

Naslovnica Moja naslovnica Moji e-kolegiji

Nije još odgovoreno
Broj bodova od 3,00
Označi pitanje

Preostalo vrijeme 1:29:01

Koristeći prikazanu topologiju, ispunite konfiguraciju VPN-a korištenjem alata IPsec s dijeljenim ključem.

Čvor	:	r1
Local IP address:	:	10.0.1.1/24
Local subnet:	:	10.0.0.0/24
Peers IP address:	:	10.0.3.1/24

Čvor	:	r2
Local IP address:	:	10.0.3.1
Local subnet:	:	10.0.2.0/24
Peers IP address:	:	10.0.1.1/24

Napomena: netočan odgovor NE nosi negativne bodove.

Type here to search

sigkom / Međuispit 2022./2023.



TEST

Međuispit 2022./2023.

Natrag

Preostalo vrijeme 1:29:09

Pitanje 11

Nije još
odgovoreno

Broj bodova od
1,00

▼ Označi
pitanje

Na slici je prikazan paket snimljen nakon postavljanja GRE tunela. Koji dio paketa je enkapsuliran?

```
> Frame 15: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface -, id 0
> Ethernet II, Src: 42:00:aa:00:00:03 (42:00:aa:00:00:03), Dst: 42:00:aa:00:00:02 (42:00:aa:00:00:02)
> Internet Protocol Version 4, Src: 10.0.0.20, Dst: 10.0.3.10
> Generic Routing Encapsulation (IP)
Internet Protocol Version 4, Src: 11.11.11.1, Dst: 11.11.11.2
Internet Control Message Protocol
```

Napomena: netočan odgovor nosi -25% bodova.

- a. Ništa od navedenog.
- b. IPv4, EthernetII i Frame.
- c. Cijeli paket je enkapsuliran.
- d. Samo ICMP zaglavje.
- e. IPv4 i ICMP.

Sljedeća stranica

Prethodna stranica

+
d/quiz/attempt.php?attempt=821883&cmid=15490&page=6

Moja naslovnica Moji e-kolegiji

sigkom / Međuispit 2022./2023.

TEST

Međuispit 2022./2023.

Natrag

Pitanje 7

Nije još odgovoreno

Broj bodova od 3,00

▼ Označi pitanje

Preostalo vrijeme 1:29:14

Odaberite stavke koje sadrži osobni digitalni certifikat.

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

- a. privatni ključ korisnika
- b. informacije o instituciji koja je izdala certifikat
- c. javni ključ institucije koja je izdala certifikat
- d. informacije o korisniku
- e. digitalni potpis korisnika
- f. početno i krajnje vrijeme važenja certifikata
- g. javni ključ korisnika
- h. digitalni potpis institucije koja je izdala certifikat
- i. informacije o CRL/OCSP
- j. privatni ključ institucije koja je izdala certifikat

Sljedeća stranica

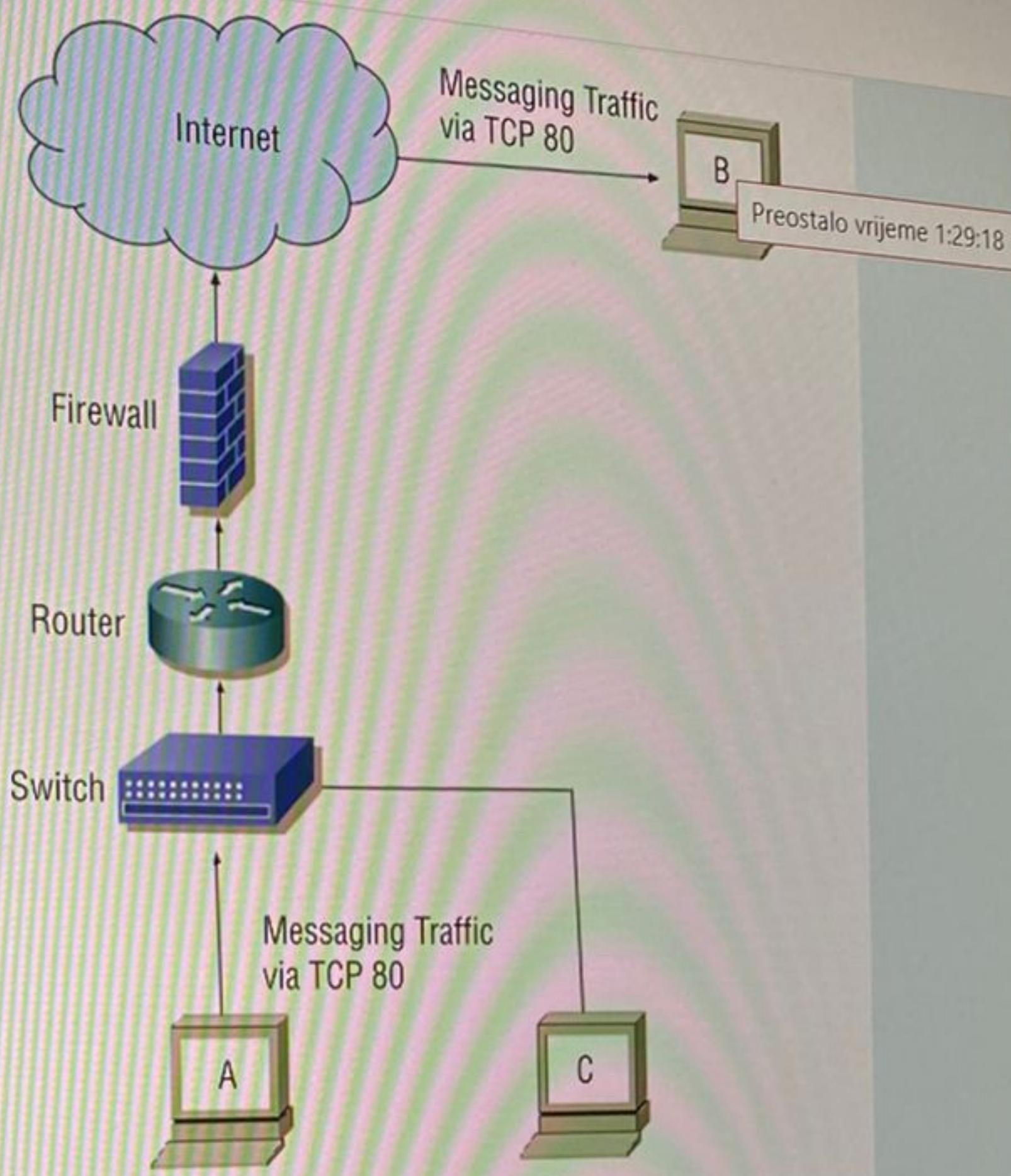
Prethodna stranica

pt.php?attempt=821883&cmid=15490&page=7#

Windows taskbar icons: File Explorer, Edge, File Manager, Mail, Google Chrome.

ROK logo in the bottom right corner.

1. Učenac
pitanje



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

slike mreže?

Odaberite neistinu tvrdnju kod razmjene poruka između A i B?

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

Sljedeća stranica

Prethodna stranica



Type here to search

The diagram illustrates a network topology. Computer A is connected to a Switch. The Switch is connected to a Router. The Router is connected to a Firewall. The Firewall is connected to the Internet. Computer C is also connected to the Switch. A red box labeled "Messaging Traffic via TCP 80" encloses the path from A to B. An arrow points from A to B with the label "via TCP 80". A red box in the top right corner contains the text "Preostalo vrijeme 0:58:51".

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

HTTP

Odaberite nešto što je izmjenjuju kod razmjene poruka između A i B?

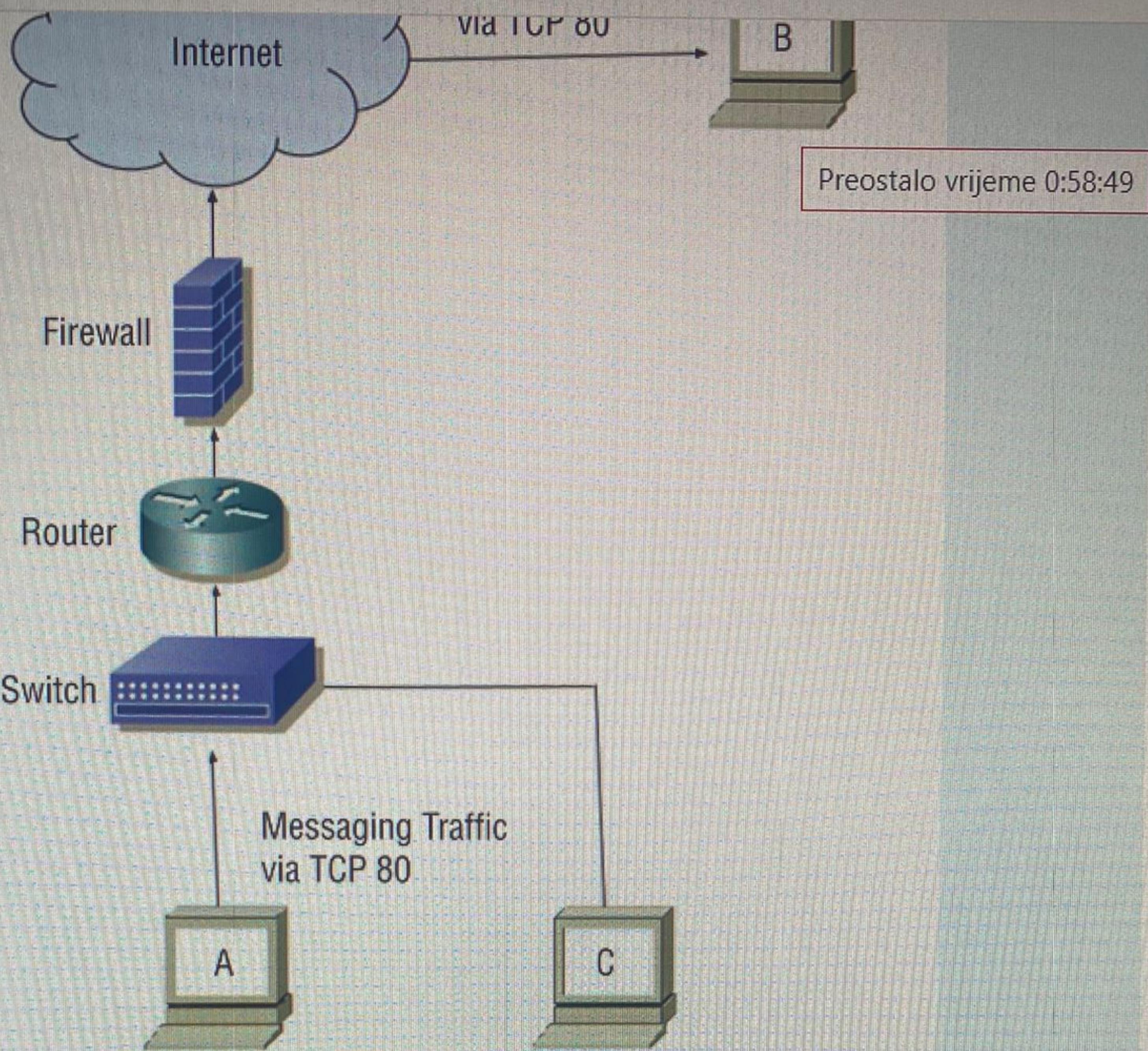
C može čitati

Napomena:

ovor NE nosi negativne bodove.

Prethodna stranica

Sljedeća stranica



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?

C može čitati poruke koje izmjenjuju A i B ako je switch u "hub" načinu rada.

C može čitati poruke koje izmjenjuju A i B ako je switch u "hub" načinu rada.

Poruke se razmjenjuju bez kriptografske zaštite.

Bilo tko u "Internetu" tko vidi taj promet može čitati poruke koje razmjenjuju A i B.

Poruke se razmjenjuju s kriptografskom zaštitom.



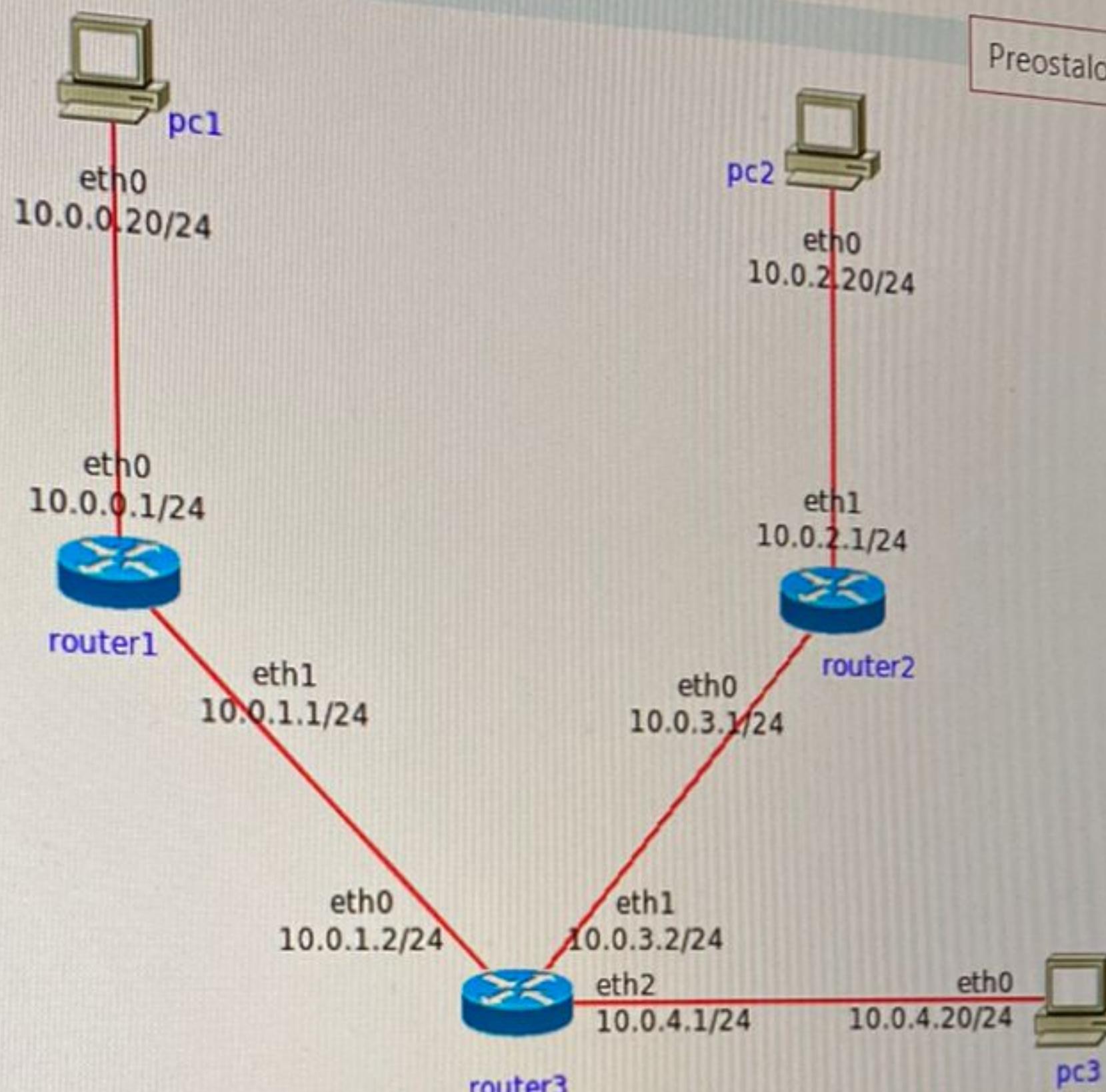
Pitanje 14

Nije još
odgovoreno

Broj bodova od
3,00

Označi
pitanje

Preostalo vrijeme 1:29:03



Koristeći prikazanu topologiju, ispunite konfiguraciju VPN-a korištenjem alata IPsec s dijeljenim ključem.

Čvor :

Local IP address:

Local subnet:

Peers IP address:

Čvor :

Local IP address:

sigkom / Međuispit 2022./2023.

TEST



Međuispit 2022./2023.

Natrag

Pitanje 12

Nije još
odgovoreno

Broj bodova od
1,00

▼ Označi
pitanje

Preostalo vrijeme 1:29:08

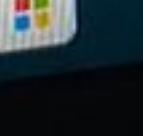
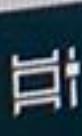
Navedene su neke preporuke za sigurnost bežičnih mreža. Odaberite netočnu preporuku.

Napomena: netočan odgovor nosi -25% bodova.

- a. Upotrebljavati WPA3 Personal ili Enterprise verzije ako je ikako moguće.
- b. Koristiti složene lozinke koje nije jednostavno pogoditi.
- c. Koristiti WPS.
- d. U slučaju WPA2 Enterprise paziti na korištenje odgovarajućih EAP metoda.
- e. Upotrebljavati WPA2 Enterprise verziju.

Sljedeća stranica

Prethodna stranica



AOC

sigkom / Međuispit 2022./2023.



TEST

Međuispit 2022./2023.

Natrag

Pitanje 8

Nije još
odgovoreno

Broj bodova od
1,00

Označi
pitanje

Preostalo vrijeme 1:29:13

Napad *UDP based amplification* je:

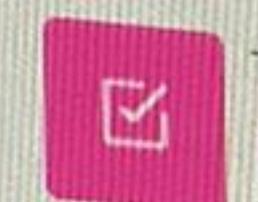
Napomena: netočan odgovor nosi negativne bodove (-25%).

- a. Napad u kojem napadač prema veličini odgovora dobivenog od strane poslužitelja otkriva točnu verziju servisa na poslužitelju.
- b. Napad u kojem napadač pokušava otkriti UDP poslužitelje koji se vrte na računalu.
- c. Napad u kojem napadač šalje ogroman broj TCP SYN paketa sa više računala kako bi zagušio poslužitelj.
- d. Napad u kojem se servisu koji koristi UDP (bez autentifikacije) pošalje upit s lažiranom izvořnom adresom a njegov odziv sadrži više podataka od upita.

Sljedeća stranica

Prethodna stranica

sigkom / Međuispit 2022./2023.



TEST

Međuispit 2022./2023.

Natrag

Pitanje 4

Nije još odgovoren

Broj bodova od
1,00

▼ Označi pitanje

Preostalo vrijeme 1:29:30

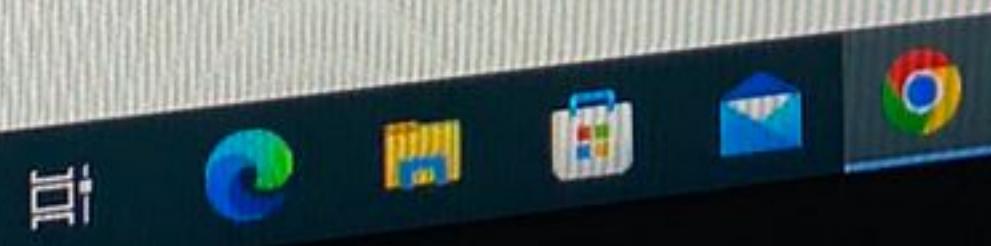
Pouzdanije rezultate pri skeniranju vrata prikazat će protokol TCP ili UDP?

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

- a. UDP zbog toga što možemo koristiti "Urgent" zastavice (polje URG u zaglavlju UDP datagrama).
- b. TCP zbog ICMP poruka koje se generiraju u slučaju da su vrata zatvorena.
- c. UDP zbog sigurnosnih mehanizama kojima operacijski sustav štiti TCP vrata.
- d. TCP zbog toga što je UDP nespojni transportni protokol.

Prethodna stranica

Sljedeća stranica



Type here to search

Moja naslovnica Moji e-kolegiji

Natrag

Pitanje 2
Nije još odgovoreno
Broj bodova od 2,00
Oznaci pitanje

ISPIS #2: 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 83.129.34.99:22 83.129.34.220:40136 SYN_RECV
...
tcp 0 0 83.129.34.99:80 83.129.34.220:40432 SYN_RECV
tcp 0 0 83.129.34.99:81 83.129.34.220:40058 SYN_RECV
tcp 0 0 83.129.34.99:82 83.129.34.220:40322 SYN_RECV

Preostalo vrijeme 1:29:35

Prikazan je ispis naredbe netstat na napadnutom računalu. U ispisu #2 vidi se da se s IP adresom 83.129.34.220 najvjerojatnije izvodi na računalo s IP adresom 83.129.34.99.

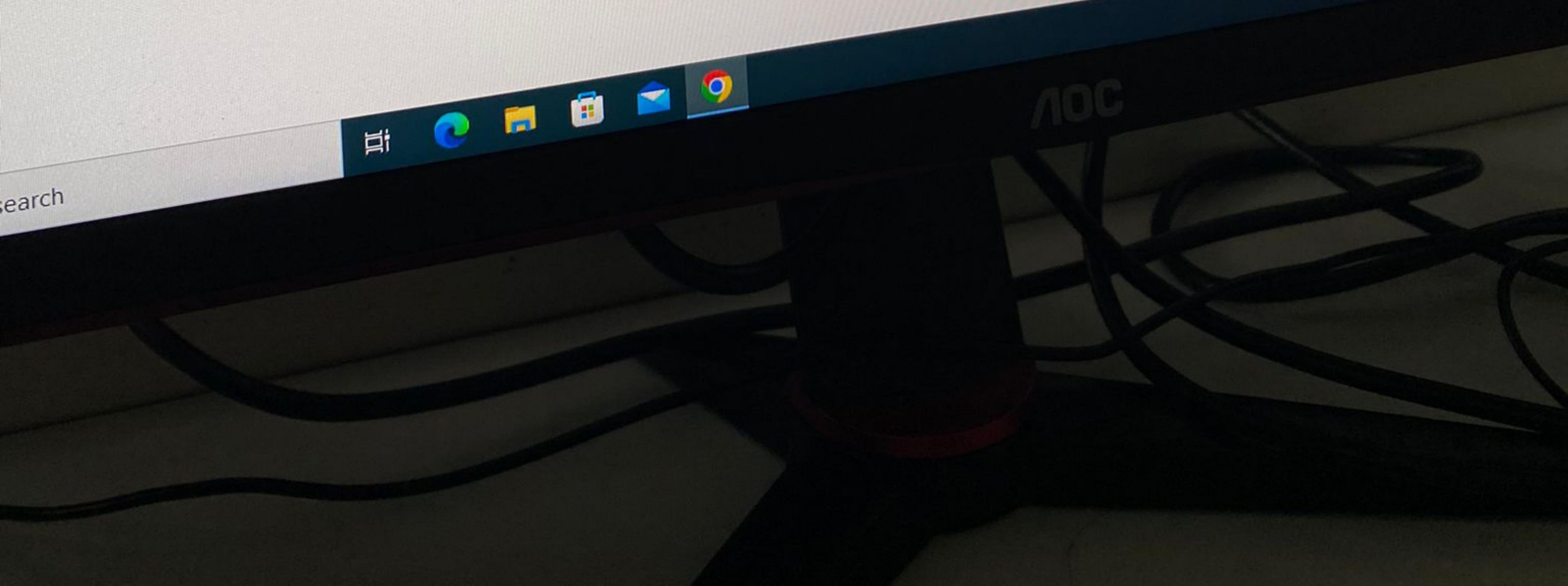
Povucite ponuđeni odgovor na ispravno mjesto u tekstu.

Napomena: netočan odgovor NE nosi negativne bodove.

UDP spoofing RST or FIN flood skeniranje portova
TCP connect flood SYN flood SYN-ACK flood
UDP hijacking UDP flood UDP amplification napad
UDP reflection napad
83.129.34.220 83.129.34.99 0.0.0.0
--- ne možemo znati ---

Slijedeća stranica

Prethodna stranica



Natrag

Pitanje 23

Odgovor
pohranjen

Broj bodova od
1,00

▼ Označi
pitanje

Preostalo vrijeme 1:23:46

Skraćenica CIA u pogledu kibernetičke sigurnosti odnosi se na svojstva:

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

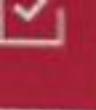
- a. Tajnosti, Integriteta, Raspoloživosti
- b. Tajnosti, Identifikacije, Raspoloživosti
- c. Kredibiliteta, Integriteta, Autentičnosti
- d. Kredibiliteta, Identifikacije, Autentičnosti

[Obriši moj odabir](#)

[Prethodna stranica](#)

[Završi test ...](#)





Međuispit 2022./2023.

Natrag

Pitanje 22

Nije još
odgovoren

Broj bodova od
1,00

Označi
pitanje

Preostalo vrijeme 1:23:49

Snimili ste 24 okvira bežičnog prometa zaštićenog WEP sigurnosnim algoritmom.

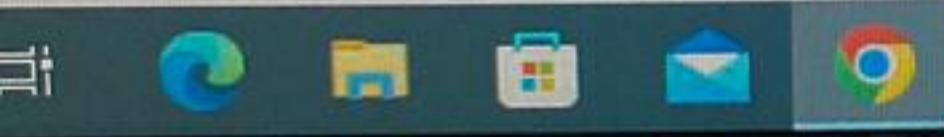
Napomena: netočan odgovor nosi **-50%** bodova.

- a. Alatom aircrack-ng možete doći do dijeljene tajne.
- b. Alatom aircrack-ng **ne** možete doći do dijeljene tajne.

Potrebno je 50k okvira

Prethodna stranica

Sljedeća stranica



Pitanje 20Nije još
odgovorenoBroj bodova od
1,00P Označi
pitanje

Konfigurirate IPSec VPN za tvrtku u kojoj će VPN koristiti 1000 ljudi. Zbog jednostavnosti izvedbe iz navedene tvrtke predlažu da IPSec konfigurirate s dijeljenim ključem (engl. *shared key*). Ulazite u raspravu s dijelatnicima tvrtke, te kao glavni argument protiv dijeljenog ključa dajete tvrdnju:

Napomena: netočan odgovor nosi **-25%** bodova.

- a. IPSec u konfiguraciji s dijeljenim ključem koristi asimetričnu kriptografiju te je šifriranje jako sporo.
- b. Protokol IPSec ne podržava šifriranje nego samo enkapsulaciju paketa.
- c. Protokol IPSec ne može se konfigurirati s dijeljenim ključem.
- d. Protokol IPSec koristi simetričnu kriptografiju i zbog toga je šifriranje jako sporo.
- e. IPSec u konfiguraciji s dijeljenim ključem koristi simetričnu kriptografiju kojoj je najveći problem distribucija ključa.
- f. Ništa od navedenog.

Prethodna stranica

Sljedeća stranica

Međuispit 2022./2023.

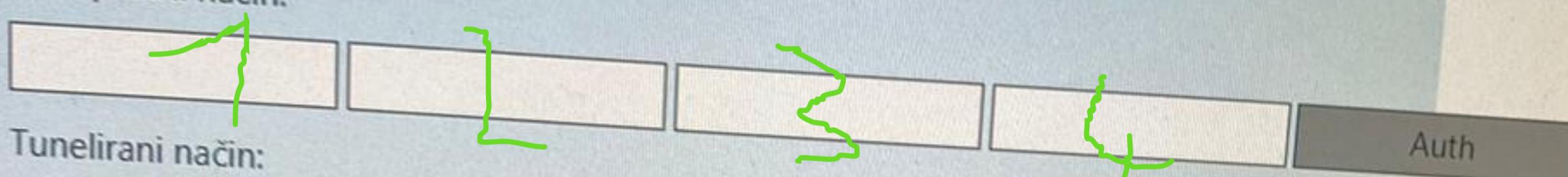
atrag

anje 17
e još
govoreno
oj bodova od
00
Označi
tanje

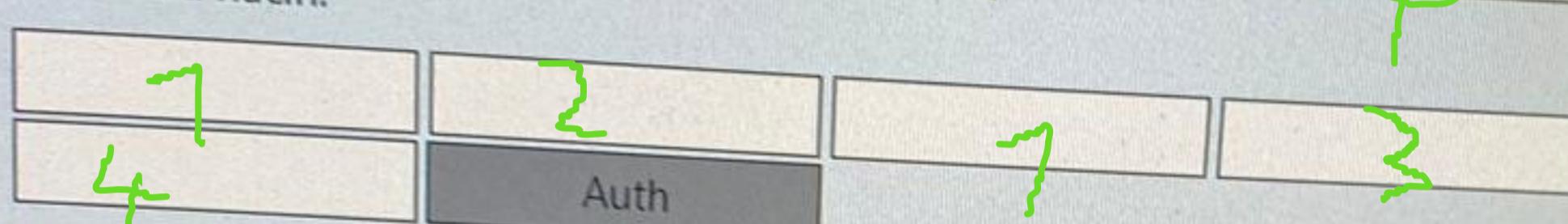
Preostalo vrijeme 1:24:03

Poredajte zaglavja unutar IPsec poruke prilikom korištenja transportnog i tuneliranog načina rada:

Transportni način:



Tunelirani način:



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

ESP trailer

IP podaci (payload)

ESP zaglavljje

IP zaglavljje

Prethodna stranica

4

3

2

1

Slijedeća stranica

age n 174



LG



Međuispit 2022./2023.

Natrag

Preostalo vrijeme 1:24:20

Pitanje 12

Nije još odgovoreno

Broj bodova od 1,00

Označi pitanje

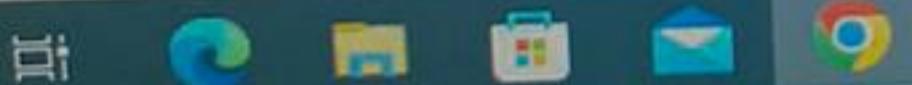
Napad *Ping of Death* je:

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

- a. Napad u kojem napadač šalje sveodredišni (*engl. broadcast*) ICMP zahtjev s lažiranim izvořišnom IP adresom. Računala iz mreže potom odgovaraju na sveodredišni zahtjev, a kako je promijenjena izvořišna adresa sveodredišnog paketa u žrtvinu odgovori zagušuju njenu mrežu.
- b. Napad fragmentacijom u kojem se kreira i šalje fragmentirani IP datagram ukupne veličine veće od 65535 okteta.
- c. Napad fragmentacijom u kojem napadač u svakom paketu postavi zastavicu *More Fragments* zbog čega poslužitelj nastavlja čekati ostale fragmente. Kontinuiranim slanjem takvih paketa napadač zagušuje poslužitelj.
- d. Napad fragmentacijom u kojem napadač pokušava zaobići vatrozid (*engl. Firewall*) na način da port postavljen u prvom fragmentu paketa prepiše nekim od sljedećih fragmenata (mijenja polje *Fragment Offset* u zaglavju IP paketa).

Prethodna stranica

Sljedeća stranica

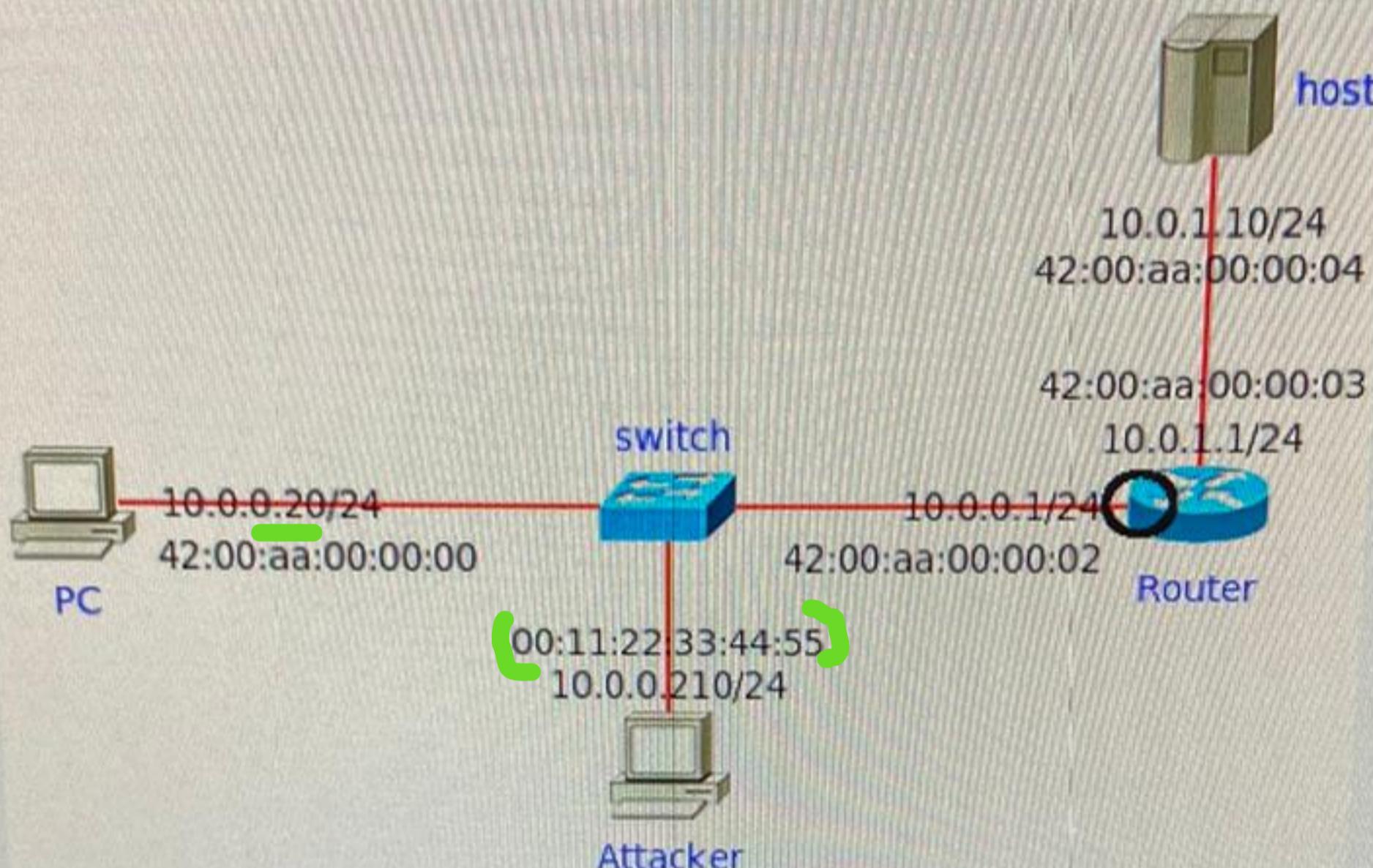


TEST

Međuispit 2022./2023.

[Natrag](#)

Preostalo vrijeme 1:25:52

Pitanje 3Nije još
odgovorenBroj bodova od
1,00
 Označi
pitanje


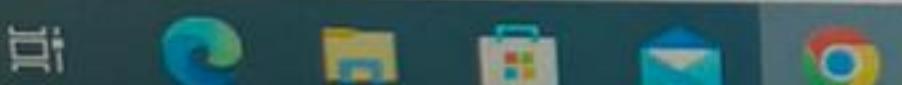
Na slici je prikazana topologija korištena u prvoj laboratorijskoj vježbi. Promet se snima na sučelju čvora *Router* označenom na slici. Korisnik sa čvora *PC* izvodi naredbu *ping* 10.0.1.10. Unutar programa Wireshark uhvatili smo paket prikazan na slici ispod.

- ▶ Frame 440: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
- ▶ Ethernet II, Src: CIMSYS_33:44:55 (00:11:22:33:44:55), Dst: 42:00:aa:00:00:02 (42:00:aa:00:00:02)
- ▶ Internet Protocol Version 4, Src: 10.0.0.20, Dst: 10.0.1.10
- ▶ Internet Control Message Protocol

Je li napadač sa čvora *PC* pokrenuo napad MITM (engl. *Man In The Middle*)?

Napomena: netočan odgovor nosi **-50%** bodova.

* Napadač **nije** pokrenuo napad MITM.

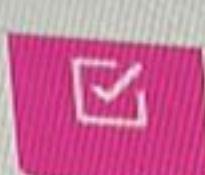


Pitanje 17Nije još
odgovorenoBroj bodova od
1,00▼ Kliknite za
uklanjanje
oznake
neprikladnosti

Koja se vrsta kriptografije koristi za zaštitu poruka kod DNSSEC-a?

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

- a. Koristi se kriptografija javnog ključa pri digitalnom potpisivanju zapisa na poslužitelju.
- b. Koristi se simetrična kriptografija za šifriranje cijelog odgovora poslužitelja.
- c. Koristi se privatni ključ za šifriranje cijelog odgovora poslužitelja. ne sifira, samo autentificira
- d. Koriste se asimetrična i simetrična kriptografija pri šifriranju zapisa na poslužitelju.
- e. Koristi se javni ključ klijenta za šifriranje cijelog odgovora poslužitelja.



Međuispit 2022./2023.

Natrag

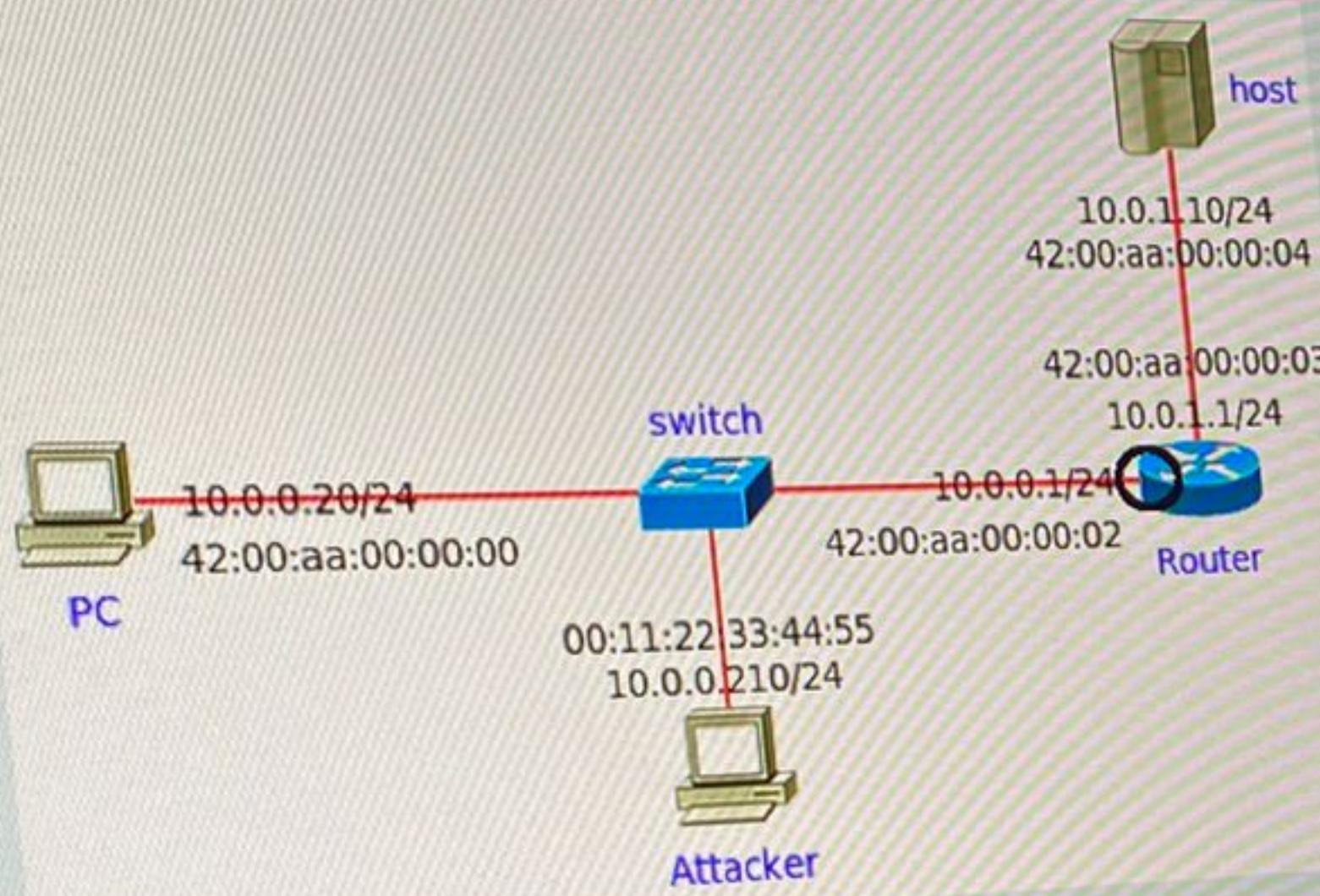
Pitanje 1

Nije još odgovoren

Broj bodova od 2,00

Označi pitanje

Preostalo vrijeme 1:29:40



U mreži prikazanoj na slici, napadač s računala Attacker pokreće napad alatom arpspoof s namjerom snimanja sveg prometa između računala PC i host. Prilikom izvođenja napada snima se promet na označenom sučelju čvora Router. Odredite adrese u ARP paketu koji je poslao napadač, a na navedenom sučelju primio čvor Router.

Pošiljateljeva (engl. sender) MAC adresa: 00:11:22:33:44:55
Primateljeva (engl. target) MAC adresa: 42:00:aa:00:00:02

Pošiljateljeva (engl. sender) IP adresa: 10.0.0.20 pc
Primateljeva (engl. target) IP adresa: 10.0.0.1

Napomena: netočan odgovor NE nosi negativne bodove.
 Broadcast 42:00:aa:00:00:00 00:11:22:33:44:55 42:00:aa:00:00:04
 42:00:aa:00:00:03 42:00:aa:00:00:02 10.0.0.1 10.0.0.20 10.0.1.1 10.0.0.210
 10.0.0.1 10.0.1.10 10.0.0.20 10.0.1.1 10.0.0.210

Navigacija
1 2
8
15
22
Zav.

Pitanje 15

Nije još odgovoreno

Broj bodova od 1,00

Označi pitanje

Napad UDP based amplification je:**Napomena:** netočan odgovor nosi negativne bodove (-25%).

- a. Napad u kojem se servisu koji koristi UDP (bez autentifikacije) pošalje upit s lažiranom izvorišnom adresom a njegov odziv sadrži više podataka od upita.
- b. Napad u kojem napadač šalje ogroman broj TCP SYN paketa sa više računala kako bi zagušio poslužitelj.
- c. Napad u kojem napadač prema veličini odgovora dobivenog od strane poslužitelja otkriva točnu verziju servisa na poslužitelju.
- d. Napad u kojem napadač pokušava otkriti UDP poslužitelje koji se vrte na računalu.

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

Navedene su neke preporuke za sigurnost bežičnih mreža. Odaberite netočnu preporuku.

Napomena: netočan odgovor nosi -25% bodova.

- a. Upotrebljavati WPA2 Enterprise verziju.
- b. U slučaju WPA2 Enterprise paziti na korištenje odgovarajućih EAP metoda.
- c. Koristiti WPS.
- d. Upotrebljavati WPA3 Personal ili Enterprise verzije ako je ikako moguće.
- e. Koristiti složene lozinke koje nije jednostavno pogoditi.

ca

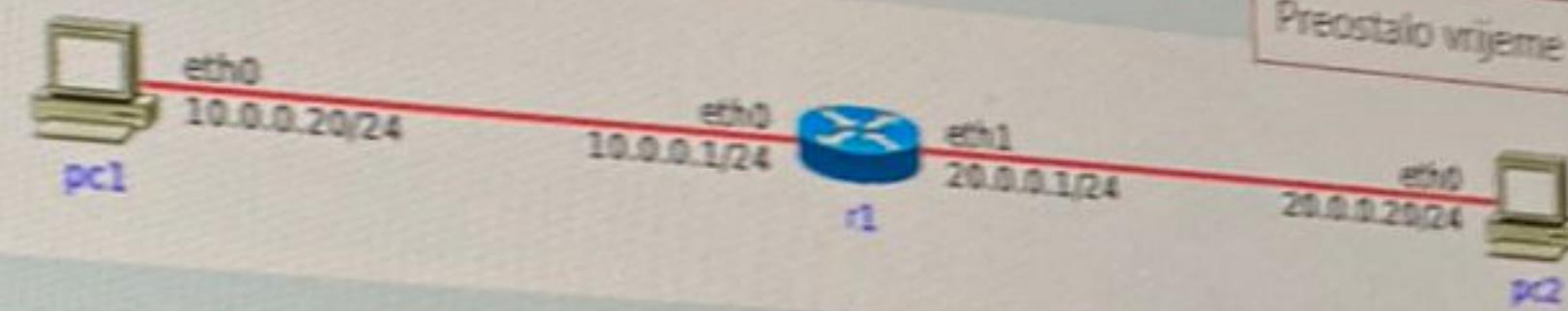
[Sljedeća stranica](#)

Pitanje 5

Nije još odgovoreno

Broj bodova od 2,00

Označi pitanje



Na usmjeritelju $r1$ s topologije prikazane na slici izvršene su naredbe:

```
$ iptables -t nat -A POSTROUTING --out-interface eth0 -j MASQUERADE  
$ iptables -A FORWARD --in-interface eth1 -j ACCEPT
```

Na sučelju $eth0$ čvora $pc2$ snimate promet alatom Wireshark. Računalo $pc2$ je pokrenulo naredbu $ping 10.0.0.20$.

Koje su izvođene i odredišne IP adrese ICMP echo request i ICMP echo reply paketa snimljenih u alatu Wireshark?

ICMP echo request paket:

Izvođena IP adresa: 20.0.0.20
Odredišna IP adresa: 10.0.0.20

ICMP echo reply paket:

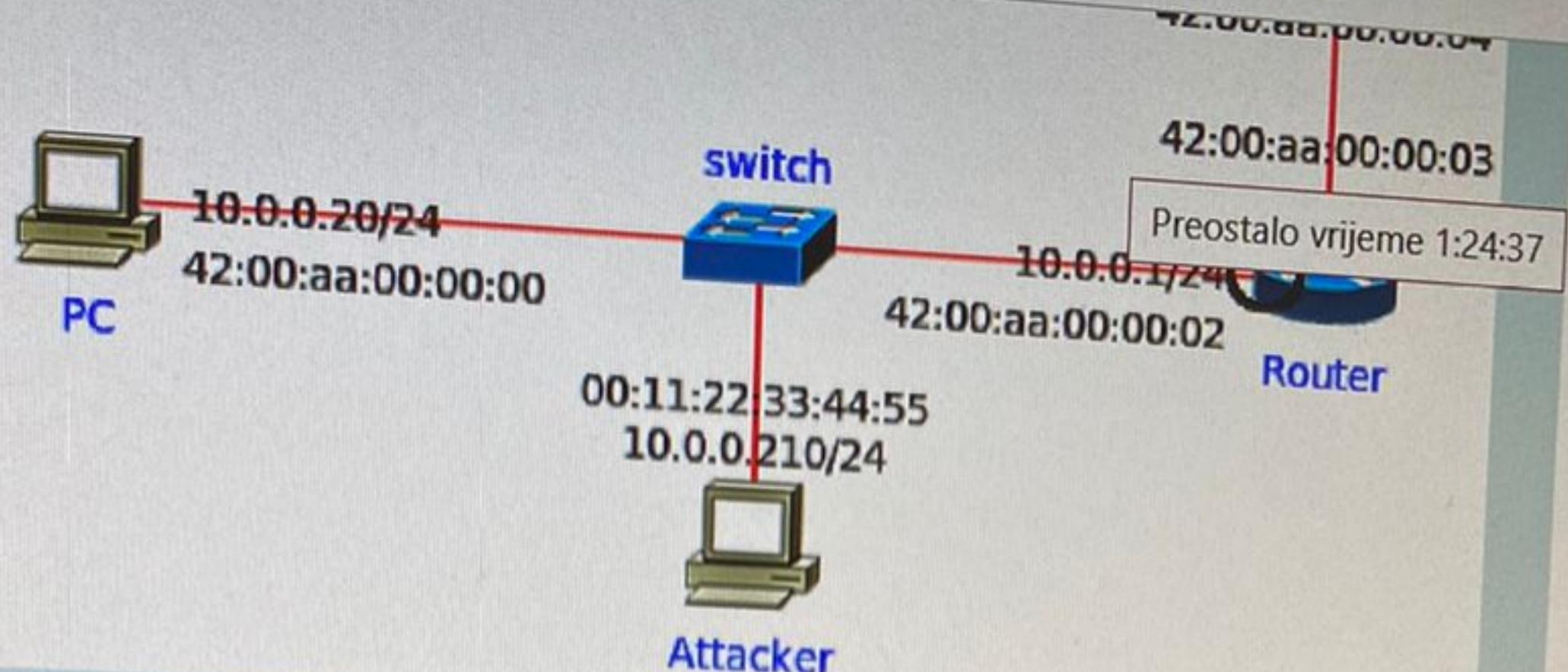
Izvođena IP adresa: 10.0.0.20
Odredišna IP adresa: 20.0.0.20

Napomena: netočan odgovor NE nosi negativne bodove.

Slijedeća stranica

Prethodna stranica





U mreži prikazanoj na slici, napadač je s računala *Attacker* uspješno pokrenuo napad alatom *arpspoof* s namjerom snimanja sveg prometa između računala *PC* i *host*.

Pretpostavimo da je na računalu **PC** pokrenuta naredba *ping 10.0.1.10*. Odaberite izvorišne i odredišne MAC i IP adrese za **ICMP Echo request** paket koji se vidi ako snimamo promet na označenom sučelju usmjeritelja *Router*.

Izvořišna MAC adresa: 00:11:22:33:44:55

Odredišna MAC adresa: router (42:00:aa:00:00:02)

Izvořišna IP adresa: 10.0.0.20

Odredišna IP adresa: 10.0.1.10 (host)

Pretpostavimo da je na računalu **host** pokrenuta naredba *ping 10.0.0.20*. Odaberite izvorišne i odredišne MAC i IP adrese za **ICMP Echo reply** paket koji se vidi ako snimamo promet na označenom sučelju usmjeritelja *Router*.

Izvořišna MAC adresa: 00:11:22:33:44:55

Odredišna MAC adresa: router (42:00:aa:00:00:02)

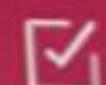
Izvořišna IP adresa: 10.0.0.20

Odredišna IP adresa: 10.0.1.10 (host)

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

42:00:aa:00:00:03 00:11:22:33:44:55 42:00:aa:00:00:02 42:00:aa:00:00:00

42:00:aa:00:00:04



TEST

Međuispit 2022./2023.

Natrag

Preostalo vrijeme 1:24:24

Pitanje 10

Nije još odgovoreno

Broj bodova od 1,00

▼ Označi pitanje

Na koji osnovni sigurnosni zahtjev informacijske sigurnosti utječe napad (D)DoS?

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

- a. Neporecivost
- b. Integritet
- c. Povjerljivost
- d. Dostupnost

Prethodna stranica

Sljedeća stranica

Međuispit 2022./2023.

g

18

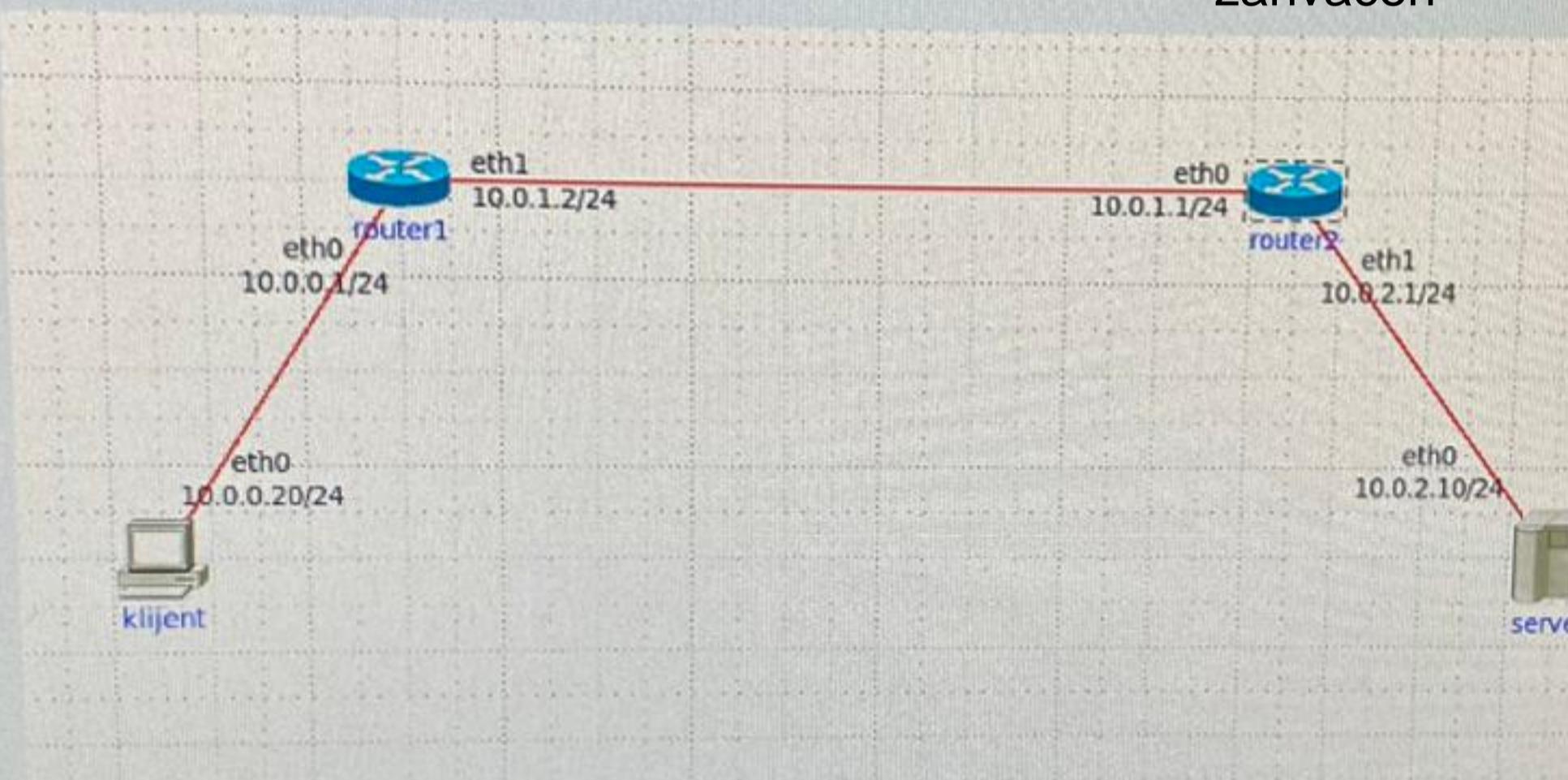
reno
od
nači
e

Preostalo vrijeme 1:24:00

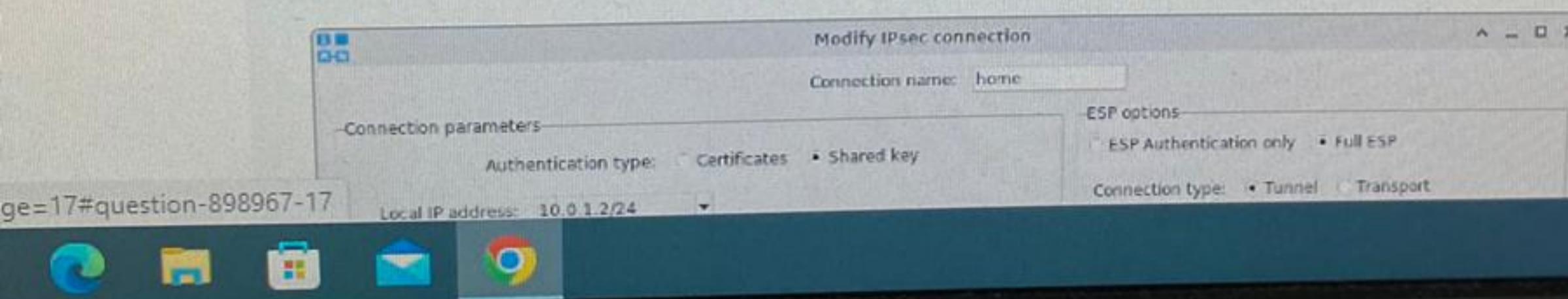
Slika 1. prikazuje topologiju mreže u kojoj se između čvorova *router1* i *router2* postavlja IPSec tunel (konfiguracija tunela prikazana je na slikama 2. i 3.). Nakon konfiguracije tunela i izvršavanja naredbe *ping 10.0.2.10* sa čvora *klijent* u programu Wireshark vidljiv je šifrirani promet koji se razmjenjuje između čvorova *klijent* i *server*. Naknadno u mrežu ubacujemo čvor *klijent2* i spajamo ga na usmjeritelj *router1*. Nakon toga, s čvora *klijent2* pokrećemo naredbu *ping 10.0.2.10*. Hoće li razmjenjeni promet biti šifriran?

Napomena: netočan odgovor nosi **-50%** bodova.

IPSec konfiguracija je dobra ali klijent2 uopće nije njome zahvacen



Slika 1. Inicijalna topologija mreže



LG