

1. ncat 10.21.78.111 12345

147 101.193912795 192.168.254.129 10.21.78.111 FTP 83 Request: STOR c75-GrabThePhisher.zip	
149 101.252377208 10.21.78.111 192.168.254.129 FTP 122 Response: 150 Opening BINARY mode data connection for c75-GrabThePhisher.zip	
[Conversation completeness: Complete, WITH_DATA (31)]	
[TCP Segment Len: 29]	
Sequence Number: 47 (relative sequence number)	
Sequence Number (raw): 258040667	
[Next Sequence Number: 76 (relative sequence number)]	
Acknowledgment Number: 593 (relative ack number)	
Acknowledgment number (raw): 1044861039	
	0000 00 50 0010 00 45 0020 4e 6f 0030 ff ff 0040 72 61 0050 70 0d

- a. Berapakah sequence number (raw) pada packet yang menunjukkan aktivitas tersebut?

Your answer: **258040667**

- b. Berapakah acknowledge number (raw) pada packet yang menunjukkan aktivitas tersebut?

Your answer: **1044861039**

149 101.252377208 10.21.78.111 192.168.254.129 FTP 122 Response: 150 Opening BINARY mode data connection for c75-GrabThePhisher.zip	
151 102.475086812 10.21.78.111 192.168.254.129 FTP 60 Request: FDSV	
[Conversation completeness: Complete, WITH_DATA (31)]	
[TCP Segment Len: 68]	
Sequence Number: 593 (relative sequence number)	
Sequence Number (raw): 1044861039	
[Next Sequence Number: 661 (relative sequence number)]	
Acknowledgment Number: 76 (relative ack number)	
Acknowledgment number (raw): 258040696	
	0000 00 0c 29 fa e2 fc 00 50 56 f5 e6 a9 08 00 4 0010 00 6c 63 7b 00 00 80 06 bf 62 0a 15 4e 6f c 0020 fe 81 00 15 e6 30 3e 47 50 6f 0f 61 63 78 5 0030 fa f0 2a c2 00 00 31 35 30 20 4f 70 65 6e 6 0040 67 20 42 49 4e 41 52 59 20 6d 6f 64 65 20 6 0050 74 61 20 63 6f 6e 6e 65 63 74 69 6f 6e 20 6 0060 72 20 63 37 35 2d 47 72 61 62 54 68 65 50 6 0070 73 68 65 72 2e 7a 69 70 0d 0a

- c. Berapakah sequence number (raw) pada packet yang menunjukkan response dari aktivitas tersebut?

Your answer: **1044861039**

- d. Berapakah acknowledge number (raw) pada packet yang menunjukkan response dari aktivitas tersebut?

Your answer: **258040696**

```
PS C:\Users\nabie> ncat 10.21.78.111 12345
a. Berapakah sequence number (raw) pada packet yang menunjukkan aktivitas tersebut?
Your answer: 258040667
Correct answer!
b. Berapakah acknowledge number (raw) pada packet yang menunjukkan aktivitas tersebut?
Your answer: 1044861039
Correct answer!
c. Berapakah sequence number (raw) pada packet yang menunjukkan response dari aktivitas tersebut?
Your answer: 1044861039
Correct answer!
d. Berapakah acknowledge number (raw) pada packet yang menunjukkan response dari aktivitas tersebut?
Your answer: 258040696
Correct answer!
Correct answers, you are good at addressing!
Here is your flag: Jarkom2023{y0u_r_g00d_4t_4dr3ssing_JoBvKyA74646623}
```

Flag: Jarkom2023{y0u_r_g00d_4t_4dr3ssing_BxKoMxD44474065}

2. ncat 10.21.78.111 13579

soal2.pcapng	Wireshark - Follow HTTP Stream (tcp.stream eq 43) - soal2.pcapng
File Edit View Go Capture Analyze Statistics Help	GET / HTTP/1.1 Host: 10.21.78.111:8000 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive Upgrade-Insecure-Requests: 1
No. Time Source	HTTP/1.1 200 OK Server: gunicorn Date: Thu, 14 Sep 2023 12:52:59 GMT Connection: keep-alive Content-Type: text/html; charset=utf-8 Content-Length: 7761 Set-Cookie: session=1f0be1b9-b4e9-484f-b90b-ffca6f74fc72.vvas5xRXgw2085_i854fJKREF5U; HttpOnly; Path=/; SameSite=Lax
1092 15.126318680 192.168.254.1	<!DOCTYPE html> <html> <head> <title>Praktikum Jarkom 2023</title> <meta charset="utf-8"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <link rel="shortcut icon" href="/themes/core-beta/static/img/favicon.ico?d=3663515f" type="image/x-icon"> <link rel="stylesheet" href="/themes/core-beta/static/assets/main.0aaf8d88.css">
1108 15.227318761 10.21.78.111	
1117 15.722866356 192.168.254.1	
1797 17.187632467 10.21.78.111	
1800 17.245757032 192.168.254.1	
1825 17.375703595 10.21.78.111	
1856 17.582310901 192.168.254.1	
1875 17.604993492 10.21.78.111	
1914 17.964798385 192.168.254.1	
1916 18.031274311 10.21.78.111	
1089 15.064180569 192.168.254.1	
1090 15.124256287 10.21.78.111	
1091 15.124677627 192.168.254.1	
1093 15.126925112 10.21.78.111	
1102 15.226352090 10.21.78.111	
1103 15.226352123 10.21.78.111	
1104 15.226491924 192.168.254.1	
1105 15.226522743 192.168.254.1	
1106 15.227011302 10.21.78.111	
1107 15.227061573 192.168.254.1	
1109 15.227343903 192.168.254.1	
1110 15.273304375 10.21.78.111	
1155 15.795020947 10.21.78.111	
1156 15.795020977 10.21.78.111	

Sebutkan web server yang digunakan pada portal praktikum Jaringan Komputer!

Your answer: **gunicorn**

Vidiawan Nabiel Arrasyid
5025221231
Jarkom E

```
PS C:\Users\nabie> ncat 10.21.78.111 13579
Sebutkan web server yang digunakan pada portal praktikum Jaringan Komputer!
Your answer: gunicorn
Correct answer!
Here is your flag: Jarkom2023{9unic0rn_1s_2k7r0ghM7a48XFW_c00l}
```

Flag: Jarkom2023{9unic0rn_1s_4dfm9qIOP4H40Xg_c00l}

3. ncat 10.21.78.111 13590

(ip.src == 239.255.255.250 || ip.dst == 239.255.255.250) && (udp.port == 3702 || tcp.port == 3702)

Filter

Wireshark capture of traffic on interface soal3.pcapng. The packet list shows multiple UDP packets from 192.168.2.1 to 239.255.255.250 on port 3702. The packet details for packet 2278 show an Ethernet II frame, an IPv4 packet, and a User Datagram Protocol (UDP) packet with source port 51410 and destination port 3702. The packet bytes show an XML payload.

a. Berapa banyak paket yang tercapture dengan IP source maupun destination address adalah 239.255.255.250 dengan port 3702?

Your answer: **21**

b. Protokol layer transport apa yang digunakan?

Your answer: **UDP**

```
PS C:\Users\nabie> ncat 10.21.78.111 13590
```

a. Berapa banyak paket yang tercapture dengan IP source maupun destination address adalah 239.255.255.250 dengan port 3702?

Your answer: **21**

Correct answer!

b. Protokol layer transport apa yang digunakan?

Your answer: **UDP**

Correct answer!

Correct answers, you are good at analysis!

Here is your flag: Jarkom2023{4nalyz3_is_1073-BiFu0gSwByD_gr3at}

Flag: Jarkom2023{4nalyz3_is_0671_ShSyAmDIFgN_gr3at}

4. ncat 10.21.78.111 13591

Wireshark capture of traffic on interface soal4.pcapng. The packet list shows a single packet (130) from 192.168.1.19 to 74.125.130.139. The packet details show a User Datagram Protocol (UDP) packet with source port 57296 and destination port 443. The packet bytes show a checksum value of 0x18e5.

Berapa nilai checksum yang didapat dari header pada paket nomor 130?

Your answer: **0x18e5**

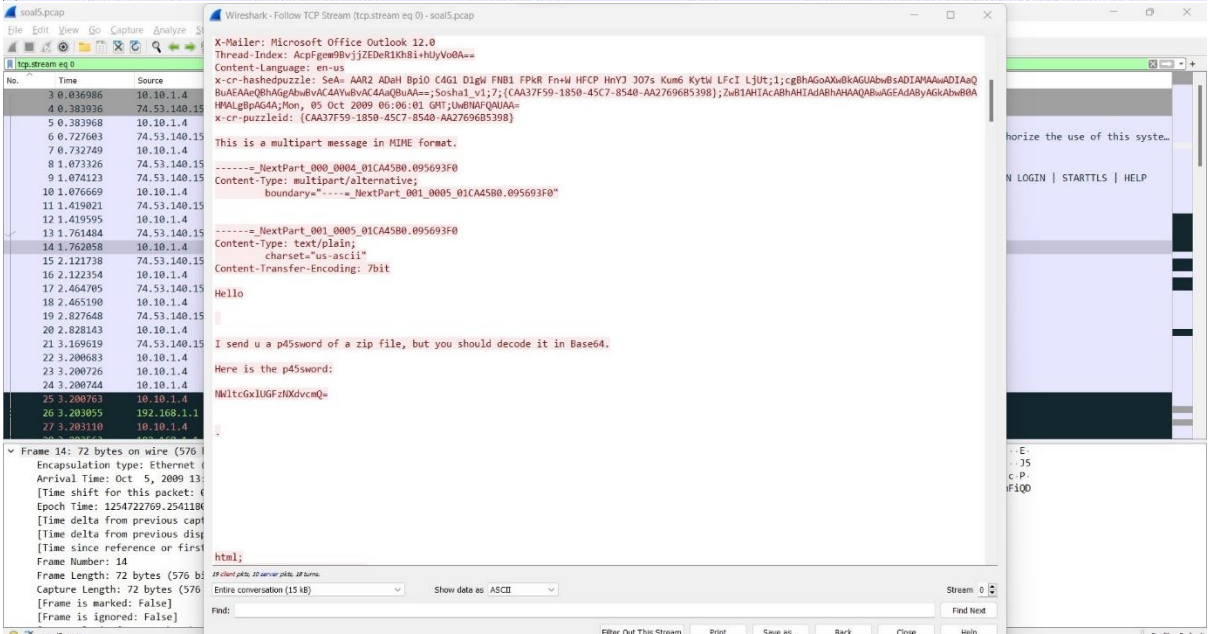
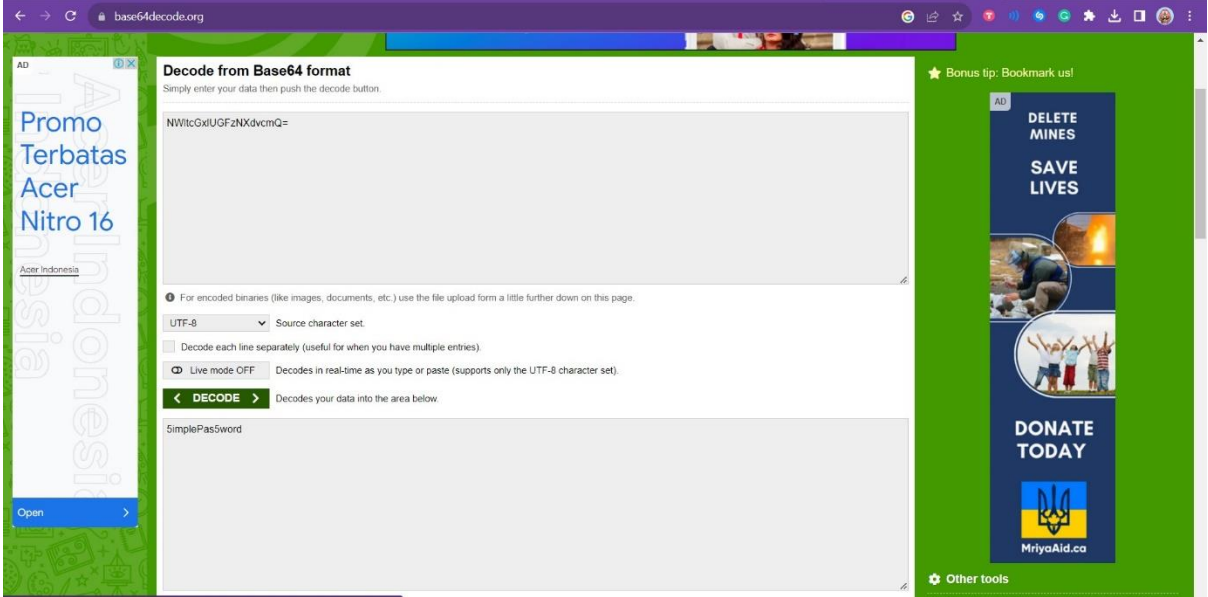
Vidiawan Nabiel Arrasyid
5025221231
Jarkom E

```
PS C:\Users\nabie> ncat 10.21.78.111 13591
Berapa nilai checksum yang didapat dari header pada paket nomor 130?
Your answer: 0x18e5
Correct answer!
Here is your flag: Jarkom2023{ch3cksum_is_u5eful_0x16e3}
```

Flag: Jarkom2023{ch3cksum_is_u5eful_0xo7y4}

5. Cari password untuk file soal

No.	Time	Source	Destination	Protocol	Length	Info
13	1.761484	74.53.140.153	10.10.1.4	SMTP	72	S: 334 UGFzc3dvcmQ6
14	1.762058	10.10.1.4	74.53.140.153	SMTP	72	C: Pass: cHVuamFiQDEyMw==
15	2.121738	74.53.140.153	10.10.1.4	SMTP	84	S: 235 Authentication succeeded

Decode Base64

```
CONNECT TO THIS INSTANCE TO ANSWER THE QUESTION :D
nc 10.21.78.111 11111
```


Vidiawan Nabiel Arrasyid

5025221231

Jarkom E

Isi File

Connect dengan: **ncat 10.21.78.111. 11111**

14	1.762058	10.10.1.4	74.53.140.153	SMTP	72 C: Pass: cHVuamFiQDEyMw==
<div>> Frame 14: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) > Ethernet II, Src: CradlePo_3c:17:c2 (00:e0:1c:3c:17:c2), Dst: Netgear_d9:81:60 (00:1f:33:d9:81:60) > Internet Protocol Version 4, Src: 10.10.1.4, Dst: 74.53.140.153 ✓ Transmission Control Protocol, Src Port: 1470, Dst Port: 25, Seq: 52, Ack: 355, Len: 18 Source Port: 1470 Destination Port: 25</div>					

a. Berapa banyak packet yang berhasil di capture dari file pcap tersebut?

Your answer: **60**

b. Port berapakah pada server yang digunakan untuk service SMTP?

Your answer: **25**

c. Dari semua alamat IP yang tercapture, IP berapakah yang merupakan public IP?

Your answer: **74.53.140.153**

```
PS C:\Users\nabie> ncat 10.21.78.111 11111
a. Berapa banyak packet yang berhasil di capture dari file pcap tersebut?
Your answer: 60
Correct answer!
b. Port berapakah pada server yang digunakan untuk service SMTP?
Your answer: 25
Correct answer!
c. Dari semua alamat IP yang tercapture, IP berapakah yang merupakan public IP?
Your answer: 74.53.140.153
Correct answer!
Correct answers, you are good at analysis!
Here is your flag: Jarkom2023{k0w4lski_9577_BimjkREwERA_4nalysis}
```

Flag: Jarkom2023{k0w4lski_9619_kAyAPFmjDzQ_4nalysis}

6. ncat 10.21.78.111 6666

PESAN TERSEMBUNYI

Seorang anak bernama Udin Berteman dengan Slamet yang merupakan seorang penggemar film detektif. sebagai teman yang baik, Ia selalu mengajak slamet untuk bermain valoranT bersama. suatu malam, terjadi sebuah hal yang tak terduga. ketika udin mereka membuka game tersebut, laptop udin menunjukkan sebuah field text dan Sebuah kode Invalid bertuliskan "server SOURCE ADDRESS 7812 is invalid". ketika ditelusuri di google, hasil pencarian hanya menampilkan a1 e5 u21. jiwa detektif slamet pun bergejolak. bantulah udin dan slamet untuk menemukan solusi kode error tersebut.

"SUBSTITUSI" -> Kapital

Vidiawan Nabiel Arrasyid
5025221231
Jarkom E

▼ View Hint

Clue 1: Sepertinya ada yang salah dengan penulisan tersebut secara KBBI. Ada sesuatu yang Besar di depan mata.

▼ View Hint

Jenis cipher merupakan substitusi a1z26 Cipher

▼ View Hint

Rentang Huruf yang digunakan Huruf A-R, 1-18 dengan Jawaban 6 Huruf.

▼ View Hint

SOURCE ADDRESS ADALAH KUNCI SEMUANYA.

No.	Time	Source
7812	454.073930	104.18.14.101

Seorang anak bernama **Udin Berteman** dengan **Slamet** yang merupakan seorang penggemar film detektif. sebagai **Teman** yang baik, Ia selalu mengajak slamet untuk bermain valorant bersama. suatu malam, Terjadi sebuah hal yang tak terduga. ketika **Udin** mereka membuka game tersebut, laptop udin menunjukkan sebuah field text dan aSebuah kode Invalid bertuliskan "server SOURCE ADDRESS 7812 is invalid".

ketika ditelusuri di google, hasil pencarian hanya menampilkan a1 e5 u21. jiwa detektif slamet pun bergejolak.

bantulah udin dan slamet untuk menemukan solusi kode error tersebut.

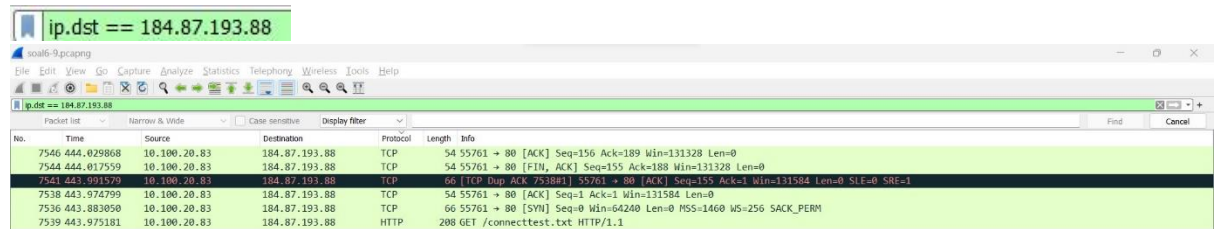
➔ **104.18.14.101** ➔ **0-18** ➔ **10 4 18 14 10 1** ➔ **J D R N J A**

Your answer: **JDRNJA**

```
PS C:\Users\nabie> ncat 10.21.78.111 6666
Seorang anak bernama Udin Berteman dengan Slamet yang merupakan seorang penggemar film detektif.
sebagai Teman yang baik, Ia selalu mengajak slamet untuk bermain valorant bersama. suatu malam, Terjadi sebuah hal yang
tak terduga.
ketika Udin mereka membuka game tersebut, laptop udin menunjukkan sebuah field text dan Sebuah kode Invalid bertuliskan
"server SOURCE ADDRESS 7812 is invalid".
ketika ditelusuri di google, hasil pencarian hanya menampilkan a1 e5 u21.
iwa detektif slamet pun bergejolak.
bantulah udin dan slamet untuk menemukan solusi kode error tersebut.
Your answer: JDRNJA
Correct answer!
Here is your flag: Jarkom2023{h3h3_ctf_d1k1t_a0M64A0DNKC58638F7kx}
```

Flag: Jarkom2023{h3h3_ctf_d1k1t_a0GO675X225VW71QZ7kx}

7. ncat 10.21.78.111 6565



No.	Time	Source	Destination	Protocol	Length	Info
7546	444.029808	10.100.20.83	184.87.193.88	TCP	54	55761 → 80 [ACK] Seq=156 Ack=189 Win=131328 Len=0
7544	444.017559	10.100.20.83	184.87.193.88	TCP	54	55761 → 80 [FIN, ACK] Seq=155 Ack=188 Win=131328 Len=0
7547	443.901572	10.100.20.83	184.87.193.88	TCP	60	55761 → 80 [ACK] Seq=155 Ack=188 Win=131328 Len=0
7538	443.974799	10.100.20.83	184.87.193.88	TCP	54	55761 → 80 [ACK] Seq=155 Ack=188 Win=131328 Len=0
7536	443.883050	10.100.20.83	184.87.193.88	TCP	66	55761 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7539	443.975181	10.100.20.83	184.87.193.88	HTTP	208	GET /connecttest.txt HTTP/1.1

Berapa jumlah packet yang menuju IP 184.87.193.88?

Your answer: 6

```
PS C:\Users\nabie> ncat 10.21.78.111 6565
Berapa jumlah packet yang menuju IP 184.87.193.88?
Your answer: 6
Correct answer!
Here is your flag: Jarkom2023{8Nvw8lA83HRN2C9HeA_4n0th3r_f1lt3ring}
```

Flag: Jarkom2023{c94ERFV5EG9Rgy2Oa0_4n0th3r_f1lt3ring}

8. ncat 10.21.78.111 7171

Berikan kueri filter sehingga wireshark hanya mengambil semua protokol paket yang menuju port 80! (Jika terdapat lebih dari 1 port, maka urutkan sesuai dengan abjad)

Your answer: `tcp.dstport == 80 || udp.dstport == 80`

```
PS C:\Users\nabie> ncat 10.21.78.111 7171
Berikan kueri filter sehingga wireshark hanya mengambil semua protokol paket yang menuju port 80! (Jika terdapat lebih d
ari 1 port, maka urutkan sesuai dengan abjad)
Your answer: tcp.dstport == 80 || udp.dstport == 80
Correct answer!
Here is your flag: Jarkom2023{qu3ryyyyying_760109_QgQiFh0tQwR_15_fun}
```

Flag: Jarkom2023{qu3ryyyyying_998893_AzNwFxEHduO_15_fun}

9. ncat 10.21.78.111 7272

Berikan kueri filter sehingga wireshark hanya mengambil paket yang berasal dari alamat 10.51.40.1 tetapi tidak menuju ke alamat 10.39.55.34!

Your answer: `ip.src == 10.51.40.1 && ip.dst != 10.39.55.34`

```
PS C:\Users\nabie> ncat 10.21.78.111 7272
Berikan kueri filter sehingga wireshark hanya mengambil paket yang berasal dari alamat 10.51.40.1 tetapi tidak menuju ke
alamat 10.39.55.34!
Your answer: ip.src == 10.51.40.1 && ip.dst != 10.39.55.34
Correct answer!
Here is your flag: Jarkom2023{y3s_its_PhNhNk0jNiQ_qu3ry1ng}
```

Flag: Jarkom2023{y3s_its_RkOkNkNINmO_qu3ry1ng}

10. ncat 10.21.78.111 7373

81 19.343911022	172.16.0.254	172.16.0.4	TELNET	91 Telnet Data ...
> Frame 81: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface tap2, id 0 > Ethernet II, Src: 26:82:4f:e4:c2:07 (26:82:4f:e4:c2:07), Dst: 0c:c8:32:27:00:00 (0c:c8:32:27:00:00) > Internet Protocol Version 4, Src: 172.16.0.254, Dst: 172.16.0.4 > Transmission Control Protocol, Src Port: 57784, Dst Port: 23, Seq: 1, Ack: 13, Len: 25 > Telnet				
Data: dhafin:kesayangannyak0k0\n				

Sebutkan kredensial yang benar ketika user mencoba login menggunakan Telnet, format [username]:[password]!

Your answer: `dhafin:kesayangannyak0k0`

```
PS C:\Users\nabie> ncat 10.21.78.111 7373
Sebutkan kredensial yang benar ketika user mencoba login menggunakan Telnet, format [username]:[password]!
Your answer: dhafin:kesayangannyak0k0
Correct answer!
Here is your flag: Jarkom2023{t3lnet_is_C78B1zB4CyyCyy38A_N0tSecu2e}
```

Flag: Jarkom2023{t3lnet_is_017x3AzyABCCB2zz0_N0tSecu2e}