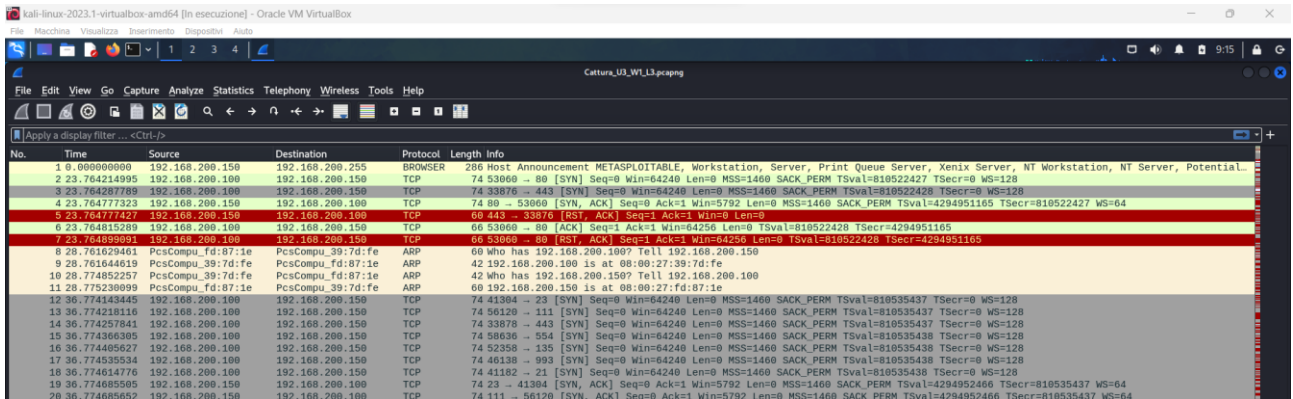


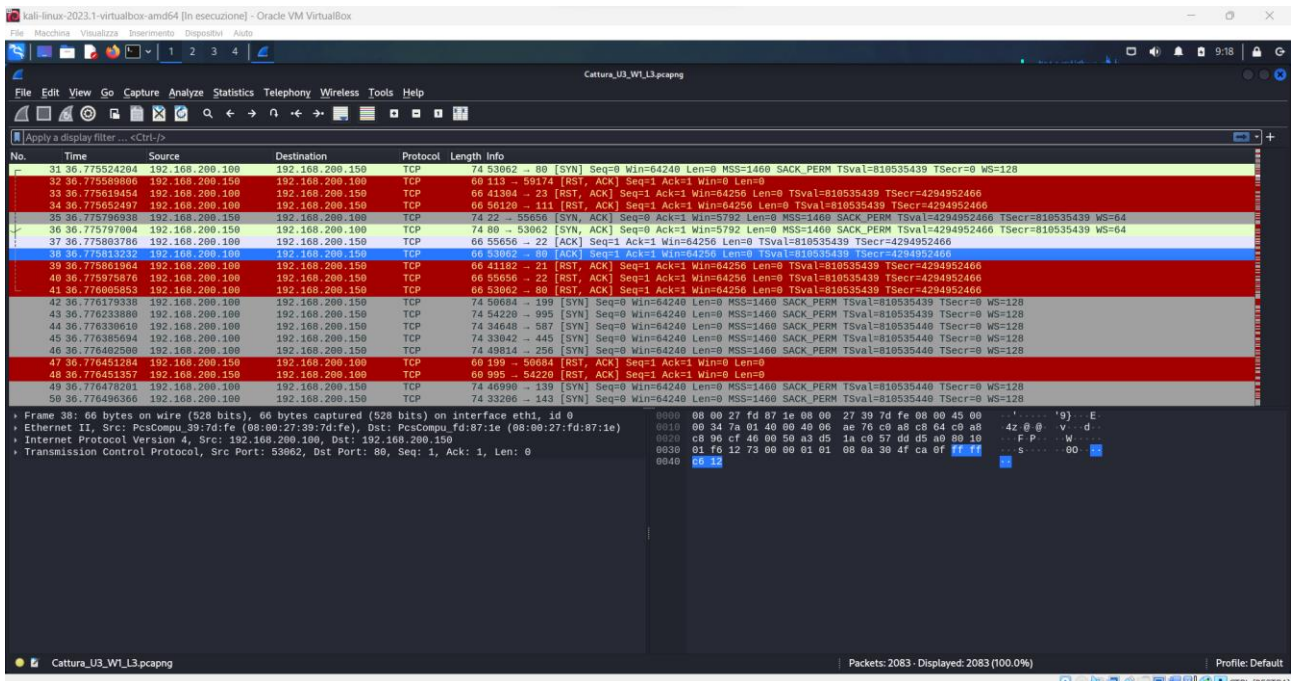
Epicode Unit 3 Day 3

L'esercizio odierno prevede lo studio di una scansione eseguita con Wireshark per individuare eventuali IoC sulla macchina scelta come bersaglio dell'attacco (Metasploitable).



No.	Time	Source	Destination	Protocol	Length	Info
10	0.000000000	192.168.200.150	192.168.200.255	BROWSER	286	Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Potential...
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522427 TSecr=0 WS=128
3	23.764297785	192.168.200.100	192.168.200.150	TCP	74	53076 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522428 TSecr=0 WS=128
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 → 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294951165 TSecr=810522427 WS=64
5	23.764777427	192.168.200.150	192.168.200.100	TCP	60	443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
7	23.764859451	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
8	23.761624861	PcsCompu, fd:87:1e	PcsCompu, 39:7d:fe	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PcsCompu, 39:7d:fe	PcsCompu, fd:87:1e	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	PcsCompu, 39:7d:fe	PcsCompu, fd:87:1e	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	28.775238999	PcsCompu, fd:87:1e	PcsCompu, 39:7d:fe	ARP	60	192.168.200.150 is at 08:00:27:fd:87:1e
12	36.774543445	192.168.200.100	192.168.200.150	TCP	74	41304 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
13	36.774218116	192.168.200.100	192.168.200.150	TCP	74	56120 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
14	36.774257841	192.168.200.100	192.168.200.150	TCP	74	53878 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
15	36.774366305	192.168.200.100	192.168.200.150	TCP	74	50836 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
16	36.774460527	192.168.200.100	192.168.200.150	TCP	74	52358 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
17	36.774535534	192.168.200.100	192.168.200.150	TCP	74	46138 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
18	36.774614776	192.168.200.100	192.168.200.150	TCP	74	41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
19	36.774655505	192.168.200.150	192.168.200.100	TCP	74	23 → 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
20	36.774659552	192.168.200.150	192.168.200.100	TCP	74	111 → 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64

Come si può notare dallo screen, una volta conclusa la fase di richieste ARP che andrà a mettere in comunicazione le due macchine (verosimilmente su rete interna), dalla macchina attaccante inizia una serie di richieste con Protocollo TCP che però non vanno a concludere il three-way-handshake.



No.	Time	Source	Destination	Protocol	Length	Info
31	36.775524204	192.168.200.100	192.168.200.150	TCP	74	53062 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
32	36.775589806	192.168.200.150	192.168.200.100	TCP	60	113 → 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	36.775619454	192.168.200.100	192.168.200.150	TCP	66	41304 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
34	36.775652497	192.168.200.100	192.168.200.150	TCP	66	56120 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
35	36.775796938	192.168.200.150	192.168.200.100	TCP	74	22 → 55656 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
36	36.775797004	192.168.200.150	192.168.200.100	TCP	74	80 → 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
37	36.775839760	192.168.200.100	192.168.200.150	TCP	66	55656 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
38	36.775913232	192.168.200.100	192.168.200.150	TCP	66	53062 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
39	36.775961964	192.168.200.150	192.168.200.100	TCP	66	41182 → 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
40	36.775975876	192.168.200.100	192.168.200.150	TCP	66	55656 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
41	36.776059853	192.168.200.100	192.168.200.150	TCP	66	53062 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
42	36.776179335	192.168.200.100	192.168.200.150	TCP	74	50864 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
43	36.776233880	192.168.200.100	192.168.200.150	TCP	74	54220 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
44	36.776339610	192.168.200.100	192.168.200.150	TCP	74	34648 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
45	36.776385494	192.168.200.100	192.168.200.150	TCP	74	33042 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
46	36.776402580	192.168.200.100	192.168.200.150	TCP	74	49814 → 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
47	36.776451284	192.168.200.150	192.168.200.100	TCP	60	199 → 50684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
48	36.776451357	192.168.200.150	192.168.200.100	TCP	60	995 → 54220 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
49	36.776476201	192.168.200.100	192.168.200.150	TCP	74	46099 → 133 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
50	36.776496366	192.168.200.100	192.168.200.150	TCP	74	33265 → 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128

Frame 46: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth1, id 0
Ethernet II, Src: PcsCompu, 39:7d:fe (08:00:27:39:7d:fe), Dst: PcsCompu, fd:87:1e (08:00:27:fd:87:1e)
Internet Protocol Version 4, Src: 192.168.200.100, Dst: 192.168.200.150
Transmission Control Protocol, Src Port: 53062, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

Andando inoltre ad analizzare i pacchetti nel dettaglio possiamo verificare come moltissime porte (se non tutte) vengano prese “di mira” dalle richieste della macchina attaccante.

Alla luce di ciò possiamo supporre di aver intercettato una scansione di tipo “stealth” probabilmente eseguita da un tool come Nmap (se non proprio Nmap) per andare ad identificare le porte aperte sulla macchina bersaglio, probabilmente per andare poi a verificarne e sfruttarne successivamente le vulnerabilità.

Potenziamenti azioni di rimedio:

Considerando le valutazioni precedentemente fatte, possiamo mitigare la minaccia in diversi modi:

- Blocco dell’Indirizzo IP da cui arrivano le richieste;
- Chiusura delle porte della macchina bersaglio sulle quali non “girano” servizi necessari per l’utente;
- Impostazione di una policy “DROP” dei pacchetti tramite una regola firewall;
- Eventuali aggiornamenti (patch) di servizi vulnerabili qualora possibile;
- Implementazione di un IDS per un eventuale “Double-Check” dei dati analizzati con Wireshark;
- Implementazione di un IPS per il blocco automatico dei pacchetti (più efficace in teoria che in pratica, vista la probabilità di “falsi positivi”).

Controlli aggiuntivi:

Qualora si decidesse di effettuare ulteriori controlli di Cross-Check per una maggiore sicurezza sull’affidabilità dei dati, si potrebbe inoltre decidere di utilizzare un secondo software di analisi, come ad esempio, per citarne soltanto uno, netsniff-ng.

```
There is NO WARRANTY, to the extent permitted by law.  
[kali@kali]~  
$ sudo netsniff-ng -i eth0 --out /home/kali/Desktop/capture-eth0.pcap  
[sudo] password for kali:  
Running! Hang up with ^C!
```

Una volta avviato il tool, avvio una scansione di tipo -sS su nmap per riprodurre le condizioni dell’attacco. Con il comando sopra mostrato, non solo saremo in grado di visualizzare il traffico da terminale, bensì anche di consultarlo ogniqualvolta si vorrà sia da Desktop, sia da altri tool, come lo stesso Wireshark.

```

< eth0 60 1687960440s.769682562ns #44970
[ Eth MAC (08:00:27:98:12:f6 => 08:00:27:c7:e1:36), Proto (0x0800, IPv4) ]
[ Vendor (PCS Systemtechnik GmbH => PCS Systemtechnik GmbH) ]
[ Eth trailer 0003c00 ]
[ IPv4 Addr (192.168.240.120 => 192.168.240.100), Proto (6), TTL (64), TOS (0), Ver (4), IHL (5), Tlen (40), ID (0), Res (0), NoFrag (1), MoreFrag (0), FragOff (0), CSum (0xd8a1) is ok ]
[ TCP Port (14017 => 38121), SN (0x0), AN (0x18a06373), DataOff (5), Res (0), Flags (RSTACK), Window (0), CSum (0x05e4), UrgPtr (0) ]

< eth0 60 1687960440s.769682607ns #44971
[ Eth MAC (08:00:27:98:12:f6 => 08:00:27:c7:e1:36), Proto (0x0800, IPv4) ]
[ Vendor (PCS Systemtechnik GmbH => PCS Systemtechnik GmbH) ]
[ Eth trailer 0003c00 ]
[ IPv4 Addr (192.168.240.120 => 192.168.240.100), Proto (6), TTL (64), TOS (0), Ver (4), IHL (5), Tlen (40), ID (0), Res (0), NoFrag (1), MoreFrag (0), FragOff (0), CSum (0xd8a1) is ok ]
[ TCP Port (12014 => 38121), SN (0x0), AN (0x18a06373), DataOff (5), Res (0), Flags (RSTACK), Window (0), CSum (0x0db7), UrgPtr (0) ]

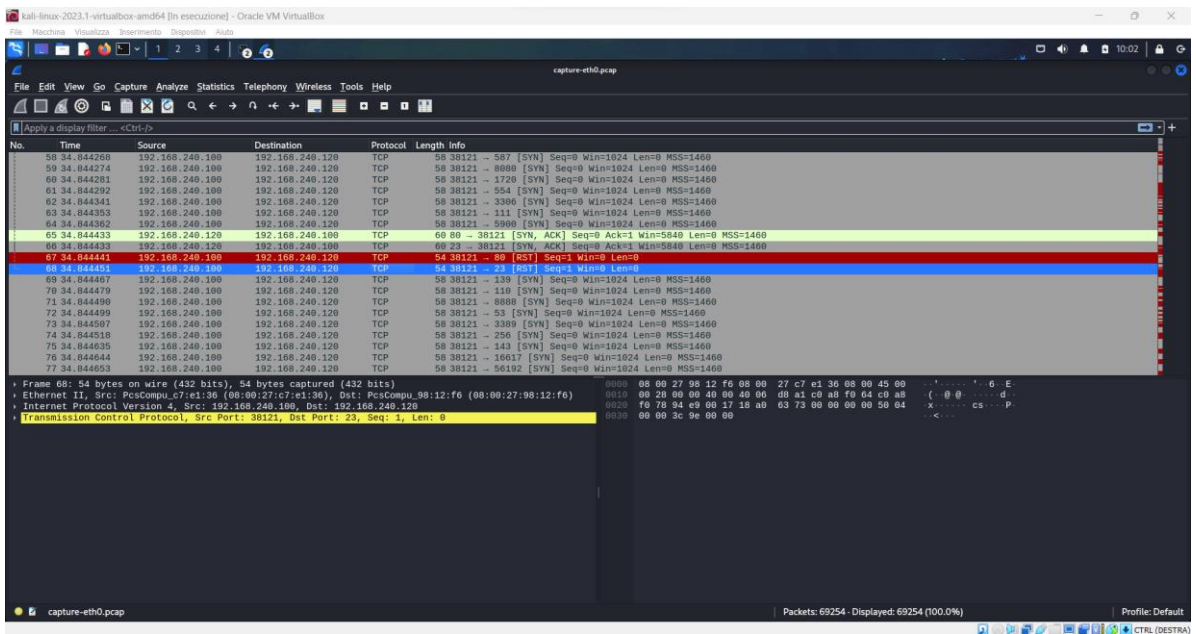
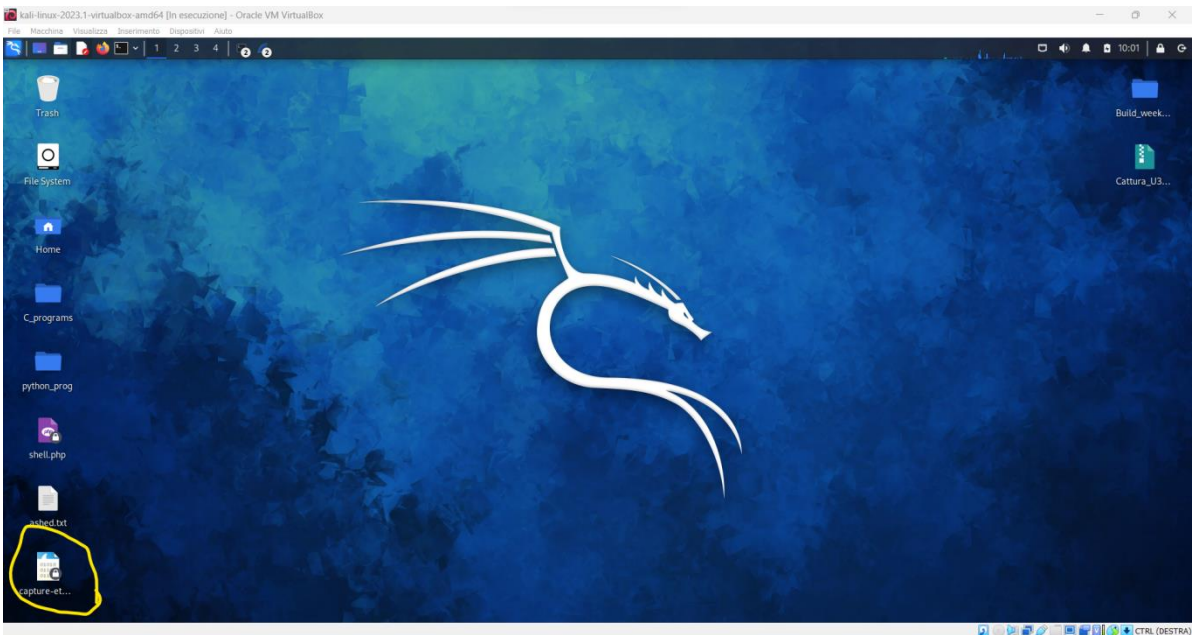
< eth0 60 1687960440s.769682659ns #44972
[ Eth MAC (08:00:27:98:12:f6 => 08:00:27:c7:e1:36), Proto (0x0800, IPv4) ]
[ Vendor (PCS Systemtechnik GmbH => PCS Systemtechnik GmbH) ]
[ Eth trailer 0003c00 ]
[ IPv4 Addr (192.168.240.120 => 192.168.240.100), Proto (6), TTL (64), TOS (0), Ver (4), IHL (5), Tlen (40), ID (0), Res (0), NoFrag (1), MoreFrag (0), FragOff (0), CSum (0xd8a1) is ok ]
[ TCP Port (46701 => 38121), SN (0x0), AN (0x18a06373), DataOff (5), Res (0), Flags (RSTACK), Window (0), CSum (0x8637), UrgPtr (0) ]

< eth0 60 1687960440s.769682711ns #44973
[ Eth MAC (08:00:27:98:12:f6 => 08:00:27:c7:e1:36), Proto (0x0800, IPv4) ]
[ Vendor (PCS Systemtechnik GmbH => PCS Systemtechnik GmbH) ]
[ Eth trailer 0003c00 ]
[ IPv4 Addr (192.168.240.120 => 192.168.240.100), Proto (6), TTL (64), TOS (0), Ver (4), IHL (5), Tlen (40), ID (0), Res (0), NoFrag (1), MoreFrag (0), FragOff (0), CSum (0xd8a1) is ok ]
[ TCP Port (42528 => 38121), SN (0x0), AN (0x18a06373), DataOff (5), Res (0), Flags (RSTACK), Window (0), CSum (0x968a), UrgPtr (0) ]

< eth0 60 1687960440s.769682760ns #44974
[ Eth MAC (08:00:27:98:12:f6 => 08:00:27:c7:e1:36), Proto (0x0800, IPv4) ]
[ Vendor (PCS Systemtechnik GmbH => PCS Systemtechnik GmbH) ]
[ Eth trailer 0003c00 ]
[ IPv4 Addr (192.168.240.120 => 192.168.240.100), Proto (6), TTL (64), TOS (0), Ver (4), IHL (5), Tlen (40), ID (0), Res (0), NoFrag (1), MoreFrag (0), FragOff (0), CSum (0xd8a1) is ok ]
[ TCP Port (4313 => 38121), SN (0x0), AN (0x18a06373), DataOff (5), Res (0), Flags (RSTACK), Window (0), CSum (0x2bcc), UrgPtr (0) ]

< eth0 60 1687960440s.769682805ns #44975
[ Eth MAC (08:00:27:98:12:f6 => 08:00:27:c7:e1:36), Proto (0x0800, IPv4) ]
[ Vendor (PCS Systemtechnik GmbH => PCS Systemtechnik GmbH) ]
[ Eth trailer 0003a00 ]
[ IPv4 Addr (192.168.240.120 => 192.168.240.100), Proto (6), TTL (64), TOS (0), Ver (4), IHL (5), Tlen (40), ID (0), Res (0), NoFrag (1), MoreFrag (0), FragOff (0), CSum (0xd8a1) is ok ]
[ TCP Port (16008 => 38121), SN (0x0), AN (0x18a06373), DataOff (5), Res (0), Flags (RSTACK), Window (0), CSum (0xfe1c), UrgPtr (0) ]

```



Come possiamo notare dagli screen soprastanti, anche in questo caso notiamo come le richieste TCP non completino il three-way-handshake, confermando l'ipotesi di scansione Stealth inizialmente proposta.