

Stanje	Završeno
Započeto	ponedjeljak, 30. lipnja 2025., 17:34
Završeno	ponedjeljak, 30. lipnja 2025., 18:22
Utrošeno vrijeme	47 min 53 s
Ocjena	Još nije ocijenjeno

Pitanje 1

Točno

Broj bodova: 2,50 od 2,50

"The Open Web Application Security Project" (OWASP) svake godine izdaje popis 10 najraširenijih rizika na **IoT uređajima**. Povežite rizike s ponuđenim metodama za ublažavanje ili sprječavanje:

- Nesigurne mrežne usluge (**Insecure Network Services**) je rizik koji se ublažava/sprječava
gašenjem nepotrebnih servisa, ažuriranje servisa na najnoviju verziju. ✓
- Nesigurni mehanizmi nadogradnji (**Lack of Secure Update Mechanism**) je rizik koji se ublažava/sprječava
šifriranjem kanala za ažuriranje firmwarea. ✓
- Zastarjele komponente (Use of Insecure or Outdated Components) ✓ je rizik koji se ublažava/sprječava promjenom sklopovlja ili pojedinih elemenata sklopovlja na uređaju.
- Nedovoljno šifriranje (Insecure Data Transfer and Storage) ✓ je rizik koji se ublažava/sprječava ispravnim korištenjem infrastrukture PKI.
- Nedostatak upravljanja (**Lack of Device Management**) je rizik koji se ublažava/sprječava
popisivanjem uređaja i njihovih lokacija te čestim provjerama. ✓

Povucite ponuđene odgovore na ispravno mjesto u tekstu.

Napomena: netočan odgovor **NE** nosi negativne bodove.

Loše lozinke (Weak Guessable, or Hardcoded Passwords)

Loše početne postavke (Insecure Default Settings)

Nesigurne mrežne usluge (Insecure Network Services)

Loša privatnost (Insufficient Privacy Protection)

Nedostatak upravljanja (Lack of Device Management)

Nesigurni mehanizmi nadogradnji (Lack of Secure Update Mechanism)

Nesigurna sučelja (Insecure Ecosystem Interfaces)

Fizička sigurnost (Lack of Physical Hardening)

ispravnim korištenjem infrastrukture PKI.

promjenom sklopovlja ili pojedinih elemenata sklopovlja na uređaju.

zaključavanjem prostorije u kojoj se nalazi uređaj.

autentifikacijom na web poslužitelju koji služi kao agregator podataka.

postavljanjem lozinke uređaja na dugački, komplicirani niz slova, brojeva i drugih znakova.

uključivanjem anonimizacije podataka.

brisanjem default korisnika (admin, user, pi...)

Vaš odgovor je točan.

Ispravan odgovor je:

"The Open Web Application Security Project" (OWASP) svake godine izdaje popis 10 najraširenijih rizika na **IoT uređajima**. Povežite rizike s ponuđenim metodama za ublažavanje ili sprječavanje:

- Nesigurne mrežne usluge (**Insecure Network Services**) je rizik koji se ublažava/sprječava [gašenjem nepotrebnih servisa, ažuriranje servisa na najnoviju verziju.]
- Nesigurni mehanizmi nadogradnji (**Lack of Secure Update Mechanism**) je rizik koji se ublažava/sprječava [šifriranjem kanala za ažuriranje firmwarea.]
- [Zastarjele komponente (Use of Insecure or Outdated Components)] je rizik koji se ublažava/sprječava promjenom sklopovlja ili pojedinih elemenata sklopovlja na uređaju.
- [Nedovoljno šifriranje (Insecure Data Transfer and Storage)] je rizik koji se ublažava/sprječava ispravnim korištenjem infrastrukture PKI.
- Nedostatak upravljanja (**Lack of Device Management**) je rizik koji se ublažava/sprječava [popisivanjem uređaja i njihovih lokacija te čestim provjerama.]

Povucite ponuđene odgovore na ispravno mjesto u tekstu.

Napomena: netočan odgovor **NE** nosi negativne bodove.

Pitanje 2

Završeno

Broj bodova od 5,00

Objasnite napad u SS7 kojim napadač može otkriti lokaciju korisnika.

U SS7 napadu napadač može preko paging callova utvrditi koji baznim stanicama se korisnik javio te preko lokacija tih baznih stanica zaključiti gdje se korisnik nalazi.

Pitanje 3

Završeno

Broj bodova od 2,00

Što je USSD (Unstructured Supplementary Service Data) i za što se koristi? Navedite primjer!

Dodatni podatci o korisnici koji operateri koriste/zadržavaju u bazi. Najčešće se danas koristi za provjeru stanja na računu (za korisnike sa bonovima) dok se prije s USSD-om mogao plaćati parking, računi....

Često je korišten u napadima gdje su ljudima skidali novce koje bi im onda telekom kasnije naplatio.

Pitanje 4

Točno

Broj bodova: 1,00 od 1,00

Što znači skraćenica TMSI u kontekstu signalizacije u telekomunikacijskim mrežama?

Napomena: netočan odgovor nosi negativne bodove (-20%).

- ☐ a. Traditional Mobile Subscriber Identity
- ☐ b. Telecom Mobile Subscriber Identity
- ☐ c. Transmission Mobile Subscriber Identity
- ☐ d. Temporal Mobile Subscriber Identity
- ☒ e. Temporary Mobile Subscriber Identity ✓

Vaš odgovor je točan.

Ispravan odgovor je:

Temporary Mobile Subscriber Identity



Pitanje 5

Netočno

Broj bodova: 0,00 od 1,00

Koje sve podatke mreža čuva o korisnicima?

Napomena: Svi odabrani odgovori moraju biti **točni** da bi se ostvarili bodovi u ovom zadatku.

- ☒ a. Popis svih baznih stanica (CellID, MCC, LAC) na kojima su se uređaji nalazili. 
- ☐ b. Snimke svih poruka.
- ☐ c. Snimke svih poziva.
- ☒ d. Zapise o korisnicima u smislu poziva i pristupa mreži i lokacijama (Call Data Records, CDR). 

Vaš odgovor nije točan.

Ispravan odgovor je:

Zapise o korisnicima u smislu poziva i pristupa mreži i lokacijama (Call Data Records, CDR).

Pitanje 6

Završeno

Broj bodova od 5,00

U kratko objasnite što sadrži IOT Security Verification Standard. Za što se sve može koristiti?

Definira pravila kako na siguran način upravljati i koristiti IOT uređaje tj. smjernice koje bi trebali pratiti.
Najkorisniji pri izradi mreže senzora ili autorizacije korisnika u firmama (RF-uređaji, BLE čipovi).

Pitanje 7

Točno

Broj bodova: 1,00 od 1,00

Na koji se način provodila kompromitacija IoT uređaja kod tzv. Mirai Botneta?

Napomena: netočan odgovor nosi negativne bodove (-25%).

- ☐ a. Korištenjem tehnika društvenog inženjeringa za prevaru korisnika da preuzmu zlonamjerni kod.
- ☐ b. Inficiranjem uređaja putem zlonamjernih web stranica.
- ☒ c. Iskorištavanjem slabih vjerodajnica na IoT uređajima. ✓
- ☐ d. Iskorištavanje *buffer overflow* ranjivosti u servisima koje koriste IoT uređaji.

Vaš odgovor je točan.

Ispravan odgovor je:

Iskorištavanjem slabih vjerodajnica na IoT uređajima.

Pitanje 8

Točno

Broj bodova: 1,00 od 1,00

Universal Plug and Play uređaji koriste autentifikaciju ključevima i stoga ih nije moguće iskoristiti za napade.

Napomena: netočan odgovor nosi negativne bodove (-50%).

- ☒ a. Netočno ✓
- ☐ b. Točno

Vaš odgovor je točan.

Ispravan odgovor je:

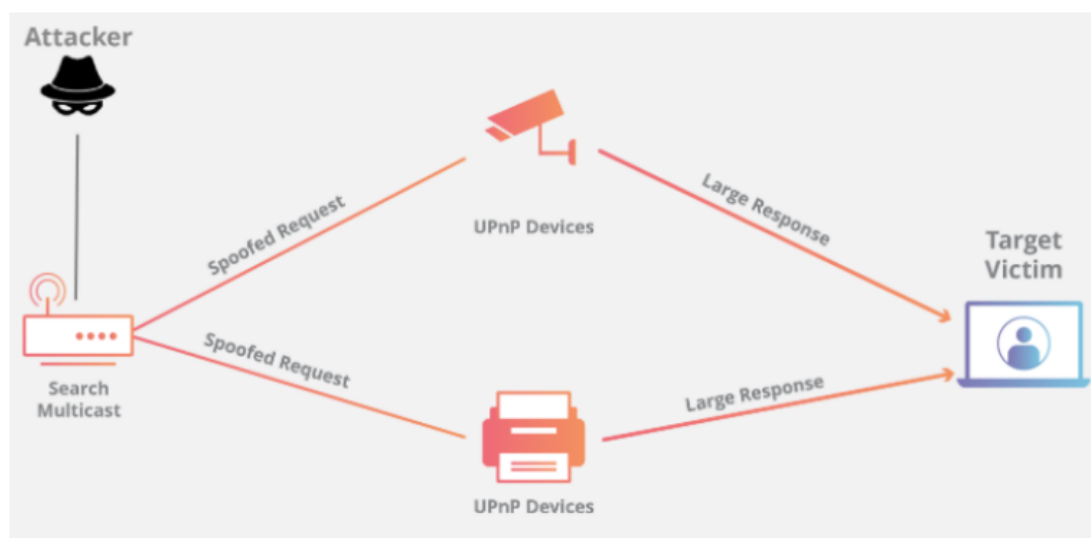
Netočno

Pitanje 9

Točno

Broj bodova: 1,00 od 1,00

Slika prikazuje napad DDoS napad korištenjem protokola SSDP. Odredite koja od navedenih svojstava napadač koristi u napadu.



- ☒ a. Amplification i Reflection ✓
- ☐ b. Amplification
- ☐ c. Reflection
- ☐ d. Ništa od navedenog

Vaš odgovor je točan.

Ispravan odgovor je:

Amplification i Reflection

Pitanje 10

Završeno

Broj bodova od 1,00

Dobili ste e-poštu s adrese dekan@fer.unizg.hr. Pregledom zaglavlja vidljivo je da su provjere SPF i DMARC u redu. Možete li biti sigurni da je poruku uistinu poslao Dekan FER-a?

Malo čudno pitanje s obzirom da poruku nije morao poslati Dekan već bilo tko sa pristupom njegovom računu.

Što se konkretne sigurnosti tiče možemo biti sigurni da sadržaj poruke nije mijenjan.

Pitanje 11

Točno

Broj bodova: 1,00 od 1,00

Prenosi se poruka kodirana korištenjem base64. MITM napadač može saznati sadržaj te poruke.

Napomena: netočan odgovor nosi negativne bodove (-50%).

- ☒ a. Točno ✓
- ☐ b. Netočno

Vaš odgovor je točan.

Ispravan odgovor je:

Točno

Pitanje 12

Točno

Broj bodova: 1,00 od 1,00

DM

Dian Mawanti <hellenkratti@gmail.com>

Ja sam gospođa Dian Mawanti, glavna odvjetnica pokojnog Ing. Ivan Petrović (Moj klijent) iz vaše zemlje, koji je bio direktor građevinske tvrtke Orient ovdje u Indoneziji prije nego što je preminuo od leukemije 3. ožujka 2016. u vojnoj bolnici Gatot Soebroto, Indonezija. S tim u vezi želim vas obavijestiti da mi je Banka izdala obavijest da na njegov račun dostavim najbliže rođake. Već četiri godine ne uspijevam locirati rodbinu svog pokojnog klijenta.

Svečano tražim vaš pristanak da vas predstavim kao najbližeg rođaka pokojnika budući da imate isto državljanstvo, tako da će vam prihodi s ovog računa, u vrijednosti od tri milijuna osamsto tisuća dolara, biti uplaćeni vama, kako bismo ih podijelili u omjeru 50% za mene i 50% za tebe. Sve što mi je potrebna je vaša iskrena suradnja kako biste nam omogućili da dovršimo ovu transakciju.

Tvoje puno ime:

Adresa:

Dob:

Okupacija:

Telefon ili mobitel:

Čekam vaš hitan odgovor kako bih vam mogao dati dodatna pojašnjenja.

Iskreno

Barr. Dian Mawanti

Prikazanu poruku dobili ste u Vaš sandučić elektroničke pošte pri čemu osobu Dian Mawanti **NE** poznajete. Navedena poruka prikazuje:

Napomena: netočan odgovor nosi negativne bodove (-20%).

- ☒ a. Pokušaj phishinga ✓
- ☐ b. Pokušaj instaliranja zlonamjernog programa tipa "virus" na Vaše računalo
- ☐ c. Pokušaj phreakinga
- ☐ d. Pokušaj phrakinga.
- ☐ e. Pokušaj instaliranja zlonamjernog programa tipa "ransomware" na Vaše računalo

Vaš odgovor je točan.

Ispravan odgovor je:

Pokušaj phishinga

Pitanje 13

Točno

Broj bodova: 1,00 od 1,00

Simple Mail Transfer Protocol (SMTP) sadrži sigurnosne mehanizme.

Napomena: netočan odgovor nosi negativne bodove (-50%).

- ☐ a. Točno
- ☒ b. Netočno ✓

Vaš odgovor je točan.

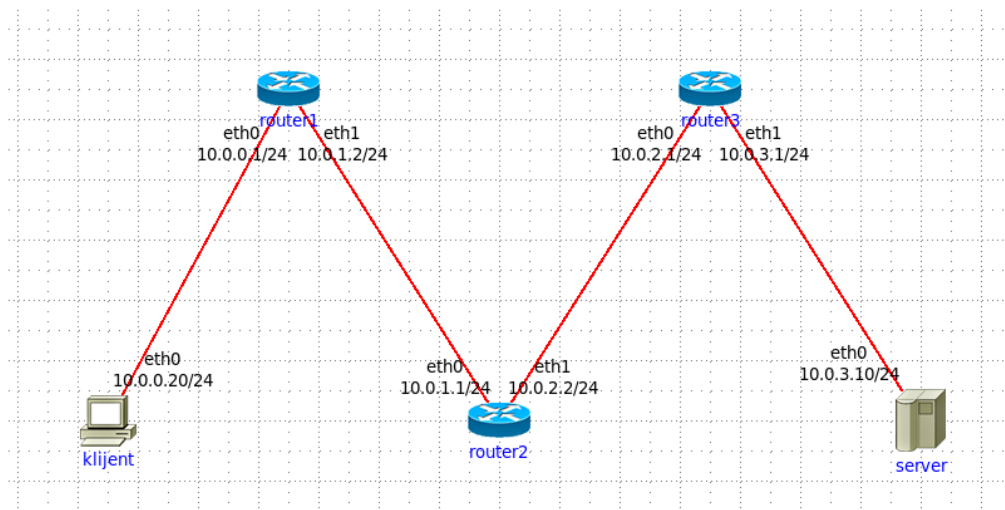
Ispravan odgovor je:

Netočno

Pitanje 14

Točno

Broj bodova: 1,00 od 1,00



U mreži prikazanoj na slici, napravljen je GRE tunel između čvorova *klijent* i *server* naredbama:

```
root@klijent:/# ip tunnel add gre11 mode gre remote 10.0.3.10 local 10.0.0.20 ttl 255
root@klijent:/# ip link set gre11 up
root@klijent:/# ip addr add 11.11.11.1/24 dev gre11
root@klijent:/# ip addr show dev gre11
```

i

```
root@server:/# ip tunnel add gre11 mode gre remote 10.0.0.20 local 10.0.3.10 ttl 255
root@server:/# ip link set gre11 up
root@server:/# ip addr add 11.11.11.2/24 dev gre11
root@server:/# ip addr show gre11
```

Odredite istinitu tvrdnju.

Napomena: netočan odgovor nosi -25% bodova.

- ☐ a. Čvorovi tipa *Router* **ne** rade usmjeravanje na mrežnom sloju te zbog toga **ne** analiziraju GRE zaglavlje.
- ☐ b. Čvorovi tipa *Router* **ne** rade usmjeravanje na mrežnom sloju te zbog toga analiziraju GRE zaglavlje.
- ☒ c. Čvorovi tipa *Router* rade usmjeravanje na mrežnom sloju te zbog toga **ne** analiziraju GRE zaglavlje. ✓
- ☐ d. Čvorovi tipa *Router* rade usmjeravanje na mrežnom sloju te zbog toga analiziraju GRE zaglavlje.

Vaš odgovor je točan.

Ispravan odgovor je:

Čvorovi tipa *Router* rade usmjeravanje na mrežnom sloju te zbog toga **ne** analiziraju GRE zaglavlje.


Pitanje 15

Netočno

Broj bodova: -0,20 od 1,00

Koja od sljedećih tvrdnji **nije točna**?

Napomena: netočan odgovor nosi **negativne** bodove (-20%).

- ☐ a. DNSSEC ne štiti od DDoS napada
- ☐ b. DNSSEC osigurava kriptografski dokaz ispravnosti primljenih podataka.
- ☐ c. DNSSEC nema nikakav utjecaj na mrežu i vatrozide
- ☒ d. Kod DNSSEC-a zapisi na poslužitelju (RR – Resource Records) se potpisuju privatnim ključem 
- ☐ e. DNSSEC ne osigurava povjerljivost podataka.

Vaš odgovor nije točan.

Ispravan odgovor je: DNSSEC nema nikakav utjecaj na mrežu i vatrozide

Pitanje 16

Točno

Broj bodova: 2,00 od 2,00

Povežite pojmove s objašnjenjima:

Dual Homed Gateway	✓	je uređaj koji se smješta između privatne mreže i Interneta i mora biti " <i>bastion host</i> ".
Bastion host	✓	je uređaj koji je kritična ali dobro osigurana točka u mreži.
Screening router	✓	je uređaj koji obavlja usmjeravanje uz mogućnost neke vrste filtriranja paketa
Screened Host Gateway	✓	sav promet iz javne mreže " <i>screening router</i> " propušta samo do " <i>bastion hosta</i> " smještenog u privatnoj mreži.

Napomena: netočan odgovor **NE** nosi negativne bodove.

Screened Subnet

Demilitarized Zone

Vaš odgovor je točan.

Ispravan odgovor je:

Povežite pojmove s objašnjenjima:

[Dual Homed Gateway] je uređaj koji se smješta između privatne mreže i Interneta i mora biti "*bastion host*".

[Bastion host] je uređaj koji je kritična ali dobro osigurana točka u mreži.

[Screening router] je uređaj koji obavlja usmjeravanje uz mogućnost neke vrste filtriranja paketa

U [Screened Host Gateway] sav promet iz javne mreže "*screening router*" propušta samo do "*bastion hosta*" smještenog u privatnoj mreži.**Napomena:** netočan odgovor **NE** nosi negativne bodove.**Pitanje 17**

Završeno

Broj bodova od 3,00

Kako se dijele sustavi za detekciju napada? Objasnite ih.

EDR, NDR, XDR, IDS, NIDS, SIEM...

EDR - Endpoint Detection & Response

Nadzor i zaštita krajnjih točaka

NDR - Network Detection & Response

Nadzor i zaštita mreže

XDR - Extended Detection & Response

Evoluirani nadzor i zaštita - EDR+NDR+nadzor maila+...

IDS - Intrusion Detection System

Sustav za detekciju upada u sustav

NIDS - Network Intrusion Detection System

Sustav za detekciju upada u mrežu


Pitanje 18

Netočno

Broj bodova: -0,50 od 1,00

SSH tehnika "jump host" je tehnika u kojoj se ssh veza proslijeđuje na konačno odredište kroz jedan ili više posredničkih poslužitelja. Da bi se ssh veza mogla proslijediti ako koristimo kriptografiju javnog ključa, na krajnje računalo mora se instalirati privatni ključ, a na sva ostala računala između korisničkog i krajnjeg računala mora se instalirati javni ključ.

Napomena: netočan odgovor nosi negativne bodove (-0,5).

-
- ☒ a. Točno 
- ☐ b. Netočno

Vaš odgovor nije točan.

Ispravan odgovor je:

Netočno

Pitanje 19

Završeno

Broj bodova od 3,00

Objasnite značenje pojma "*port forwarding*" u kontekstu korištenja programa *ssh* (*Secure Shell*).

Port forwarding je mogućnost "prosljeđivanja" servisa preko portova. Najpoznatiji je primjer gdje su napadači iskorištavali tu mogućnost za napad na printere (zato sada većina poduzeća ima isključen port forwarding na svojim uređajima). Port forwarding u kontekstu ssh bi značilo pristup ssh servisu na nekom uređaju kroz indirektan port.

Pitanje 20

Završeno

Broj bodova od 3,00

Koja je razlika između *TCP SYN* i *TCP connect()* skeniranja otvorenih vrata? Kako biste otkrili da ste žrtva *TCP connect()* skeniranja? Objasnite.

TCP SYN napad ne ostvari 3-way-handshake dok TCP connect() ostvari, to nam dovodi do toga da sa TCP SYN skenom brže skeniramo no imamo manju pouzdanost o dostupnosti servisa dok sa TCP connectom možemo biti sigurni da na nekom portu postoji određeni servis i da ODGOVARA!

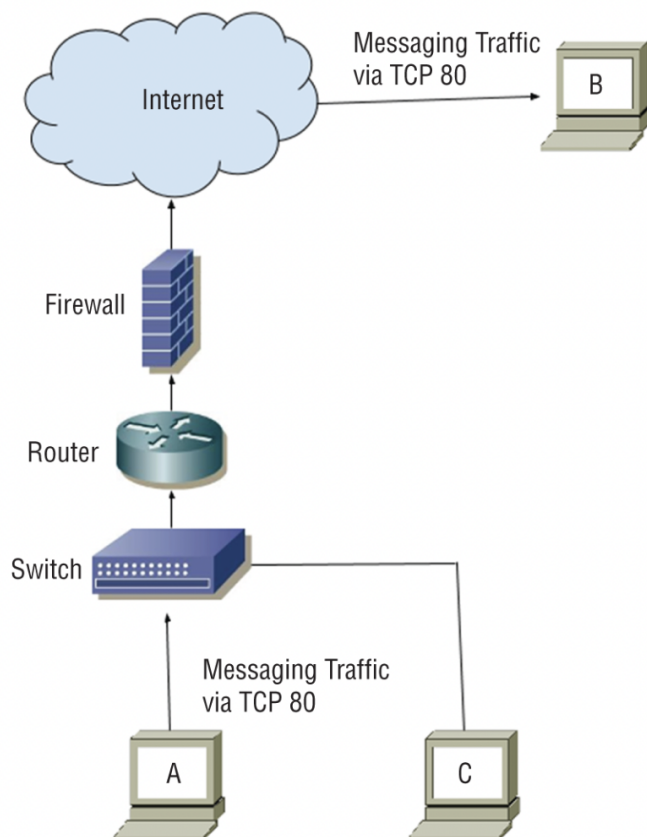
Primjetili bi da smo žrtva TCP connect skena po tome što se najčešće skeniraju servisi slijedno po portovima (1-65536) i po tome što bi stanje umjesto syn_recv bilo ack_recv kada bi gledali kroz IP logove/Wireshark.

Pitanje 21

Točno

Broj bodova: 2,00 od 2,00

Anina organizacija već nekoliko godina koristi popularnu uslugu razmjene poruka. Nedavno se pojavila zabrinutost u vezi s njenim korištenjem.



Koji protokol se najvjerojatnije koristiti za razmjenu poruka između A i B na temelju prikazane slike mreže?

HTTP



Odaberite neistinitu tvrdnju kod razmjene poruka između A i B?

Poruke se razmjenjuju s kriptografskom zaštitom.

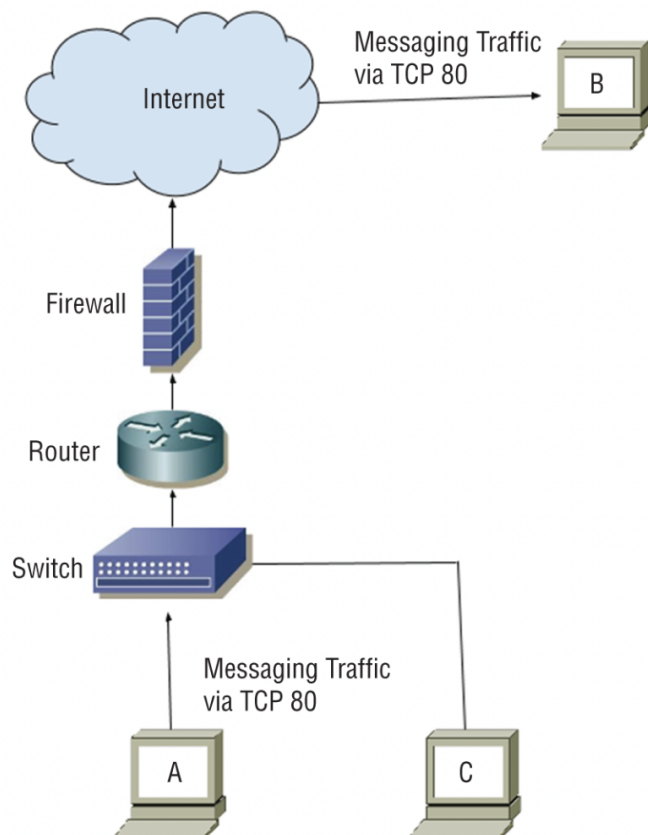


Napomena: netočan odgovor **NE** nosi negativne bodove.

Vaš odgovor je točan.

Ispravan odgovor je:

Anina organizacija već nekoliko godina koristi popularnu uslugu razmjene poruka. Nedavno se pojavila zabrinutost u vezi s njenim korištenjem.



Koji protokol se najvjerojatnije koristiti za razmjenu poruka između A i B na temelju prikazane slike mreže? [HTTP]

Odaberite neistinitu tvrdnju kod razmjene poruka između A i B? [Poruke se razmjenjuju s kriptografskom zaštitom.]

Napomena: netočan odgovor **NE** nosi negativne bodove.

Pitanje 22

Djelomično točno

Broj bodova: 1,50 od 2,00

"The Open Web Application Security Project" (OWASP) objavljuje popis 10 najraširenijih rizika na **mobilnim uređajima**. Povežite rizike s ponuđenim metodama za ublažavanje ili sprječavanje:

Nesigurno spremanje podataka (**Insecure Data Storage**) je rizik koji se ublažava/sprječava



Nedovoljna sigurnost na transportnom sloju (**Insufficient Transport Layer Protection**) je rizik koji se ublažava/sprječava



je rizik koji se ublažava/sprječava implementacijom kontrole pristupa sadržaju prema ulogama korisnika.

Reverzno inženjerstvo (**Reverse Engineering**) je rizik koji se ublažava/sprječava



Napomena: netočan odgovor **NE** nosi negativne bodove.

Vaš odgovor je djelomično točan.

Broj točnih odgovora: 3

Ispravan odgovor je:

"The Open Web Application Security Project" (OWASP) objavljuje popis 10 najraširenijih rizika na **mobilnim uređajima**. Povežite rizike s ponuđenim metodama za ublažavanje ili sprječavanje:

Nesigurno spremanje podataka (**Insecure Data Storage**) je rizik koji se ublažava/sprječava [šifriranjem podataka prije spremanja.]

Nedovoljna sigurnost na transportnom sloju (**Insufficient Transport Layer Protection**) je rizik koji se ublažava/sprječava [korištenjem SSL/TLS-a.]

[Nesigurna Autorizacija (Insecure Authorization)] je rizik koji se ublažava/sprječava implementacijom kontrole pristupa sadržaju prema ulogama korisnika.

Reverzno inženjerstvo (**Reverse Engineering**) je rizik koji se ublažava/sprječava [obfuskacijom koda.]

Napomena: netočan odgovor **NE** nosi negativne bodove.

Pitanje 23

Djelomično točno

Broj bodova: 0,50 od 1,50

Uparite navedene Bluetooth ranjivosti s njihovim opisom.

Napomena: netočan odgovor **NE** nosi negativne bodove.

Blue jacking	Neovlašteni pristup uređaju s Bluetoothom	⊗
Blue snarfing	Korištenje Bluetooth-a kako bi se pratila lokacija žrtve (obično je cilj pametni sat)	⊗
Blue sniping	Proširenje Bluetooth napada većim dometom antene	✓

Vaš odgovor je djelomično točan.

Broj točnih odgovora: 1

Ispravan odgovor je:

Blue jacking → Slanje poruka na uređaj putem Bluetootha,

Blue snarfing → Neovlašteni pristup uređaju s Bluetoothom,

Blue sniping → Proširenje Bluetooth napada većim dometom antene

Pitanje 24

Završeno

Broj bodova od 1,00

Za što se koristi reverzno inženjerstvo kod mobilnih aplikacija?

Reverzno inženjerstvo se koristi kod aplikacija kako bi razumjeli kako one funkcioniraju tj. kako ih se može iskoristiti. Primjer toga je bilo kada se prije par godina moglo ugasiiti tuđi iPhone jednom Whatsapp porukom koju korisnik nije morao ni otvoriti.

Reverziranjem aplikacija i uvidom u njihove dozvole mogu se napraviti izuzetno "dobri" (u kontekstu kvalitete i sofisticiranosti) zero-day napadi.

Pitanje 25

Točno

Broj bodova: 1,00 od 1,00

U kontekstu mobilnih uređaja, kontejnerizacija je:

Napomena: netočan odgovor nosi negativne bodove (-25%).

- ☒ a. Virtualna particija na pokretnom uređaju. ✓
- ☐ b. Stavljanje vlastitog javnog ključa u poseban siguran direktorij (engl. *container*).
- ☐ c. Izolacija segmenta mreže kako bi se moglo pratiti (osiguravati) zaposlenike za vrijeme radnog vremena.
- ☐ d. Ostavljanje pametnog telefona u posudi (engl. *container*) prilikom dolaska na posao da ih zaposlenici ne bi koristili za vrijeme radnog vremena.

Vaš odgovor je točan.

Ispravan odgovor je:

Virtualna particija na pokretnom uređaju.