

sigkom / Završni ispit 2022./2023.



TEST

Završni ispit 2022./2023.

Natrag

Preostalo vrijeme 0:59:34

Pitanje 1

Nije još
odgovoreno

Broj bodova od
1,00

▼ Označi
pitanje

SSH tehnika "jump host" je tehnika u kojoj se ssh veza proslijeđuje na konačno odredište kroz jedan ili više posredničkih poslužitelja. Navedena tehnika radi samo za korisnike koji su "root".

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

- a. Netočno
- b. Točno

Sljedeća stranica

sigkom / Završni ispit 2022./2023.



TEST

Završni ispit 2022./2023.

Natrag

Preostalo vrijeme 0:59:31

Pitanje 2

Nije još odgovorenno

Broj bodova od 1,00

Označi pitanje

Kako svojstvo tajnosti (engl. *confidentiality*) štiti osjetljive informacije?

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

- a. Svojstvo tajnosti osigurava da podaci nisu mijenjani.
- b. Svojstvo tajnosti garantira da se podacima može pristupiti samo nakon procesa autorizacije.
- c. Svojstvo tajnosti sprječava neovlašteno otkrivanje informacija.
- d. Svojstvo tajnosti garantira da su podaci dostupni i pristupačni.

Sljedeća stranica

Prethodna stranica



Završni ispit 2022./2023.

Natrag

Pitanje 3

Nije još odgovoreno

Broj bodova od 2,00

▼ Označi pitanje

Preostalo vrijeme 0:59:30

Ranjivosti koje iskorištavaju tehnologiju Bluetooth nastaju zbog:

Napomena: Više ponuđenih odgovora može biti točno. **Svi** navedeni **odgovori** moraju biti točni kako bi se ostvarili bodovi na ovom zadatku.

- a. Korištenja starih uređaja.
- b. Ne postoje Bluetooth ranjivosti jer se ne koristi IP složaj.
- c. Zbog programerskih grešaka pri rukovanju Bluetooth vezama.
- d. Zbog nestandardiziranosti Bluetooth složaja.

Sljedeća stranica

Prethodna stranica

Pitanje 4

Nije još odgovorenno

Broj bodova od 1,00

Označi pitanje

NAPOMENA: sva pitanja vezana za vatrozid koriste jednaku konfiguraciju i topologiju, a na svako pitanje potrebno je odgovoriti zasebno.

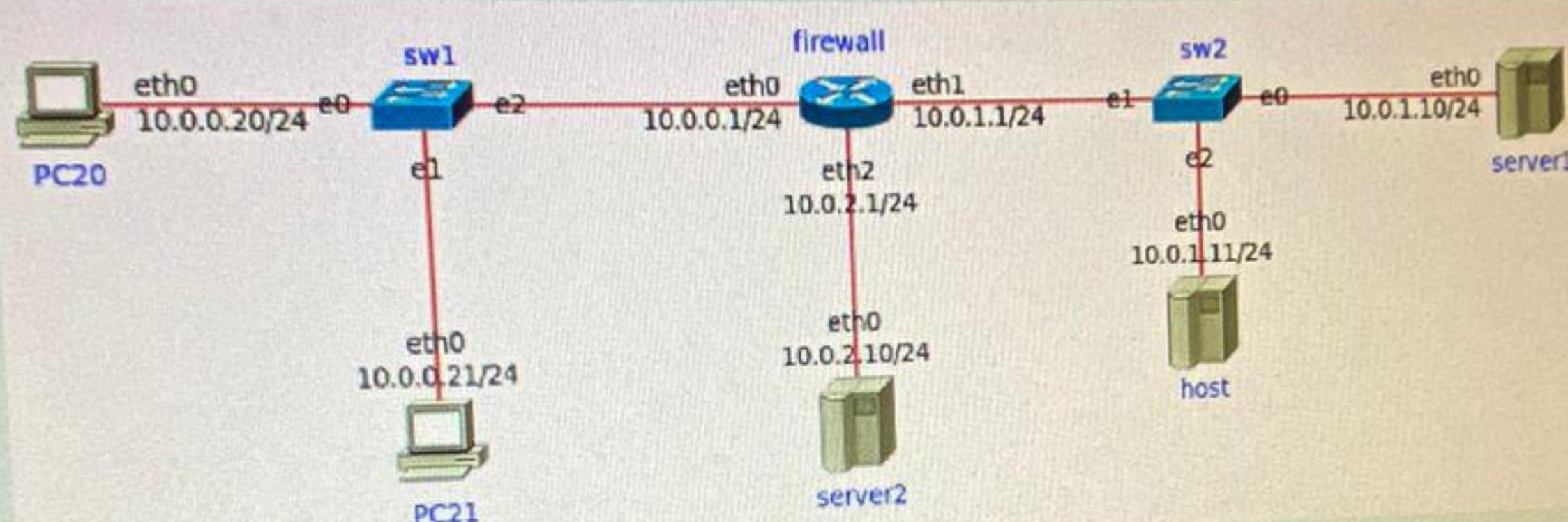
Dana je konfiguracija vatrozida na čvoru *firewall* prikazane topologije

Preostalo vrijeme 0:59:25

```
#!/bin/sh
$cmd="/sbin/iptables"
$cmd -P INPUT DROP
$cmd -P OUTPUT DROP
$cmd -P FORWARD DROP
$cmd -F INPUT
$cmd -F OUTPUT
$cmd -F FORWARD
$cmd -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$cmd -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$cmd -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

$cmd -A FORWARD -p tcp -s 10.0.0.20 -d 10.0.1.10 --dport 22 -j ACCEPT
```

SSH TCP/22
DNS UDP/53
DNS TCP/53
HTTP TCP/80



Odredite pravilo koje je potrebno dodati na kraj konfiguracije da bi se omogućio pristup web poslužitelju na računalu *server2* s bilo koje adrese.

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

- a. \$cmd -A FORWARD -p tcp 80 -s 10.0.2.10 -i eth2 -j ACCEPT
- b. \$cmd -A FORWARD -p tcp -d 10.0.2.10 --dport 80 -j ACCEPT
- c. \$cmd -A FORWARD -p tcp -i eth0 -d 10.0.2.10 --dport 80 -j ACCEPT
- d. \$cmd -A FORWARD -p tcp -i eth0 -o eth2 --dport 80 -j ACCEPT
- e. \$cmd -A FORWARD -p tcp -d 10.0.2.10:80 -j ACCEPT

Sledeća stranica

Prethodna stranica



Pitanje 5Nije još
odgovorenoBroj bodova od
1,00P Označi
pitanje

Preostalo vrijeme 0:59:16

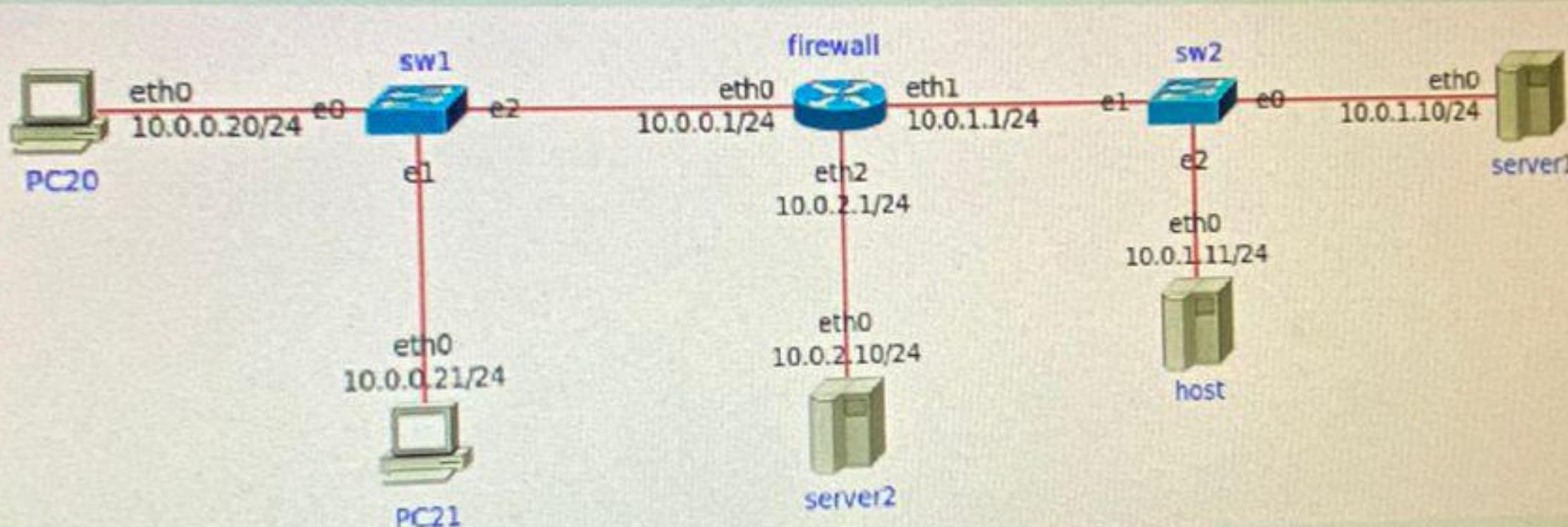
NAPOMENA: sva pitanja vezana za vatrozid koriste jednaku konfiguraciju i topologiju, a na svako pitanje potrebno je odgovoriti zasebno.

Dana je konfiguracija vatrozida na čvoru *firewall* prikazane topologije:

```
#!/bin/sh
cmd="/sbin/iptables"
$cmd -P INPUT DROP
$cmd -P OUTPUT DROP
$cmd -P FORWARD DROP
$cmd -F INPUT
$cmd -F OUTPUT
$cmd -F FORWARD
$cmd -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$cmd -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$cmd -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

$cmd -A FORWARD -p tcp -s 10.0.0.20 -d 10.0.1.10 --dport 22 -j ACCEPT
```

SSH TCP/22
DNS UDP/53
DNS TCP/53
HTTP TCP/80



Odredite pravilo koje je potrebno dodati na kraj konfiguracije da bi se omogućilo računalu *server1* da nespojnim transportnim protokolom može slati upite domenskom poslužitelju na računalu *server2*.

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

- a. \$cmd -A FORWARD -p tcp -s 10.0.1.10 -d 10.0.2.10 --dport 80 -j ACCEPT
- b. \$cmd -A FORWARD -p udp -s 10.0.1.10 -d 10.0.2.10 --dport 53 -j ACCEPT
- c. \$cmd -A FORWARD -p tcp 80 -s 10.0.1.10 -d 10.0.2.10 -j ACCEPT
- d. \$cmd -A OUTPUT -p udp -d 10.0.2.10 --dport 53 -j ACCEPT



TEST

Završni ispit 2022./2023.

[Natrag](#)**Pitanje 6**

Nije još odgovoreno

Broj bodova od 1,00

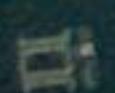
▼ Označi pitanje

Preostalo vrijeme 0:59:13

Pegasus je:

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

- a. Skup ranjivosti i iskorištavanja (exploit) namijenjen operacijskom sustavu Windows.
- b. Skup ranjivosti i iskorištavanja (exploit) namijenjen operacijskom sustavu Symbian.
- c. Skup ranjivosti i iskorištavanja (exploit) namijenjen operacijskom sustavu Apple iOS.
- d. Skup ranjivosti i iskorištavanja (exploit) namijenjen operacijskom sustavu Linux.

[Prethodna stranica](#)[Sljedeća stranica](#)

LG

TEST

Završni ispit 2022./2023.

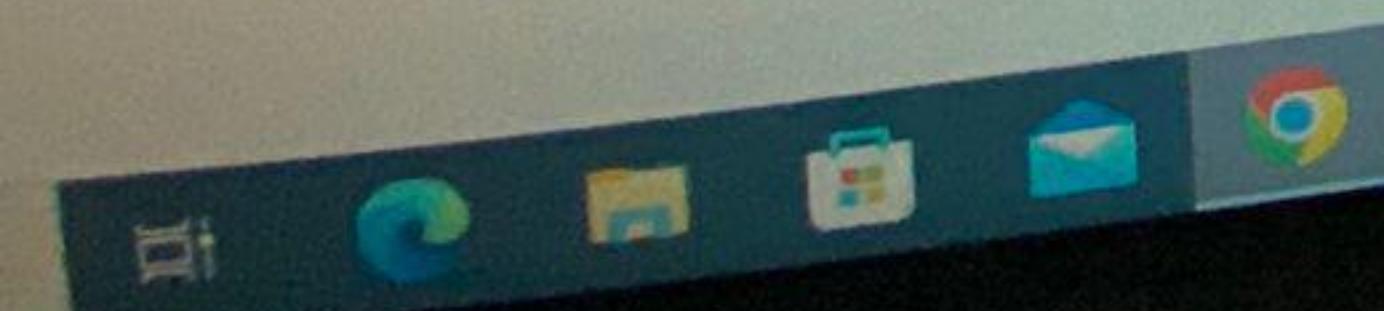
[Natrag](#)**Pitanje 7**Nije još
odgovorenoBroj bodova od
1,00 Označi
pitanje

Preostalo vrijeme 0:59:12

U kontekstu mobilnih uređaja, kontejnerizacija je:

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

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

[Prethodna stranica](#)[Sljedeća stranica](#)

TEST

Završni ispit 2022./2023.

[Natrag](#)**Pitanje 8**

Nije još odgovoreno

Broj bodova od 3,00

 Označi pitanje

Preostalo vrijeme 0:59:08

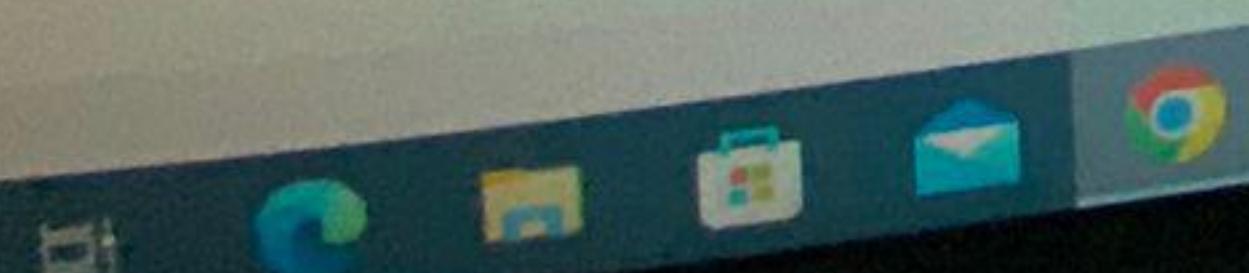
ISPIS #1: netstat -ant

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	0.0.0.0:80	0.0.0.0:*	LISTEN
tcp	0	0	83.129.34.99:80	162.83.43.137:40136	SYN_RECV
...					
tcp	0	0	83.129.34.99:80	162.83.43.179:40432	SYN_RECV
tcp	0	0	83.129.34.99:80	162.83.43.59:40058	SYN_RECV
tcp	0	0	83.129.34.99:80	162.83.43.69:40322	SYN_RECV

Prikazan je ispis naredbe netstat na napadnutom računalu. Koji napad izvodi napadač, a vidljiv je u ispisu #1?

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

- a. UDP reflection napad
- b. SYN-ACK flood
- c. SYN flood
- d. UDP flood
- e. TCP SYN scan

[Sljedeća stranica](#)[Prethodna stranica](#)

LG

sigkom / Završni ispit 2022./2023.

TEST

Završni ispit 2022./2023.

Natrag

Pitanje 9
Nije još odgovoreno
Broj bodova od 3,00
Označi pitanje

Preostalo vrijeme 0:59:03

Povežite funkcije MIME ekstenzije električne pošte s njihovim opisima:

- enveloped-data
- signed-data
- clear-signed-data

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

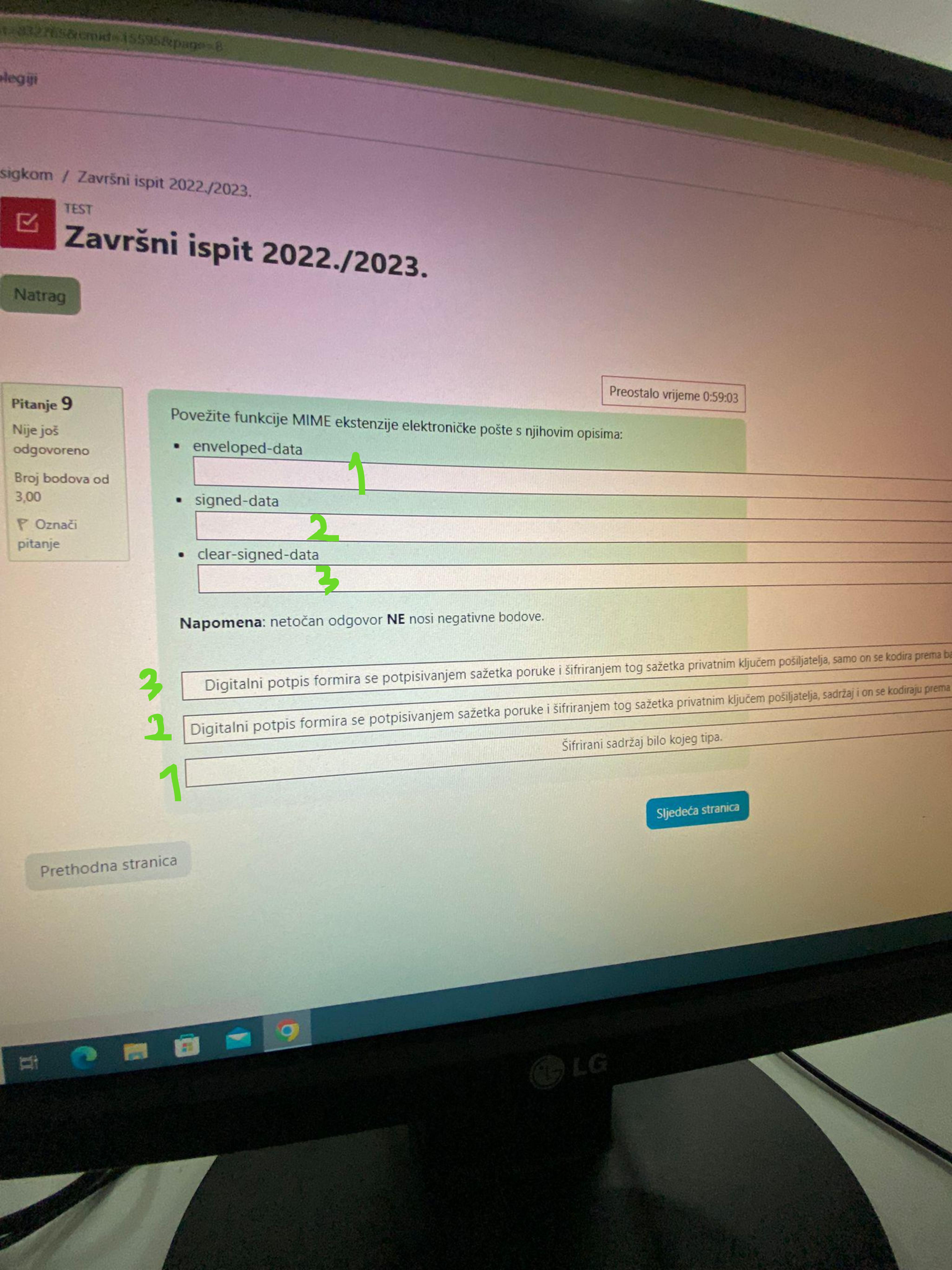
3 Digitalni potpis formira se potpisivanjem sažetka poruke i šifriranjem tog sažetka privatnim ključem pošiljatelja, samo on se kodira prema

1 Digitalni potpis formira se potpisivanjem sažetka poruke i šifriranjem tog sažetka privatnim ključem pošiljatelja, sadržaj i on se kodiraju prema

1 Šifrirani sadržaj bilo kojeg tipa.

Sljedeća stranica

Prethodna stranica



sigkom / Završni ispit 2022./2023.



TEST

Završni ispit 2022./2023.

Natrag

Pitanje 10

Nije još
odgovoreno

Broj bodova od
1,00

Označi
pitanje

Preostalo vrijeme 0:58:58

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

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

- a. Netočno
- b. Točno

Prethodna stranica

Sljedeća stranica



Završni ispit 2022./2023.

Natrag

Pitanje 11

Nije još odgovoren

Broj bodova od 1,00

Označi pitanje

Preostalo vrijeme 0:58:56

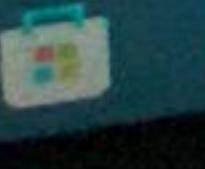
NAT otežava "hakiranje" klijenata od napadača i ako je napadač unutar iste lokalne mreže kao i klijenti.

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

- a. Netočno
- b. Točno

Prethodna stranica

Sljedeća stranica



LG



TEST

Završni ispit 2022./2023.

[Natrag](#)**Pitanje 12**

Nije još odgovoreno

Broj bodova od 1,00

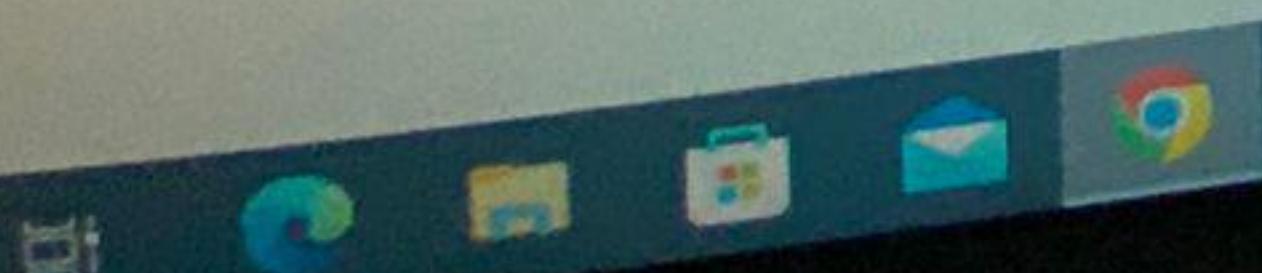
Označi pitanje

Preostalo vrijeme 0:58:55

Koja je primarna svrha mrežnog sustava za detekciju upada (engl. *Network Intrusion Detection System - NIDS*)?

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

- a. Šifrirati osjetljive podatke kako bi ih se zaštitilo od neautoriziranog pristupa.
- b. Sprječiti sve vrste napada i upada.
- c. Pratiti mrežni promet i detektirati potencijalne sigurnosne incidente.
- d. Detektirati i ublažiti/pokrpati (engl. *mitigate*) sve ranjivosti u mreži.

[Sljedeća stranica](#)[Prethodna stranica](#)

Pitanje 13

Nije još
odgovoren

Broj bodova od
1,00

¶ Označi
pitanje

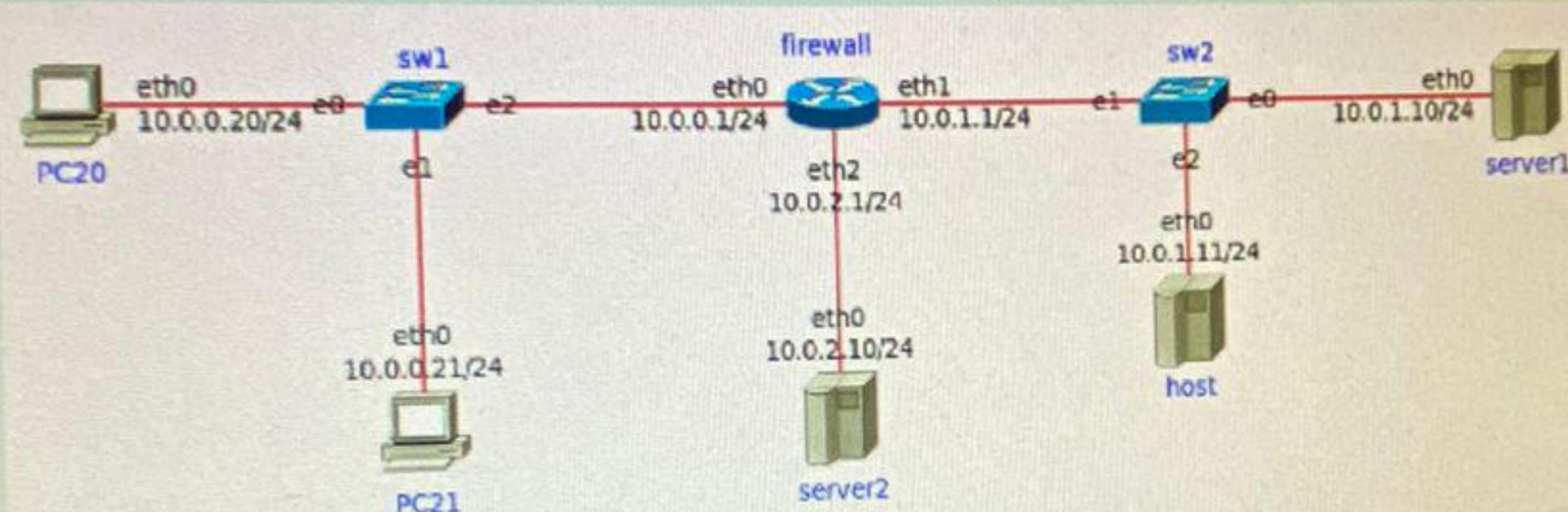
Preostalo vrijeme 0:58:43

NAPOMENA: sva pitanja vezana za vatrozid koriste jednaku konfiguraciju i topologiju, a na svako pitanje potrebno je odgovoriti zasebno.

Dana je konfiguracija vatrozida na čvoru *firewall* prikazane topologije:

```
#! /bin/sh
$cmd="/sbin/iptables"
$cmd -P INPUT DROP
$cmd -P OUTPUT DROP
$cmd -P FORWARD DROP
$cmd -F INPUT
$cmd -F OUTPUT
$cmd -F FORWARD
$cmd -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$cmd -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$cmd -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
$cmd -A FORWARD -p tcp -s 10.0.0.20 -d 10.0.1.10 --dport 22 -j ACCEPT
```

SSH TCP/22
DNS UDP/53
DNS TCP/53
HTTP TCP/80



Odredite pravilo koje je potrebno dodati na kraj konfiguracije da bi se zaštitilo računalo *server2* od „IP spoofing“ napada iz javne mreže (javna mreža je sa strane sučelja *eth0*).

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

- a. \$cmd -A FORWARD -s 10.0.1.0/24 -i eth0 -j DROP
- b. \$cmd -A FORWARD -d 10.0.1.0/24 -i eth0 -o eth2 -j DROP
- c. \$cmd -A FORWARD -d 10.0.1.0/24 -i eth0 -j DROP
- d. \$cmd -A INPUT -s 10.0.1.0/24 -i eth0 -o eth1 -j DROP
- e. \$cmd -A OUTPUT -s 10.0.1.0/24 -i eth1 -j DROP



Završni ispit 2022./2023.

Natrag

Pitanje 14

Nije još
odgovoreno

Broj bodova od
1,00

Označi
pitanje

Preostalo vrijeme 0:58:41

525 419.593881@127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR) System Information Type 2
527 419.597698@127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (SS)
529 419.656705@127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR) Paging Request Type 3
531 419.659437@127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR) Immediate Assignment
533 419.663366@127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR) Paging Request Type 3
535 419.722105@127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR) Paging Request Type 3
537 419.727733@127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR) Immediate Assignment
539 419.731985@127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR) Paging Request Type 2
541 419.789597@127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR) Paging Request Type 1
543 419.792826@127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR) Paging Request Type 1
545 419.854953@127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR) System Information Type 3
547 419.860646@127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (SS)
549 419.867761@127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR) Paging Request Type 3
551 419.925362@127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR) Paging Request Type 1
553 420.324152@127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (SS)
555 420.516427@127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR) System Information Type 2ter
557 421.236176@127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR) Immediate Assignment
559 421.365709@127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR) Paging Request Type 3

Alatom Wireshark prikupili ste podatke iz mobilne mreže kao na slici. Koja poruka vas zanima ako želite informacije o prebacivanju na drugi, potencijalno sigurniji, kanal?

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

- a. Paging request Type 1
- b. Cipher mode command
- c. Ništa od navedenog
- d. Immediate assignment
- e. Paging request Type 3

Sjedeća stranica

Prethodna stranica



TEST

Završni ispit 2022./2023.

Natrag

Pitanje 16

Nije još
odgovoren

Broj bodova od
1,00

▼ Označi
pitanje

Preostalo vrijeme 0:58:31

S/MIME podržava šifriranje s kraja na kraj.

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



- a. Točno
- b. Netočno

Prethodna stranica

Sljedeća stranica

Pitanje 18

Nije još
odgovoreno

Broj bodova od
1,00

F Označ
pitanje

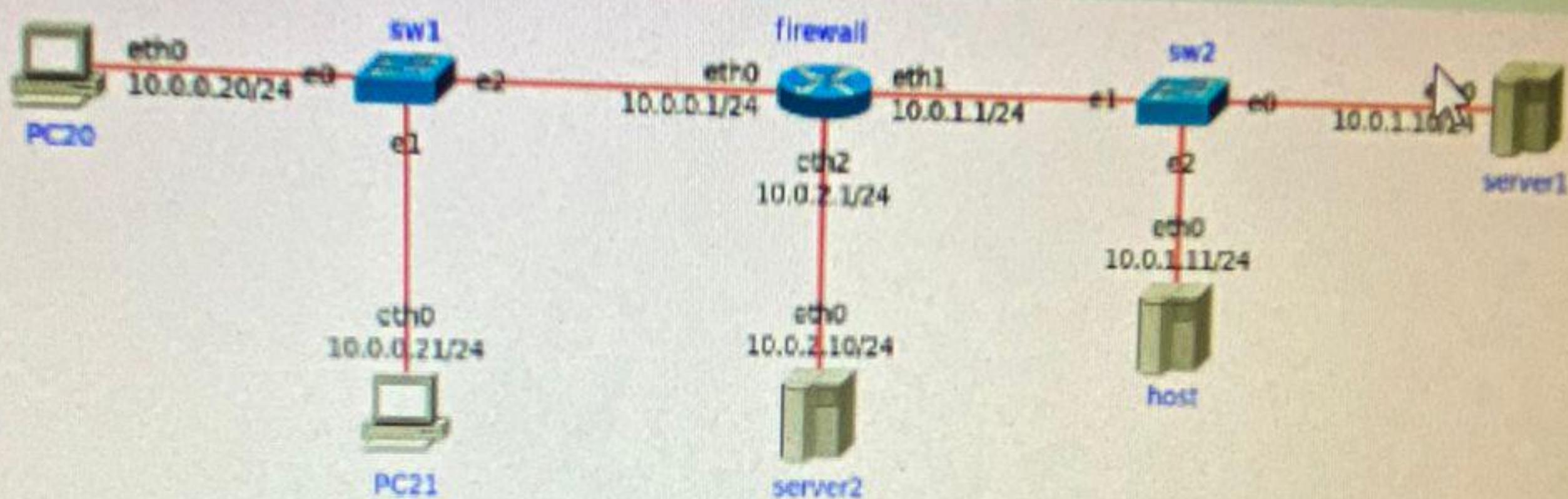
Preostalo vrijeme 0:58:24

NAPOMENA: sva pitanja vezana za vatrozid koriste jednaku konfiguraciju i topologiju, a na svako pitanje potrebno je odgovoriti zasebno.

Dana je konfiguracija vatrozida na čvoru *firewall* prikazane topologije:

```
#!/bin/sh
$cmd="/sbin/iptables"
$cmd -P INPUT DROP
$cmd -P OUTPUT DROP
$cmd -P FORWARD DROP
$cmd -F INPUT
$cmd -F OUTPUT
$cmd -F FORWARD
$cmd -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$cmd -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$cmd -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
$cmd -A FORWARD -p tcp -s 10.0.0.20 -d 10.0.1.10 --dport 22 -j ACCEPT
```

SSH TCP/22
DNS UDP/53
DNS TCP/53
HTTP TCP/80



Odredite pravilo koje je potrebno dodati na kraj konfiguracije da bi se omogućio ping računala *server2* isključivao s računalom *PC20*.

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

- a. \$cmd -A FORWARD -p icmp -s 10.0.0.20 -d 10.0.2.10 -j ACCEPT
- b. \$cmd -A OUTPUT -p icmp -s 10.0.0.20 -i eth2 -j ACCEPT
- c. \$cmd -A FORWARD -p ping -s 10.0.0.20 -i eth2 -j ACCEPT
- d. \$cmd -A OUTPUT -p ping -s 10.0.0.20 -d 10.0.2.10 -j ACCEPT
- e. \$cmd -A FORWARD -p icmp -i eth0 -o eth2 -d 10.0.2.10 -j ACCEPT

Sjedeća stranica

Prethodna stranica



Završni ispit 2022./2023.

Natrag

Preostalo vrijeme 0:58:22

Pitanje 19

Nije još
odgovoreno

Broj bodova od
1,00

Označi
pitanje

Koje podatke mreža čuva o korisnicima?

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

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

Prethodna stranica

Slijedeća stranica

Završni ispit 2022./2023.

Natrag

Preostalo vrijeme 0:58:22

Pitanje 19

Nije još
odgovoreno

Broj bodova od
1,00

Označi
pitanje

Koje podatke mreža čuva o korisnicima?

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

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

Prethodna stranica

Slijedeća stranica

Završni ispit 2022./2023.

Prethodna

Pitanje 20

Nije još odgovoreno

Broj bodova od 1,00

Označi pitanje

Preostalo vrijeme 0:58:19

Ana je osmisnila sigurnosni mehanizam koji uključuje korištenje lažnih vjerodajnica za prijavu zaposlenika. Kako su vjerodajnice izmišljene, nikada se ne bi trebale koristiti u stvarnom sustavu. Anin sustav prati upisane vjerodajnice od strane zaposlenika i ako utvrdi da su vjerodajnice jednake lažnim generira sigurnosni alarm.

Kojem sigurnosnom mehanizmu je Anin mehanizam najsličniji?

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

- a. Honeypotu
- b. Sustavu za prevenciju napada
- c. Dvofaktorskoj autentikaciji
- d. Vatrozidu

Sljedeća stranica

Prethodna stranica

ZAVRŠNI ISPIT ZVJEZD./ZVJEZD.**Natrag**

Preostalo vrijeme 0:58:14

Pitanje 21

Nije još odgovoreno

Broj bodova od 1,00

F Označiti pitanje

Potrebna radnja: Upozorenje korisnickoj podrsci | 6/6/2023

Poruka je prepoznata kao bezvrijedna. Izbrisati ćemo je nakon 25 dana.

Zadržavanje Junk Email (30 dana) Istječe: pet. 6.7.2023. 9:38

FN

Fer-Automated Notification <andrew.leece@acenet.co.za>

Primatelj: sui



Fer Obavijest sustava

Vaša sui@fer.hr lozinka za pristup ističe danas 6/6/2023.

Upotrijebite TAB ispod kako biste nastavili koristiti svoju trenutnu lozinku.

[Zadrži Moju Lozinku](#)

NAPOMENA: Vaš će pristup biti zaključan nakon 48 sati.

Fer Tim za poštu

Please consider the environment before printing this email.

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

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

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



Završni ispit 2022./2023.

Natrag

Preostalo vrijeme 0:58:12

Pitanje 22

Nije još
odgovoreno

Broj bodova od
1,00

Označi
pitanje

DMZ je skraćenica za:

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

- a. Demilitarized Militarized Zone - sigurno područje mreže između dva filtera paketa koje je pod napadom
- b. Demilitarized Zone - područje mreže između dva filtera paketa
- c. Destabilized Military Zone - područje mreže koje nije sigurno jer je u njemu detektiran napad
- d. Distributed Militarized Zone - područje mreže s raspodijeljenim servisima koji detektiraju napade

Prethodna stranica

Sljedeća stranica





Završni ispit 2022./2023.

Preostalo vrijeme 0:58:11

Pitanje 23

Nije još
odgovoreno

Broj bodova od
3,00

1^o Označi
pitanje

Ako pristigla elektronička pošta ne prolazi SPF ili **DKIM** ¹ provjeru pošiljatelja,

konštenjem **DMARC** ² protokola možemo ju poslati u *spam direktorij mail sandučića*.

1 - engl. skraćenica

2 - engl. skraćenica

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

Prethodna stranica

Sljedeća stranica

Završni ispit 2022./2023.

Natrag

Preostalo vrijeme 0:58:07

Pitanje 24

Nije još
odgovoren

Broj bodova od
1,00

Označi
pitanje

Extended Simple Mail Transfer Protocol (ESMTP) sadrži sigurnosne mehanizme.

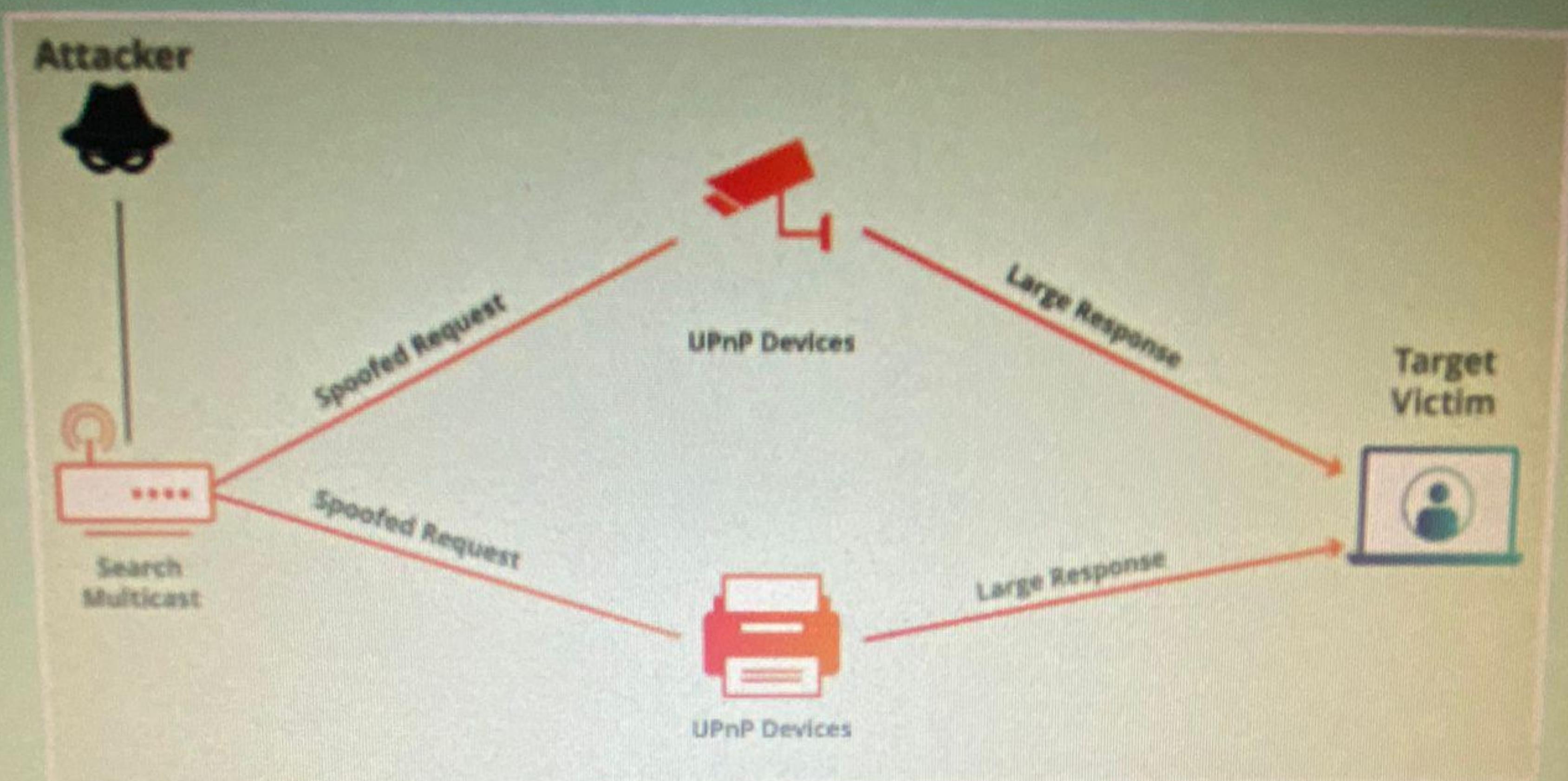
Napomena: netočan odgovor nosi negativne bodove (-50%).

- a. Točno
- b. Netočno

Prethodna stranica

Sljedeća stranica

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



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



Završni ispit 2022./2023.

Patreći

anje 26

e još

govoreno

oj bodova od

10

Označi
ranje

Preostalo vrijeme 0:57:58

Na koji se način provodila kompromitacija IoT uređaja kod tzv. Mirai Botnet-a?

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

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

Prethodna stranica

Sljedeća stranica

Završni ispit 2022./2023.

Preostalo vrijeme 0:57:54

Pomažete CIP-u osigurati poslužitelj koji poslužuje stranicu www.fer.unizg.hr. Iz CIP-a Vam govore kako su uočili da napadači često za metu napada imaju SSH poslužitelj. Kako biste ga zaštitili, uređujete datoteku `/etc/ssh/sshd_config`. Uočavate sljedeće linije u datoteci:

PasswordAuthentication

- no (iako je lozinka najsigurniji način prijave, nesigurno se pohranjuje na poslužitelju)
- no (iako je lozinka najsigurniji način prijave, prilikom postupka prijave uočljiva je u obliku čistog teksta)
- yes (jer se korisnik mora moći prijaviti)
- yes (jer će korisnik imati lozinku koju je teže pogoditi od ključa)
- yes (jer je lozinka najsigurniji način prijave zbog toga što nigdje nije pohranjena u obliku čistog teksta)
- no (postoje sigurniji načini prijave)

Port

Na koje vrijednosti ćete postaviti **svaku** od navedenih opcija kako biste poboljšali sigurnost

SSH poslužitelja?

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

Sjedeća stranica

Završni ispit 2022./2023.

strag

je 27

jaš

zvorenio

bodova od

znači

je

Preostalo vrijeme 0:57:51

Pomažete CIP-u osigurati poslužitelj koji poslužuje stranicu www.fer.unizg.hr. Iz CIP-a Vam govore kako su uočili da napadači često za metu napada imaju SSH poslužitelj. Kako biste ga zaštitili, uređujete datoteku `/etc/ssh/sshd_config`. Uočavate sljedeće linije u datoteci:

PasswordAuthentication

PubkeyAuthentication

- yes (ali samo ključevi dobiveni algoritmom RSA-256)
- no (ključ je malen i u prosjeku kraći od lozinke a samim time i nesigurniji)
- no (ključevi su pohranjeni u obliku čistog teksta i kao takvi su nesigurni)
- no (generirani ključ može imati jako malu entropiju a samim time može biti jako nesiguran)
- yes (ključevi su sigurniji od lozinki)
- no (PrivkeyAuthentication je sigurniji jer koristi privatni ključ)
- yes (ali samo ako su dijelovi privatnog ključa pohranjeni na više lokacija radi pojačane sigurnosti)
- no (ključevi su jako nesigurni obzirom da se nalaze kod korisnika)

SSH poslužitelja?

Napomena: netočan odgovor NE nosi negativne bodove.

Sljedeća stranica

thodna stranica

Završni ispit 2022./2023.

Preostalo vrijeme 0:57:50

Pomažete CIP-u osigurati poslužitelj koji poslužuje stranicu www.fer.unizg.hr. Iz CIP-a Vam govore kako su uočili da napadači često za metu napada imaju SSH poslužitelj. Kako biste ga zaštitali, uređujete datoteku `/etc/ssh/sshd_config`. Uočavate sljedeće linije u datoteci:

`PasswordAuthentication`

`PubkeyAuthentication`

`PermitRootLogin`

- yes (korisnika root štiti jezgra operacijskog sustava)
- no (jer korisnik root ima najveće ovlasti na operacijskom sustavu)
- yes (nije bitno koji je korisnik ako koristimo sigurne metode autentifikacije)
- no (iako korisnika root štiti jezgra operacijskog sustava ova opcija predstavlja dodatnu razinu sigurnosti)
- yes (korisnik root je nebitan dok god napadač ne provali u profil stvarnog korisnika)
- no (iako je korisnik root nebitan moramo smanjiti vektor napada napadaču)
- yes (ako korisnik root ne postoji)

Sjedeća stranica

Završni ispit 2022./2023.

Preostalo vrijeme 0:57:48

Pomažete CIP-u osigurati poslužitelj koji poslužuje stranicu www.fer.unizg.hr. Iz CIP-a Vam govore kako su uočili da napadači često za metu napada imaju SSH poslužitelj. Kako biste ga zaštitili, uređujete datoteku `/etc/ssh/sshd_config`. Uočavate sljedeće linije u datoteci:

PasswordAuthentication

PubkeyAuthentication

PermitRootLogin

Port

- 0 (operacijski sustav odabrat će prvi slobodni port koji će koristiti, ovakvo dodijeljivanje porta je pseudoslučajno i samim time sigurno)
443 (jer je na portu 443 https poslužitelj koji koristi protokol SSL/TLS)
C 64223 (jer ćemo tako samo mi znati da poslužitelj sluša na tom portu)
80 (operacijski sustav zna da je na portu 80 http poslužitelj pa želimo iskoristiti njegovu zaštitu)
66832 (jer je navedeni port van raspona mogućih portova, pa je sigurniji za korištenje)
22 (operacijski sustav zna da je na portu 22 ssh poslužitelj pa će ga zaštiti)

Sljedeća stranica





TEST

Završni ispit 2022./2023.

Natrag

Pitanje 28

Nije još
odgovoreno

Broj bodova od
2,00

Označi
pitanje

Preostalo vrijeme 0:57:44

Povežite pojmove s objašnjenjima:

1 je uređaj koji se smješta između privatne mreže i Interneta i mora biti "bastion host".

2 je uređaj koji je kritična ali dobro osigurana točka u mreži.

3 je uređaj koji obavlja usmjeravanje uz mogućnost neke vrste filtriranja paketa

U 4 sav promet iz javne mreže "screening router" propušta samo do "bastion hosta" smještenog u privatnoj mreži.

Napomena: netočan odgovor NE nosi negativne bodove.

1 Dual Homed Gateway

2 Screened Subnet

3 Screening router

Demilitarized Zone

4 Bastion host

Screened Host Gateway

1

3

4

Sljedeća stranica

Prethodna stranica

Završni ispit 2022./2023.

Natrag

Pitanje 29

Nije još
odgovoreno

Broj bodova od
1,00

Označi
pitanje

Koja je tvrdnja točna?

Preostalo vrijeme 0:57:42

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

- a. Kod mobilnih mreža druge generacije (GSM), algoritam A5 koristi se za autentifikaciju bazne stanice.
- b. Kod mobilnih mreža druge generacije (GSM), algoritam A3 koristi se za autentifikaciju bazne stanice.
- c. Kod mobilnih mreža druge generacije (GSM), algoritam A8 koristi se za autentifikaciju bazne stanice.
- d. Niti jedna.

Prethodna stranica

Sljedeća stranica

Završni ispit 2022./2023.

Natrag

Pitanje 30

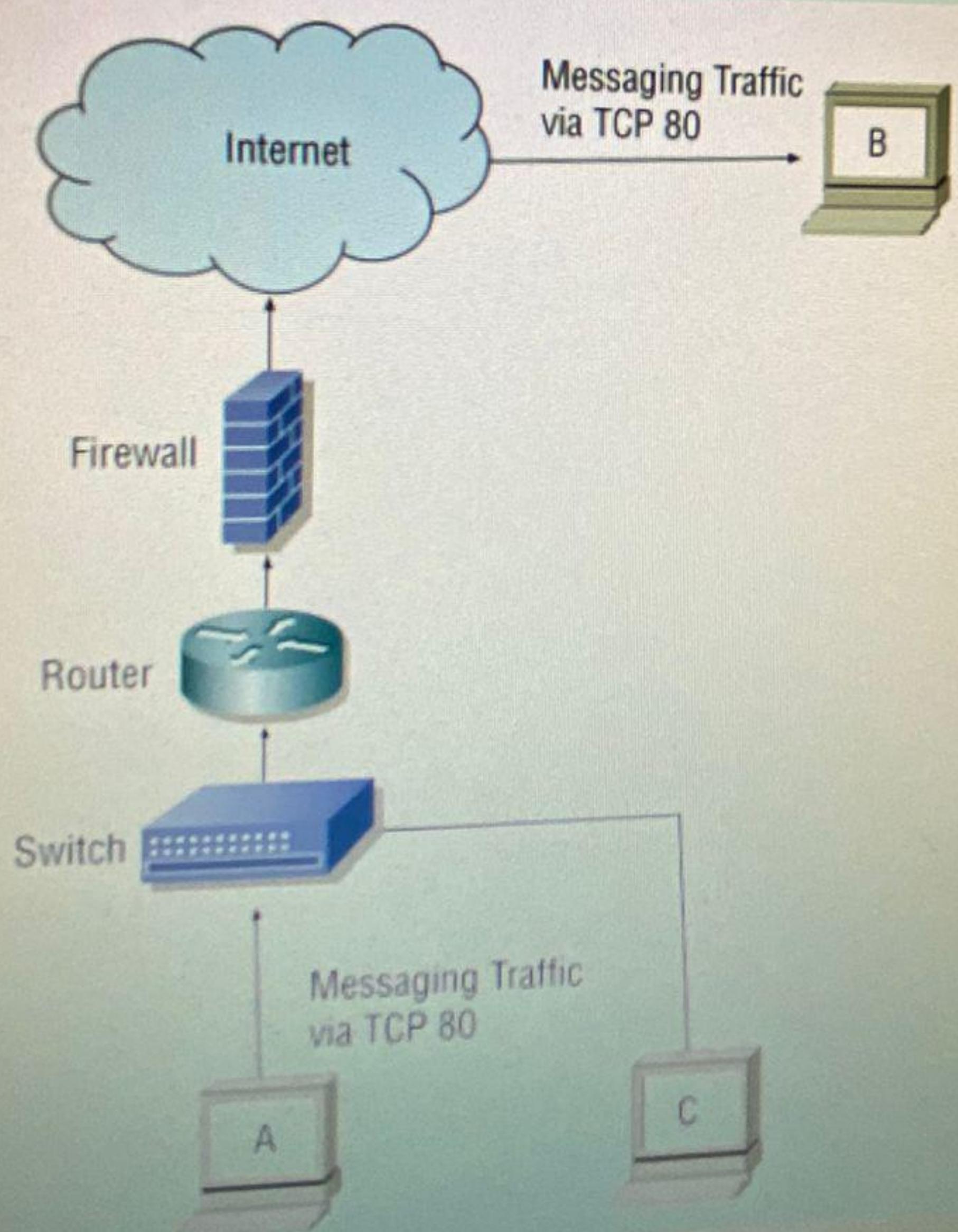
Nije još odgovorenno

Broj bodova od 1,00

Označi pitanje

Preostalo vrijeme 0:57:40

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?

= 80

Odaberite neistinu tvrdnju da razmjenjene poruke između A i B su razmjenjuju se kriptografskom zastitu

Preostalo vrijeme 0:57:31

Materijal 31

Nije još
odgovorenBroj bodova od
1,00Oznaka
pitanje

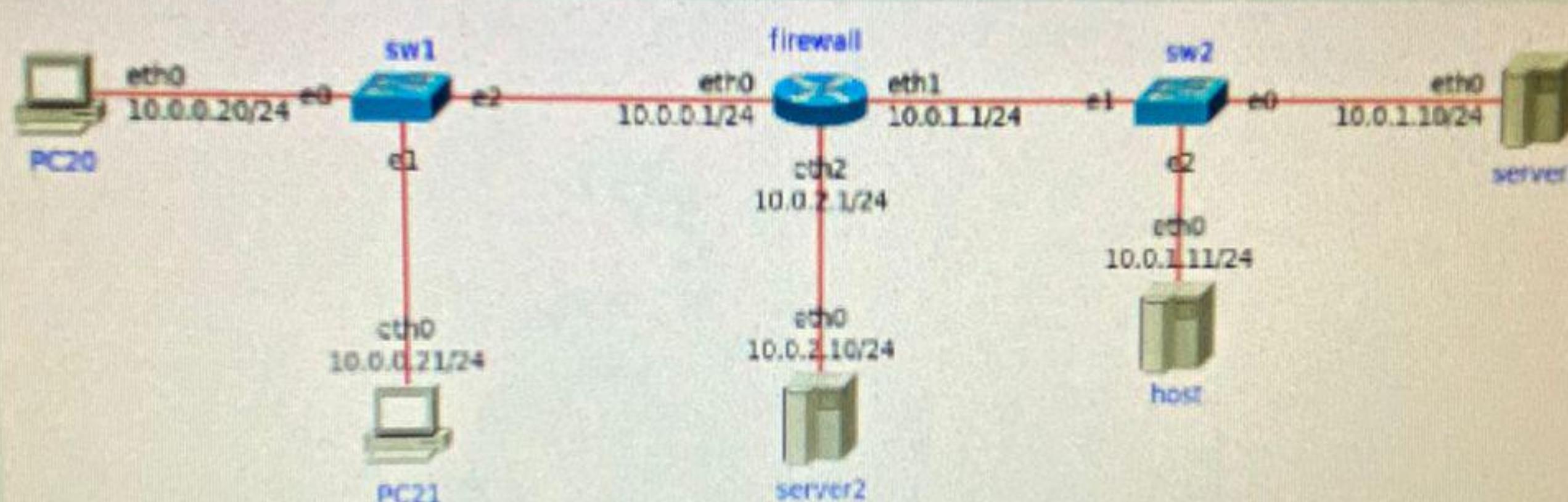
NAPOMENA: sva pitanja vezana za vatrozid koriste jednaku konfiguraciju i topologiju, a na svako pitanje potrebno je odgovoriti zasebno.

Dana je konfiguracija vatrozida na čvoru *firewall* prikazane topologije:

```
#!/bin/sh
$cmd -P INPUT DROP
$cmd -P OUTPUT DROP
$cmd -P FORWARD DROP
$cmd -F INPUT
$cmd -F OUTPUT
$cmd -F FORWARD
$cmd -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$cmd -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$cmd -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

$cmd -A FORWARD -p tcp -s 10.0.0.20 -d 10.0.1.10 --dport 22 -j ACCEPT
```

SSH TCP/22
DNS UDP/53
DNS TCP/53
HTTP TCP/80



Odredite pravilo koje je potrebno dodati na kraj konfiguracije da bi se omogućio pristup vatrozidu (*firewall*) korištenjem protokola SSH s računala *PC21*.

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

- a. \$cmd -A FORWARD -p tcp -s 10.0.0.21 --dport 22 -j ACCEPT
- b. \$cmd -A FORWARD -p tcp 22 -s 10.0.0.21 -d 10.0.0.1 -j ACCEPT
- c. \$cmd -A INPUT -p tcp -s 10.0.0.21 -d 10.0.0.1 --dport 22 -j ACCEPT
- d. \$cmd -A FORWARD -p tcp -s 10.0.0.21 -d 10.0.0.1 --dport 22 -j ACCEPT
- e. \$cmd -A INPUT -p tcp 22 -s 10.0.0.21 -j ACCEPT

Završi test...

Prethodna stranica

Pitanje 10

Nije još odgovoren

Broj bodova od
2,50

V. Oznaci pitanje

"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 je rizik koji se ublažava/sprječava promjenom sklopovja ili pojedinih elemenata sklopovja na uređaju.
- 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)

Nesigurna sučelja (Insecure Ecosystem Interfaces)

Nesigurne mrežne usluge (Insecure Network Services)

Loša privatnost (Insufficient Privacy Protection)

Nesigurni mehanizmi nadogradnji (Lack of Secure Update Mechanism)

Nedostatak upravljanja (Lack of Device Management)

Fizička sigurnost (Lack of Physical Hardening)

Nedovoljno štitranje (Insecure Data Transfer and Storage)

Zastarjele komponente (Use of Insecure or Outdated Components)

Loše početne postavke (Insecure Default Settings)

popisivanjem uređaja i njihovih lokacija te čestim provjerama.

gašenjem nepotrebnih servisa, ažuriranje servisa na najnoviju verziju.

uključivanjem anonimizacije podataka.

promjenom sklopovja ili pojedinih elemenata sklopovja na uređaju.

šifriranjem kanala za ažuriranje firmwarea.

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

zaključavanjem prostorije u kojoj se nalazi uređaj.

ispravnim korištenjem infrastrukture PKI.



Pitanje 22Nije još
odgovorenBroj bodova od:
2,501* Oznaci
pitanje

"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

koristenjem SSL/TLS

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

obuskfacija koda

Napomena: netočan odgovor NE nosi negativne bodove.

 Loša kvaliteta koda u klijentu (Client Code Quality)

Neispravno korištenje platforme (Improper Platform Usage)

Dodatne neželjene funkcionalnosti (Extraneous Functionality)

Nedovoljna razina kriptografije (Insufficient Cryptography)

Nesigurna autentifikacija (Insecure Authentication)

Neovlašteno mijenjanje koda (Code Tampering)

Nesigurna Autorizacija (Insecure Authorization)

Reverzno inženjerstvo (Reverse Engineering)

Nesigurna komunikacija (Insecure Communication)

Nesigurno spremanje podataka (Insecure Data Storage)

šifriranjem podataka prije spremanja.

korištenjem SSL/TLS-a.

ispravnim korištenje sigurnosnih značajki operacijskog sustava.

micanjem korisničkih podataka iz dnevničkih zapisa (logova).

korištenjem zaštitnih suma.

implementacijom validacije podataka dobivenih od korisnika.

implementacijom kontrole pristupa sadržaju prema ulogama korisnika.

implementacijom dvofaktorske autentifikacije (Two-factor Authentication).

