente**

**SBES 6/4 – Auditing je:**

Vodjenje istorijata aktivnosti u informacionom sistemu koristeci event log, logove korisnickih aplikacija.Takodj pamti vremena i korisnika za svaku transakciju,Auditing in a njemu bazirana softverska resenja su kljucne zastitne mere u borbi protiv APT.

**SBES 6/5 – Autentifikacija je:**

A. Provera prava pristupa

**B. Provera identiteta nekog entiteta u DS**

C. Otvaranje bezbednog kanala

**SBES 6/6 – Sa cim se ne radi autentifikacija?**

A. Deljeni tajni kljuc

B. Centar za distribuciju kljuceva

C. Javni kljucevi

**D. Hash funkcija**

**SBES 6/7 – Kada je matrica prava pristupa velika (sa ciljem optimizacije) uvode se:**

A. Digitalni potpisi

**B. Liste prava pristupa (Access Control List - ACL)**

**C. Dozvole (Capabilities)**

**SBES 6/8 – Sta nije potrebno za autentifikaciju.**

A. Da se zna tacan identitet obe (ili vise) strane

B. Da se ocuvaintegritet poruka

**C. Da se ekskluzivno odvoje fizicki resursi**

D. Da se ocuva tajnost poruka

**SBES 6/9 – Zaokruziti istinite iskaze o listama za kontrolu pristupa**

**A. Omogucava zastitu integriteta fajl sistema**

B. Omogucava deljenje memorijskih blokova podataka u stranice

**C. Koristi se u kontekstu kontrole fizickog pristupa**

D. Ne koristi se u kontekstu kontrole fizickog pristupa

E. Onemogucava staticku obradu podataka

**F. Efikasnije je od MAC modela u velikim sistemima**

G. Manje je efikasno od MAC modela u velikim sistemima

**SBES 6/10 – Zaokruziti istinite iskaze o merama bazbednosti za zastitu fajl sistema**

A. OS onemogucava zastitu integriteta fajl sistema

B. EFS je sistem kodiranja delova ili celog fajl sistema na Linux OS

**C. EFS je sistem kodiranja delova ili celog fajl sistema na Windows OS**

D. OS omogucava pristup sistemskim fajlovima svim korisnicima

**E. OS onemogucava pristup sistemskim fajlovima svim korisnicima**

**SBES 7/1 – Zaokruziti tacne tvrdnje o malware-u tipa trojanac i crv:**

A. Crvu je potreban nosilac

B. Trojancu nije potreban nosilac

**C. Crv se sam replicira**

D. Crv se ne replicira

**E. Trojanac se cesto koristi kao nosilac**

**SBES 7/2 – Zaokruziti istinite tvrdnje o kompaniji Symantec:**

**A. Bavi se istrazivanjem na polju informacione bezbednosti**

**B. Osnovana je u SAD**

C. Osnovana je u Rusiji

D. Detektovali su zlonamerne softvere Duqu, Stuxnet i BlackEnergy

E. Prvobitna delatnost im je bila razvoj anti-malware alata

**SBES7/3 – Najcesci komunikacioni kanal za sirenje malware-a tipa trojanac je:**

e-mail.

**BES 7/4 – Zaokruziti istinite pretnje o zlonamernim softverima keyloger i virus:**

**A. Virus je pretnja tipa modifikacija**

B. Virus je pretnja tipa prisluskivanje

**C. Keylogger je pretnja tipa prisluskivanje**

D. Keylogger je pretnja tipa fabrikacija

**E. Virus moze biti pretnja tipa ispad**

**SBES 7/5 – Zaokruziti ono sto je tacno za logicku bombu:**

1. **Jedan tip malware-a**
2. Izvrsava se preko botnet-a
3. Kreira zombie racunar
4. **Koristi se za napad na izolovane uredjaje**

**SBES 7/6 – Zaokruzite istinite tvrdnje o malware-u tipa virus i crv:**

A. Crvu jepotreban nosilac

B. Virusu nije potreban nosilac

**C. Crv se sam replicira**

D. Crv se ne replicira

**SBES 7/7 – Kaspersky Labs je detektovao sledece zlonamerne softvere (malware):**

1. Sandworm
2. **Equation Group**
3. Stuxnet
4. **BlackEnergy**
5. **Flame**

**SBES 7/8 – Zaokruziti tacno dve funkcionalnosti koje ne pruzaju moderna anti-malware resenja:**

A. Povezivanje sa jezrom operativnog sistema

1. Skeniranje e-mail priloga
2. **Staticka analiza mreznog saobracaja**
3. Ciscenje zarazenog racunara od zlonamernog softvera
4. Premestanje sumljivih datoteka u karantin
5. **Detekcija botnet-a**

**SBES 7/9 – Zaokruziti karakteristiku koja se nekoristi za klasifikaciju malware-a:**

A. Tip replikacije

B. Potreban nosilac (DA/NE)

**C. Povezivanje sa jezgrom OS (DA/NE)**

1. Kompleksnost
2. **Vidljivost tj nivo prikrivenosti malware-a**

**SBES 8/1 – Zaokruziti tacne iskaze o statickoj analizi izvornog koda:**

A. Poznata i pod imenom black box testing

**B. Kljucni ulaz je izvorni kod softvera**

**C. Postoje alati koji mogu automatizovati proces analize**

**D. Deo staticke analize je manualna analiza izvornog koda**

**E. Neki od poznatih alata za staticku analizu su u vlasnistvu kompanije IBM, Microsoft i HP**

**SBES 8/2 - Zaokruziti tacne iskaze o interaktivnoj analizi aplikativnih procesa:**

A. Poznata i pod imenom white box testing

B. Kljucni ulaz je izvorni kod softvera

**C. Kljucni ulaz je proces u izvrsavanju i ulazi procesa za potrebe testa**

**D. Postoje alati koji mogu automatizovati proces analize**

E. Deo interaktivne analzie je manualna analiza izvornog koda

**F. Ima prednosti u odnosu na staticku i dinamicku analizu, npr detekcija anomalija, manji broj laznih pozitivnih detekcija**

**SBES 8/3 – Navesti barem dve prednosti interaktivne analize izvornog koda u odnosu na druge dve tehnike analize (staticka i dinamicka):**

* manji broj laznih pozitivnih detekcija,
* detekcija u realnom vremenu,
* smanjena potreba za ekspertima koji analiziraju detektovane anomalije

**SBES 8/4 – Zaokruziti tacne iskaze o otktivanju kriticnih informacija u kontekstu razvoja bezbednog softvera:**

A. Definise se kao prototip neadekvatne validacije ulaza

B. Buffer overflow

C. SQL injection spade u ovu grupu

**D. Moguca je preko “zakodiranja” informacija u izvornom kodu**

**9 – PRAVNI ASPEKTI**

**SBES 9/1 – Zaokruziti istinite tvrdnje o zabrani konkurencije:**

A. Na trzistu nije dozvoljeno izdavanje slicnih proivoda

B. Zaposleni ima (neograniceno) parvo da predje u konkurentsku kompaniju

**C. Zaposleni ne sme da predje u konkurentsku kompaniju ako je stekao sirok krug poslovnih partnera i znanje iz oblasti**

**D. Kompanija treba da plati bivsem zaposlenom ako aktivira klauzulu ugovora o radu vezano za zabranu konkurencije**

**SBES 9/2 – Zaokruziti razloge otezanog sprovodjenja zakona u sudski procesima na polju kiber-kriminala:**

**A. Pocinioci su cesto maloletnici**

**B. Zrtve cesto ne zele da objave relevantne informacije zbog stete ugleda i iz finansijskih razloga**

**C. Nepostojanje fizickih dokaza**

**D. Kompleksnost i nerazumevanje kriminalnog akta**

**E. Otezano odredjivanje visine stete**

F. Rukovanje licnim podacima nije uskladjeno sa relevantnim zakonima nor. Zakon o informisanju bezbednosti

**SBES 9/3 – Zaokruziti tvrdnje koje su istinite o patentima i autorskom pravu:**

A. Patent traje beskonacno

B. Autorsko pravo traje beskonacno

**C. Autorsko pravo stiti intelektualnu svojinu**

D. Patent stiti intelektualnu svojnu

**E. Patent stiti naucne, tehnoloske i inzinjerske rezultate**

**SBES 9/4 – Zaokruziti krivicna dela koja KZ ne definise eksplicitno u kontekstu zastite podataka u Republici Srbiji:**

**A. Spear phishing**

B. Racunarska sabotaza

C. Racunarska prevara

1. **Ransomware**
2. Racunarska prevara
3. Sprecavanje i ogranicavanje pristupa javnoj racunarskoj mrezi, npr DoS
4. Ostecenje racunarskih podataka i programa

**SBES 9/5 – Zaokruziti istinite iskaze o zakonskoj regulativi kiber prostora u RS:**

**A. Srbija je potvrdila (medjunarodnu) konvenciju o visokotehnoloskom kriminalu**

B. Srbija nije potvrdila (medjunarodnu) konvenciju o visokotehnoloskom kriminalu

C. Krivicni zakonik (KZ) eksplictno navodi phishing kao krivicno delo

**D. KZ eksplicitno navodi racunarsku sabotazu kao krivicno delo**

**E. KZ eksplicitno navodi racunarsku prevaru kao krivicno delo**

F. KZ eksplicitno navodi ransomware kao krivicno delo

**11 – BEZBEDONOSNA POLITIKA**

**SBES 11/1 – Tokom formiranja bezbedonosne politike je potrebno napraviti popis cinioca informacionog sistema:**

**A. Poslovna tajna**

**B. Serverska soba**

**C. Kancelarija rukovodstva**

**D. Trenutno koriscene mere autentifikacije zaposlen ih**

**E. Interni procesi i procedure**

**F. Spisak svih zaposlenih**

**SBES 11/2 – Zaokruzitit mere ocvrscenja sistema (eng. system hardering):**

**A. Gasenje suvsinih servera**

B. gasenje antivirusa

**C. Zatvaranje suvisnih portova**

**D. Redovni i obavesi treninzi**

**E. Stroga kontrola fizickog pristupa**

**12 – ORGANIZACIJE, STANDARDI, PREPORUKE**

**SBES 12/1 – Koje dve mere izdvaja na pocetku SANS Top 20 Critical Security Controls:**

**A. Kreiranje popisa opreme**

B. Kontrolisana primena administrativnih prava

C. Zastita podataka

D. Upravljanje bezicnim pristupom

**E. Kreiranje popisa softvera**

1. Mogucnost oporavka podataka (npr. iz backup-a)
2. Popis svih perzistentnih pretnji u sistemu

**SBES 12/2 – Navesti glavne zadatke organizacije ISC2:**

ISC2 je medjunarodna, neprofitna organizacija,osnovana 1988, sa ciljem razvoja sigrunog i bezbednog kiber prostora.Bavi se treningom i sertifikacijom.Ima 115000 clanova i centralama im je u Palm Harbor-u (Florida, USA).

**SBES 12/3 – Zaokruziti imena institucija u RS cija je osnovna delatnost vezana za (informacionu) bezbednost:**

**A. Bezbedonosno infromativna agencija (BIA)**

B. Sluzba drzavne bezbednosti (DB)

**C. Univerzitet bezbednosti (UB)**

D. Univerzitet u Beogradu

**E. Kriminalisticko-policijski univerzitet (bivsa kriminalisticko-policijska akademija - KPA)**

**EH-001 – Zaokruziti slabosti web sadrzaja koje su kriminalci najcesce zloupotrebljavali 2019. godine:**

**A. Slabe lozinke korisnika i/ili administratora**

B. SQL injection

C. Reverzni inzinjering

D. Slabosti koriscenih biblioteka i ekstenzija web platformi

**E. Buffer overread**

**EH – 002 –Zaokruziti tacne sikaze o kontekstu reverznog inzinjeringa:**

A. Moguca je dinamicka analiza PE fajlova na Linux platformi B. SQL injection spade u ovu grupu

**C. Nije moguca je dinamicka analiza PE fajlova na Linux platformi D. Za reverzni inzinjering je potrebno poznavanje asmeblera**

E. Buffer overflow pada u grupu tehnika reverznog inzinjeringa

**44. Zaokruzi najvazniju meru u procesu jacanja bezbednosti ljudskog elementa**

**-Redovni treninzi o najnovijim pretnjama I merama**

**45. Zaokruzi 4 najvaznije mere u procesu jacanja bezbednosti ljudskog elementa**

**-Redovni treninzi o najnovijim pretnjama I merama**

**-Vodjenje istorijata o odrzanim treninzima**

**-Slanje kratkih obavestenja o najnovijim pretnjama**

**-Kreiranje modern politike bezbednosti ljudskog elementa**

46. Sta ne spade u gupu osnovnih ciljeva sigurnosti I bezbednosti

-Enkapsulacija klasa

47. Zaokruziti istinite iskaze o zakonskoj regulative kiber prostora u republici srbiji

-Srbija je ptrvrdila(Medjunarodnu)konvenciju o visko tehnoloskom kriminalu

\*FALI JOS

48. Zaokruzi odgovor koji NE sadrzi tip firewall

Antivirus

49. Zaokruzi istinite tvrdnje o poslediciama BLACK ENERGY napada na ees preduzeca u Ukrajini

-Inicijalni vector napada je bio preko SpearPhishinga kampanje

50. Formiranje I pustanje u pogon botnet-u je krivicno delo?

DA

51. Zaokruzi istinite iskaze o kradji identiteta

-Otvaranje racuna u banci sa tudjim JMBG brojem krajda identiteta

52. Miral botnet napad je 2016izveden zloupotrebama tipa:

-Zloupotreba slabo zasticenih IoT uredjaja sa javnim IP adresama

-Izdavane komande botovima prekoC&C server

53. Zaokruzi istinite iskaze o fizickom unistavanju nosioca podataka

-Nakon demagnetizacije se magnetni mediji(HARD DISK)

-Papirna dokumenta se uniste sredeerom I strucno recikliraju

54. Interaktivna analiza Aplikativnih procesa

-Kljucni ulaz je process u izvrsavanju I ulazu procesa za potrebe testa

-Postoje alati koji mogu automatizovati process analiza

-Ima prednost u odnosu na staticku dinamicku analizu

55. Zaokruziti istinite iskaze o zlonamernom softveru tipa rabbit

-Nema aktivnu ulogu u botnet-ima

-FALI JOS

56. Srbija klasifikuje kiber

-Kodiranje I dekodovanje se vrsi u aplikativnim slojevima

57. Napad u kontekstu sigurnosti I bezbednosti

-Koriscenje tudjeg identiteta

- Koriscenje salbosti nekog Sistema za postizanje nekog cilja

-Neautorizovana izmena podataka ili servisa