

## אבטחת נתונים – עבודת הגשה 6

מגישות:

צליל לוי – 206796088

לינוי אסלן – 313279036

שורת הרצה של hping3 :

```
user@infosec: ~  
File Edit Tabs Help  
user@infosec:~$ sudo hping3 -c 1 -R -p 23 -s 50874 -M 1699597593 localhost  
[sudo] password for user:  
HPING localhost (lo 127.0.0.1): R set, 40 headers + 0 data bytes  
  
--- localhost hping statistic ---  
1 packets transmitted, 0 packets received, 100% packet loss  
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

ניתן לראות שלאחר הרצת פקודה זו, התבצע ניתוק הקשר בין הלקוח לשרת:

```
user@infosec: ~  
File Edit Tabs Help  
* Documentation: https://help.ubuntu.com  
* Management: https://landscape.canonical.com  
* Support: https://ubuntu.com/advantage  
  
* Super-optimized for small spaces - read how we shrank the memory  
  footprint of MicroK8s to make it the smallest full K8s around.  
  
https://ubuntu.com/blog/microk8s-memory-optimisation  
  
* Canonical Livepatch is available for installation.  
  - Reduce system reboots and improve kernel security. Activate at:  
    https://ubuntu.com/livepatch  
  
353 packages can be updated.  
272 updates are security updates.  
  
New release '20.04.2 LTS' available.  
Run 'do-release-upgrade' to upgrade to it.  
  
user@infosec:~$ pwd  
/home/user  
user@infosec:~$ Connection closed by foreign host.  
user@infosec:~$ w
```

(המשך בעמוד הבא)

The screenshot displays the Wireshark network protocol analyzer interface. At the top, the menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and packet analysis. The main window is divided into three panes. The top pane, 'Packet List', shows a list of captured packets. Packet 132 is selected, which is a TCP segment from 127.0.0.1 to 127.0.0.1, port 50874 to 23, with sequence number 1699597593 and acknowledgment number 497579257. The middle pane, 'Packet Details', shows the hierarchical structure of the selected packet: Frame 132 (68 bytes on wire, 68 bytes captured on interface 0), Linux cooked capture, Internet Protocol Version 4 (Src: 127.0.0.1, Dst: 127.0.0.1), and Transmission Control Protocol (Src Port: 50874, Dst Port: 23, Seq: 1699597593, Ack: 497579257, Len: 0). The bottom pane, 'Packet Bytes', shows the raw data in hexadecimal and ASCII. The ASCII column shows the text 'E..4.40..@.v}...' and 'eM...t..'. The status bar at the bottom indicates 'Wireshark · Packet 132 · any'.

No.	Time	Source	Destination	Protocol	Length	Info
123	8.563203325	127.0.0.1	127.0.0.1	TCP	68	50874 → 23 [ACK] Seq=1699597589 Ack=497579179 Win=65536 Len=0 TSval=3804487764 TSecr=3804487764
124	8.731163146	127.0.0.1	127.0.0.1	TELNET	69	Telnet Data ...
126	8.731281707	127.0.0.1	127.0.0.1	TCP	68	50874 → 23 [ACK] Seq=1699597590 Ack=497579180 Win=65536 Len=0 TSval=3804487932 TSecr=3804487932
127	9.482600767	127.0.0.1	127.0.0.1	TELNET	69	Telnet Data ...
129	9.482736375	127.0.0.1	127.0.0.1	TCP	68	50874 → 23 [ACK] Seq=1699597591 Ack=497579181 Win=65536 Len=0 TSval=3804488683 TSecr=3804488683
130	10.274483654	127.0.0.1	127.0.0.1	TELNET	70	Telnet Data ...
132	10.274699815	127.0.0.1	127.0.0.1	TCP	68	50874 → 23 [ACK] Seq=1699597593 Ack=497579257 Win=65536 Len=0 TSval=3804489475 TSecr=3804489475

Wireshark · Packet 132 · any

▶ Frame 132: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0  
 ▶ Linux cooked capture  
 ▶ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1  
 ▼ Transmission Control Protocol, Src Port: 50874, Dst Port: 23, Seq: 1699597593, Ack: 497579257, Len: 0  
   Source Port: 50874  
   Destination Port: 23  
   [Stream index: 1]  
   [TCP Segment Len: 0]  
   Sequence number: 1699597593  
   [Next sequence number: 1699597593]  
   Acknowledgment number: 497579257  
   1000 .... = Header Length: 32 bytes (8)  
   ▶ Flags: 0x010 (ACK)  
   Window size value: 512  
   [Calculated window size: 65536]  
   [Window size scaling factor: 128]

0000 00 00 03 04 00 06 00 00 00 00 00 00 00 00 00 08 00 .....  
 0010 45 10 00 34 c6 34 40 00 40 06 76 7d 7f 00 00 01 E..4.40..@.v}....  
 0020 7f 00 00 01 c6 ba 00 17 65 4d cd 19 1d a8 74 f9 .....eM...t..  
 0030 08 10 02 00 fe 28 00 00 01 01 08 0a e2 c3 e7 03 .....(  
 0040 e2 c3 e7 03 .....  
 .....

Wireshark packet capture showing a TCP RST packet. The packet list shows packet 133 as a RST from 127.0.0.1 to 127.0.0.1 on port 23. The packet details show the RST flag set and the sequence number 1699597593. The packet bytes show the raw data.

No.	Time	Source	Destination	Protocol	Length	Info
123	8.563203325	127.0.0.1	127.0.0.1	TCP	68	50874 → 23 [ACK] Seq=1699597589 Ack=497579179 Win=65536 Len=0 TSval=3804487764 TSecr=3804487764
124	8.731163146	127.0.0.1	127.0.0.1	TELNET	69	Telnet Data ...
126	8.731281707	127.0.0.1	127.0.0.1	TCP	68	50874 → 23 [ACK] Seq=1699597590 Ack=497579180 Win=65536 Len=0 TSval=3804487932 TSecr=3804487932
127	9.482600767	127.0.0.1	127.0.0.1	TELNET	69	Telnet Data ...
129	9.482736375	127.0.0.1	127.0.0.1	TCP	68	50874 → 23 [ACK] Seq=1699597591 Ack=497579181 Win=65536 Len=0 TSval=3804488683 TSecr=3804488683
130	10.274483654	127.0.0.1	127.0.0.1	TELNET	70	Telnet Data ...
132	10.274699815	127.0.0.1	127.0.0.1	TCP	68	50874 → 23 [ACK] Seq=1699597593 Ack=497579257 Win=65536 Len=0 TSval=3804489475 TSecr=3804489475
133	96.762885110	127.0.0.1	127.0.0.1	TCP	56	50874 → 23 [RST] Seq=1699597593 Win=65536 Len=0

Wireshark · Packet 133 · any

- ▶ Frame 133: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface 0
- ▶ Linux cooked capture
- ▶ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
- ▼ **Transmission Control Protocol, Src Port: 50874, Dst Port: 23, Seq: 1699597593, Len: 0**
  - Source Port: 50874
  - Destination Port: 23
  - [Stream index: 1]
  - [TCP Segment Len: 0]
  - Sequence number: 1699597593
  - [Next sequence number: 1699597593]
  - ▶ **Acknowledgment number: 1161580653**
  - 0101 .... = Header Length: 20 bytes (5)
  - ▶ **Flags: 0x004 (RST)**
  - Window size value: 512
  - [Calculated window size: 65536]
  - [Window size scaling factor: 128]
  - Checksum: 0x20fc [unverified]
  - [Checksum Status: Unverified]

```

0000  00 00 03 04 00 06 00 00 00 00 00 00 08 00 08 00  .....E...
0010  45 00 00 28 85 05 00 00 40 06 f7 c8 7f 00 00 01  E...@...
0020  7f 00 00 01 c6 ba 00 17 65 4d cd 19 45 3c 50 6d  .....eM..E<Pm
0030  50 04 02 00 20 fc 00 00                                P.....
  
```