

Internet mreže: test3

Pitanja

1. Snimljen je sadržaj frejma, potrebno je odrediti dužinu prvog polja zaglavlja ovog frejma (da li u oktetima ili bitima, **VODITI RAČUNA**)
2. Odrediti tip frejma čiji je sadržaj dat u prvom pitanju.
3. Na osnovu čega se određuje tip frejma.
4. Polje IHL označava dužinu zaglavlja paketa u kojim jedinicama ?
5. IP adresa onoga kome je paket namenjen je ?
6. Ako je u polje Protocol IP zaglavlja upisana vrednost 0x11, to znači da je u paket enkapsuliran protokol ?
7. Na osnovu podataka iz prvog pitanja, odrediti koje dve aplikacije učestvuju u komunikaciji: Obrazložiti odgovor.
8. Koliki je maksimalni broj čvorišta ili nivoa kroz koji IP paket sa slike može proći.
9. Verzija IP protokola korišćenog u frejmu datom u prvom pitanju je?
10. IP adresa onoga ko šalje paket je ?
11. Upisati veličinu zaglavlja (merenu u oktetima) IP paketa koji je enkapsuliran u dati frejm?

Odgovori

Najkorisniji sajt za dekodiranje je: <https://hpd.gasmi.net>

Za listu IP protokola: https://en.m.wikipedia.org/wiki/List_of_IP_Protocol_numbers

Za listu TCP I UDP portova: https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers a za detaljniji opis <https://www.adminsub.net/tcp-udp-port-finder>

1. [zavisi od zadatka] Niko ne zna zasto, ali potrebno je samo prepisati od vec datog broja gore(vec su dali resenje nzm sto)
2. [zavisi od zadatka] Tip frejma dobijamo ako pogledamo ovaj parameter.

Decode

Hide packet

Upload

147.91.172.244 → 2.21.93.238 TCP 55011 → 80 [PSH, ACK] [TCP segment of a reassembled PDU]

0	1	2	3	4	5	6	7	8	9
00	00	0C	07	AC	01	00	1B	21	30
01	82	77	88	40	00	80	06	00	00
5D	EE	D6	E3	00	50	6E	46	11	76
40	29	A1	C7	00	00	47	45	54	20
6E	2F	76	31	37	2F	63	73	73	2F

3 protocols in packet:

EthernetIPv4TCPALL

[+] [-]

Frame 1: 80 bytes on wire (640 bits)

Ethernet II

Internet Protocol Version 4

Transmission Control Protocol

HPD v2.9.4 by Salim Gasmi.

3. Vrednost polja zaglavlja nakon adrese pošiljaoca manja od 1500(decimalno) znači da je u pitanju 802.3 frejm

4. 32-bitna reč

5. [zavisi od zadatka] Na slici ispod se vidi adresa onog ko prima paket

Decode Hide packet Upload

147.91.172.244 → 2.21.93.238 TCP 55011 → 80 [PSH, ACK] [TCP segment of a reassembled PDU]

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00	00	0C	07	AC	01	00	1B	21	30	D7	B9	08	00	45	00
01	82	77	88	40	00	80	06	00	00	93	5B	AC	F4	02	15
5D	EE	D6	E3	00	50	6E	46	11	76	61	79	14	DC	50	18
40	29	A1	C7	00	00	47	45	54	20	2F	63	6F	6D	6D	6F
6E	2F	76	31	37	2F	63	73	73	2F	68	6F	6D	65	70	61

3 protocols in packet:

Ethernet IPv4 TCP ALL

6. [zavisi od zadatka] Za ovu konkretnu vrednost je UDP ali postupak pronalaženja rešenja se zasniva tako što otvorimo ovu stranicu: https://en.m.wikipedia.org/wiki/List_of_IP_Protocol_numbers i potom nadjemo našu datu vrednost Protocol IP zaglavlja I isčitamo koji je paket enkapsuliran u protocol.

0x0E	14	EMCON	EMCON	
0x0F	15	XNET	Cross Net Debugger	IEN 158 ^[2]
0x10	16	CHAOS	Chaos	
0x11	17	UDP	User Datagram Protocol	RFC 768 ^[2]
0x12	18	MUX	Multiplexing	IEN 90 ^[3]
0x13	19	DCN-MEAS	DCN Measurement Subsystems	
0x14	20	HMP	Host Monitoring Protocol	RFC 869 ^[2]
0x15	21	PRM	Packet Radio Measurement	
0x16	22	XNS-IDP	XEROX NS IDP	
0x17	23	TRUNK-1	Trunk-1	
0x18	24	TRUNK-2	Trunk-2	
0x19	25	LEAF-1	Leaf-1	

7. [zavisi od zadatka] **Source port i destination** čitamo kao na sledeće dve slike.

Na osnovu podataka iz prvog pitanja, odrediti koje dve aplikacije učestvuju u komunikaciji. Obrazložiti odgovor.

Na osnovu podataka iz prvog pitanja zaključujemo da se koristi UDP, Source port u UDP zaglavlju je 0x35 što je u decimalnom zapisu 53, to nam govori da je jedna aplikacija DNS server. Destination port je 64184.

Završi pregled

Decode Hide packet Upload

147.91.173. → 147.91.173. User Datagram Protocol Standard query response 0xdf

Source Port: 53

0	1	2	3	4	5	6	7	8
00	1B	21	00	07	B1	00	07	EC
01	ED	00	00	3F	11	B9		
AC	EA	00	35	FA	B8	01	D9	DD
00	05	00	08	00	08	03	77	77
03	63	6F	6D	00	00	01	00	01
00	03	84	00	1D	03	77	77	77

4 protocols in packet:

Ethernet IPv4 UDP DNS ALL

Na osnovu podataka iz prvog pitanja, odrediti koje dve aplikacije učestvuju u komunikaciji. Obrazložiti odgovor.

Na osnovu podataka iz prvog pitanja zaključujemo da se koristi UDP, Source port u UDP zaglavlju je 0x35 što je u decimalnom zapisu 53, to nam govori da je jedna aplikacija DNS server. Destination port je 64184.

Završi pregled

Decode Hide packet Upload

147.91.173.3 → 147.91.173.3 User Datagram Protocol Standard query response 0xdf

Destination Port: 64184

0	1	2	3	4	5	6	7
00	1B	21	00	07	B1	00	07
01	ED	00	00	3F	11	B9	
AC	EA	00	35	FA	B8	01	D9
00	05	00	08	00	08	03	77
03	63	6F	6D	00	00	01	00
00	03	84	00	1D	03	77	77

4 protocols in packet:

Ethernet IPv4 UDP DNS ALL

[+] [-]

8. [zavisi od zadatka] Ovde tražimo prvi ovaj plavi sa atributom “Time to live” koji nam govori **maksimalan broj čvorova ili nivoa** kroz koji IP paket sa slike može proći.

Koliko je maksimalni broj čvorova III nivoa kroz koji IP paket sa slike može proći? **63**

Upisati veličinu zaglavlja (merenu u oktetima) IP paketa koji je enkapsuliran u dati frejm: **20**

Internet Protocol Version 4
Time to live: 63

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00	1B	21	30	00	00	40	00	3F	11	B9	5B	93	AC	77	4C
01	ED	00	00	FA	B8	01	D9	DD	75	DF	00	05	00	08	00
02	00	08	00	08	03	77	77	77	77	05	03	63	6F	6D	00
03	00	01	00	01	C0	0C	00	03	84	00	1D	03	77	77	77
04	00	03	84	00	1D	03	77	77	77	05	69				

9. [zavisi od zadatka] Kao na slici ispod verziju IP protokola možemo pročitati iz dva parametra.

Decode Hide packet Upload

147.91.172.244 → 2.21.93.238 TCP 55011 → 80 [PSH, ACK] [TCP segment of a reassembled PDU]

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00	00	0C	07	AC	01	00	1B	21	30	D7	B9	08	00	45	00
01	82	77	88	40	00	80	06	00	00	93	5B	AC	F4	02	15
02	00	08	00	08	03	77	77	77	77	05	03	63	6F	6D	00
03	00	01	00	01	C0	0C	00	03	84	00	1D	03	77	77	77
04	00	03	84	00	1D	03	77	77	77	05	69				

Internet Protocol Version 4

Src: 147.91.172.244
Dst: 2.21.93.238
Length: 20 bytes

Ethernet IPv4 TCP ALL

[+] [-]

- Frame 1: 80 bytes on wire (640 bits)
- Ethernet II
- Internet Protocol Version 4
- Transmission Control Protocol

10. [zavisi od zadatka] Adresa onome kome šaljem se isčitava iz ovog parametra.

147.91.172.244 → 2.21.93.238 TCP 55011 → 80 [PSH, ACK] [TCP segment of a reassembled PDU]

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00	00	0C	07	AC	01	00	1B	21	30	D7	B9	08	00	45	00
01	82	77	88	40	00	80	06	00	00	93	5B	AC	F4	02	15
5D	EE	D6	E3	00	50	6E	46	11	76	61	79	14	DC	50	18
40	29	A1	C7	00	00	47	45	54	20	2F	63	6F	6D	6D	6F
6E	2F	76	31	37	2F	63	73	73	2F	68	6F	6D	65	70	61

3 protocols in packet:

☒ Ethernet ☒ IPv4 ☒ TCP ☐ ALL

[+] [-]

- Frame 1: 80 bytes on wire (640 bits)
- Ethernet II
- Internet Protocol Version 4
- Transmission Control Protocol

11. [zavisi od zadatka] Kada počne plavi deo, pročitam koliki je "Header Length" i on nam govori veličinu zaglavlja IP paketa.

Koliki je maksimalni broj čvorista III nivoa kroz koji IP paket sa slike može proći? 63

Upisati veličinu zaglavlja (merenu u oktetima) IP paketa koji je enkapsuliran u dati frejm: 20

00 1B 21 30 D7 B1 00 07 EC 77 4C 0A 08 00 45 00 01 ED 00 00 40 00 3F 11 B9 50 93 5B AD 03 93 5B AC EA 00 35 FA B8 01 D9 DD 75 DF 3F B1 80 00 01 00 05 00 08 00 08 03 77 77 77 05 69 6E 74 65 6C 03 63 6F 6D 00 00 01 00 01 C0 0C 00 05 00 01 00 00 03 84 00 1D 03 77 77 77 05 69 6E 74 65

Decode Hide packet Upload

147.91.173.3 → 147.91.172.234 DNS Standard query response 0xdf3f A www.intel.com

Internet Protocol Version 4
0100 ... = Version: 4
... 0101 = Header Length: 20 bytes (5)
Field length: 1
Byte offset: 14

0	1	2	3	4	5	6	7	8	9	10	11
00	1B	21	30	D7	B1	00	07	EC	77	4C	0A
01	ED	00	00	40	00	3F	11	B9	5B	93	5B
AC	EA	00	35	FA	B8	01	D9	DD	75	DF	3F
00	05	00	08	00	08	03	77	77	77	05	69
03	63	6F	6D	00	00	01	00	01	C0	0C	00
00	03	84	00	1D	03	77	77	77	05	69	6E