Μάριος Γαβριήλ ΑΜ:4244 Μηνάς Ελευθερίου ΑΜ:4245

Ασφάλεια Υπολογιστικών και Επικοινωνιακών Συστημάτων – Άσκηση 2

1. Αρχικά συνδεόμαστε με κανονικό ssh από την c1 στην c2

```
root@c1:~# ssh 192.168.122.57
The authenticity of host '192.168.122.57 (192.168.122.57)' can't be established.
ECDSA key fingerprint is SHA256:+s/kPSH9lh/ermEoYpNy2S9HCiSQIa2BOVz3OSq4Aws.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.122.57' (ECDSA) to the list of known hosts.
root@192.168.122.57's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Dec  9 14:44:12 2021 from 192.168.122.1
root@c2:~#
```

2. Ξεκινάμε το Ettercap από την mye007 και επιλέγουμε sniff και μετά Unified Sniffing και σαν network interface επιλέγουμε την virbr0. Μετά επιλέγουμε Hosts και κάνουμε scan for hosts. Από το Hosts επιλέγουμε το Hosts list και βλέπουμε τα δύο θύματα c1 και c2 οπού τα επιλέγουμε και ανάλογα τα βαζούμε ως Target 1 και Target 2. Τέλος επιλέγουμε Mitm και μετά arp poisoning και από τα optional parameters επιλέγουμε sniff remote connections και μετά ok.

```
272 179.166063000  192.168.122.57   192.168.122.105  ICMP  42 Echo (ping) request  id=0x7ee7, seq=32487/59262, ttl=64 (reply in 273)
273 179.166108000  192.168.122.105  192.168.122.57   ICMP  42 Echo (ping) reply    id=0x7ee7, seq=32487/59262, ttl=64 (request in 272)
274 179.166739000  192.168.122.105  192.168.122.57   ICMP  42 Echo (ping) request  id=0x7ee7, seq=32487/59262, ttl=64 (reply in 275)
275 179.166763000  192.168.122.57   192.168.122.105  ICMP  42 Echo (ping) reply    id=0x7ee7, seq=32487/59262, ttl=64 (request in 274)
276 179.166786000  fe:5d:35:4b:52:7b  00:ff:aa:90:af:3d  ARP  42 192.168.122.57 is at fe:5d:35:4b:52:7b
277 179.166796000  fe:5d:35:4b:52:7b  Xensourc_9f:1f:32  ARP  42 192.168.122.105 is at fe:5d:35:4b:52:7b
278 180.184037000  fe:5d:35:4b:52:7b  00:ff:aa:90:af:3d  ARP  42 192.168.122.57 is at fe:5d:35:4b:52:7b
279 180.184064000  fe:5d:35:4b:52:7b  Xensourc_9f:1f:32  ARP  42 192.168.122.105 is at fe:5d:35:4b:52:7b
280 181.204612000  fe:5d:35:4b:52:7b  00:ff:aa:90:af:3d  ARP  42 192.168.122.57 is at fe:5d:35:4b:52:7b
281 181.204638000  fe:5d:35:4b:52:7b  Xensourc_9f:1f:32  ARP  42 192.168.122.105 is at fe:5d:35:4b:52:7b
282 182.221474000  fe:5d:35:4b:52:7b  00:ff:aa:90:af:3d  ARP  42 192.168.122.57 is at fe:5d:35:4b:52:7b
283 182.221513000  fe:5d:35:4b:52:7b  Xensourc_9f:1f:32  ARP  42 192.168.122.105 is at fe:5d:35:4b:52:7b
284 183.246908000  fe:5d:35:4b:52:7b  00:ff:aa:90:af:3d  ARP  42 192.168.122.57 is at fe:5d:35:4b:52:7b
285 183.246934000  fe:5d:35:4b:52:7b  Xensourc_9f:1f:32  ARP  42 192.168.122.105 is at fe:5d:35:4b:52:7b
286 193.274675000  fe:5d:35:4b:52:7b  00:ff:aa:90:af:3d  ARP  42 192.168.122.57 is at fe:5d:35:4b:52:7b
287 193.274714000  fe:5d:35:4b:52:7b  Xensourc_9f:1f:32  ARP  42 192.168.122.105 is at fe:5d:35:4b:52:7b
288 203.302743000  fe:5d:35:4b:52:7b  00:ff:aa:90:af:3d  ARP  42 192.168.122.57 is at fe:5d:35:4b:52:7b
289 203.302772000  fe:5d:35:4b:52:7b  Xensourc_9f:1f:32  ARP  42 192.168.122.105 is at fe:5d:35:4b:52:7b
290 213.324814000  fe:5d:35:4b:52:7b  00:ff:aa:90:af:3d  ARP  42 192.168.122.57 is at fe:5d:35:4b:52:7b
291 213.324854000  fe:5d:35:4b:52:7b  Xensourc_9f:1f:32  ARP  42 192.168.122.105 is at fe:5d:35:4b:52:7b
292 223.347981000  fe:5d:35:4b:52:7b  00:ff:aa:90:af:3d  ARP  42 192.168.122.57 is at fe:5d:35:4b:52:7b
293 223.348021000  fe:5d:35:4b:52:7b  Xensourc_9f:1f:32  ARP  42 192.168.122.105 is at fe:5d:35:4b:52:7b
294 233.367202000  fe:5d:35:4b:52:7b  00:ff:aa:90:af:3d  ARP  42 192.168.122.57 is at fe:5d:35:4b:52:7b
295 233.367228000  fe:5d:35:4b:52:7b  Xensourc_9f:1f:32  ARP  42 192.168.122.105 is at fe:5d:35:4b:52:7b
```

Στην γραμμή 276 παρατηρούμε ότι η IP στο 192.168.122.57 βρίσκεται στην mac fe:5d:35:4b:52:7b η οποία είναι η mac του mye007. Επίσης βλέπουμε ότι η IP στο 192.168.122.57 βρίσκεται στην mac fe:5d:35:4b:52:7b η οποία είναι η mac του mye007. Αρά επιβεβαιώνουμε οτί ο mye007 φαινέται ως c2 στην c1 και ως c1 στην c2.

Μάριος Γαβριήλ ΑΜ:4244 Μηνάς Ελευθερίου ΑΜ:4245

3. Προσπαθώντας να συνδεθούμε με ssh από την c1 στην c2 παρατηρούμε τα έξεις στο wireshark

324	344.875800000	192.168.122.105	192.168.122.57	TCP	74 60221→22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=346546 TSecr=0 WS=128
325	344.878061000	192.168.122.105	192.168.122.57	TCP	74 [TCP Out-Of-Order] 60221→22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=346546 TSecr=0 WS=128
326	345.873866000	192.168.122.105	192.168.122.57	TCP	74 [TCP Retransmission] 60221→22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=346796 TSecr=0 WS=128
327	345.878979000	192.168.122.105	192.168.122.57	TCP	74 [TCP Retransmission] 60221→22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=346796 TSecr=0 WS=128
328	347.878189000	192.168.122.105	192.168.122.57	TCP	74 [TCP Retransmission] 60221→22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=347297 TSecr=0 WS=128
329	347.886431000	192.168.122.105	192.168.122.57	TCP	74 [TCP Retransmission] 60221→22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=347297 TSecr=0 WS=128
330	349.889723000	fe:5d:35:4b:52:7b	Xensourc_9f:1f:32	ARP	42 Who has 192.168.122.57? Tell 192.168.122.1
331	349.889751000	Xensourc_9f:1f:32	fe:5d:35:4b:52:7b	ARP	42 192.168.122.57 is at 00:16:3e:9f:1f:32
332	351.890043000	192.168.122.105	192.168.122.57	TCP	74 [TCP Retransmission] 60221→22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=348300 TSecr=0 WS=128
333	351.895205000	192.168.122.105	192.168.122.57	TCP	74 [TCP Retransmission] 60221→22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=348300 TSecr=0 WS=128
334	353.549994000	fe:5d:35:4b:52:7b	00:ff:aa:90:af:3d	ARP	42 192.168.122.57 is at fe:5d:35:4b:52:7b
335	353.550017000	fe:5d:35:4b:52:7b	Xensourc_9f:1f:32	ARP	42 192.168.122.105 is at fe:5d:35:4b:52:7b
336	359.906110000	192.168.122.105	192.168.122.57	TCP	74 [TCP Retransmission] 60221→22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=350304 TSecr=0 WS=128
337	359.910273000	192.168.122.105	192.168.122.57	TCP	74 [TCP Retransmission] 60221→22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=350304 TSecr=0 WS=128
338	363.570101000	fe:5d:35:4b:52:7b	00:ff:aa:90:af:3d	ARP	42 192.168.122.57 is at fe:5d:35:4b:52:7b
339	363.570142000	fe:5d:35:4b:52:7b	Xensourc_9f:1f:32	ARP	42 192.168.122.105 is at fe:5d:35:4b:52:7b
340	373.585242000	fe:5d:35:4b:52:7b	00:ff:aa:90:af:3d	ARP	42 192.168.122.57 is at fe:5d:35:4b:52:7b
341	373.585277000	fe:5d:35:4b:52:7b	Xensourc_9f:1f:32	ARP	42 192.168.122.105 is at fe:5d:35:4b:52:7b
342	375.940326000	192.168.122.105	192.168.122.57	TCP	74 [TCP Retransmission] 60221→22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=354312 TSecr=0 WS=128
343	375.955149000	192.168.122.105	192.168.122.57	TCP	74 [TCP Retransmission] 60221→22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=354312 TSecr=0 WS=128
344	383.608452000	fe:5d:35:4b:52:7b	00:ff:aa:90:af:3d	ARP	42 192.168.122.57 is at fe:5d:35:4b:52:7b
345	383.608498000	fe:5d:35:4b:52:7b	Xensourc_9f:1f:32	ARP	42 192.168.122.105 is at fe:5d:35:4b:52:7b

Παρατηρούμε ότι ο c1 στέλνει SYN για συνδεση με τον c2 και δεν λαμβάνει ποτέ απάντηση οποτέ ξανακανεί TCP retransmission συνέχεια για αυτό έχει αποτυχία η ssh σύνδεση.

4-5. Καλούμε enable_redir στην mye007 και επαναλαμβάνουμε το βήμα 3.

374	526.004908000	192.168.122.105	192.168.122.57	TCP	74 60222→22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=391828 TSecr=0 WS=128
375	526.004947000	192.168.122.57	192.168.122.105	TCP	54 22→60222 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
376	526.007339000	192.168.122.105	192.168.122.57	TCP	74 [TCP Spurious Retransmission] 60222→22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=391828 TSecr=0 WS=128
377	531.010185000	fe:5d:35:4b:52:7b	00:ff:aa:90:af:3d	ARP	42 Who has 192.168.122.105? Tell 192.168.122.1
378	531.010202000	fe:5d:35:4b:52:7b	Xensourc_9f:1f:32	ARP	42 Who has 192.168.122.57? Tell 192.168.122.1
379	531.010220000	00:ff:aa:90:af:3d	fe:5d:35:4b:52:7b	ARP	42 192.168.122.105 is at 00:ff:aa:90:af:3d
380	531.010225000	Xensourc_9f:1f:32	fe:5d:35:4b:52:7b	ARP	42 192.168.122.57 is at 00:16:3e:9f:1f:32
381	533.857787000	fe:5d:35:4b:52:7b	00:ff:aa:90:af:3d	ARP	42 192.168.122.57 is at fe:5d:35:4b:52:7b
382	533.857813000	fe:5d:35:4b:52:7b	Xensourc_9f:1f:32	ARP	42 192.168.122.105 is at fe:5d:35:4b:52:7b
383	543.874665000	fe:5d:35:4b:52:7b	00:ff:aa:90:af:3d	ARP	42 192.168.122.57 is at fe:5d:35:4b:52:7b
384	543.874690000	fe:5d:35:4b:52:7b	Xensourc_9f:1f:32	ARP	42 192.168.122.105 is at fe:5d:35:4b:52:7b
385	553.890706000	fe:5d:35:4b:52:7b	00:ff:aa:90:af:3d	ARP	42 192.168.122.57 is at fe:5d:35:4b:52:7b
386	553.890731000	fe:5d:35:4b:52:7b	Xensourc_9f:1f:32	ARP	42 192.168.122.105 is at fe:5d:35:4b:52:7b
387	563.901298000	fe:5d:35:4b:52:7b	00:ff:aa:90:af:3d	ARP	42 192.168.122.57 is at fe:5d:35:4b:52:7b
388	563.901323000	fe:5d:35:4b:52:7b	Xensourc_9f:1f:32	ARP	42 192.168.122.105 is at fe:5d:35:4b:52:7b
389	573.918312000	fe:5d:35:4b:52:7b	00:ff:aa:90:af:3d	ARP	42 192.168.122.57 is at fe:5d:35:4b:52:7b
390	573.918348000	fe:5d:35:4b:52:7b	Xensourc_9f:1f:32	ARP	42 192.168.122.105 is at fe:5d:35:4b:52:7b
391	583.945338000	fe:5d:35:4b:52:7b	00:ff:aa:90:af:3d	ARP	42 192.168.122.57 is at fe:5d:35:4b:52:7b
392	583.945371000	fe:5d:35:4b:52:7b	Xensourc_9f:1f:32	ARP	42 192.168.122.105 is at fe:5d:35:4b:52:7b

Παρατηρούμε ότι ο c1 στέλνει SYN για σύνδεση με τον c2 και λαμβάνει απάντηση RST, ACK γιατί το port 22 που αποστέλνεται το SYN , στην μηχανή mye007 δεν χρησιμοποιείτε και αποτυγχάνει η σύνδεση ssh.

6-7. Σε νέο τερματικό του mye007 εκτελούμε mitm-ssh 192.168.122.105 -vp 2222 για να παρεβληθούμε στην επικοινωνία ssh από την c1 στην c2 προκειμένου να ανακατευθύνουμε την κυκλοφορία που φτάνει στην θύρα 22 του mye007 στη θύρα 2222 οπού ακούει το mitm-ssh.

Συνδεόμαστε από την c1 στην c2 με ssh και στην προτροπή εισάγουμε μερικά λαθός συνθηματικά,πριν χρησιμοποιήσουμε το σωστό.

22	68.842910000	192.168.122.105	192.168.122.57	TCP	74 60229→22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=874191 TSecr=0 WS=128
23	68.842948000	192.168.122.57	192.168.122.105	TCP	74 22→60229 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=874191 TSecr=874191 WS=128
24	68.842964000	192.168.122.105	192.168.122.57	TCP	66 60229→22 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=874191 TSecr=874191
25	68.843686000	192.168.122.57	192.168.122.105	SSHv2	89 Server: Protocol (SSH-1.99-OpenSSH_3.9p1)
26	68.843703000	192.168.122.105	192.168.122.57	TCP	66 60229→22 [ACK] Seq=1 Ack=24 Win=29312 Len=0 TSval=874192 TSecr=874192
27	68.843766000	192.168.122.105	192.168.122.57	SSHv2	101 Client: Protocol (SSH-2.0-OpenSSH_7.3p1 Debian-3+b1)
28	68.843784000	192.168.122.57	192.168.122.105	TCP	66 22→60229 [ACK] Seq=24 Ack=36 Win=29056 Len=0 TSval=874192 TSecr=874192
29	68.843836000	192.168.122.57	192.168.122.105	SSHv2	706 Server: Key Exchange Init
30	68.843942000	192.168.122.105	192.168.122.57	SSHv2	1498 Client: Key Exchange Init
31	68.883771000	192.168.122.57	192.168.122.105	TCP	66 22→60229 [ACK] Seq=664 Ack=1468 Win=31872 Len=0 TSval=874202 TSecr=874192
32	68.883824000	192.168.122.105	192.168.122.57	SSHv2	90 Client: Diffie-Hellman Group Exchange Request
33	68.883837000	192.168.122.57	192.168.122.105	TCP	66 22→60229 [ACK] Seq=664 Ack=1492 Win=31872 Len=0 TSval=874202 TSecr=874202
34	68.884046000	192.168.122.57	192.168.122.105	SSHv2	346 Server: Diffie-Hellman Group Exchange Group
35	68.886241000	192.168.122.105	192.168.122.57	SSHv2	338 Client: Diffie-Hellman Group Exchange Init
36	68.888538000	192.168.122.57	192.168.122.105	SSHv2	914 Server: Diffie-Hellman Group Exchange Reply, New Keys
37	68.927532000	192.168.122.105	192.168.122.57	TCP	66 60229→22 [ACK] Seq=1764 Ack=1792 Win=33536 Len=0 TSval=874213 TSecr=874203
38	70.162954000	fe:5d:35:4b:52:7b	00:ff:aa:90:af:3d	ARP	42 192.168.122.57 is at fe:5d:35:4b:52:7b
39	70.163000000	fe:5d:35:4b:52:7b	Xensourc_9f:1f:32	ARP	42 192.168.122.105 is at fe:5d:35:4b:52:7b (duplicate use of 192.168.122.57 detected!)
40	80.182543000	fe:5d:35:4b:52:7b	00:ff:aa:90:af:3d	ARP	42 192.168.122.57 is at fe:5d:35:4b:52:7b
41	80.182570000	fe:5d:35:4b:52:7b	Xensourc_9f:1f:32	ARP	42 192.168.122.105 is at fe:5d:35:4b:52:7b (duplicate use of 192.168.122.57 detected!)
42	90.216707000	fe:5d:35:4b:52:7b	00:ff:aa:90:af:3d	ARP	42 192.168.122.57 is at fe:5d:35:4b:52:7b
43	90.216740000	fe:5d:35:4b:52:7b	Xensourc_9f:1f:32	ARP	42 192.168.122.105 is at fe:5d:35:4b:52:7b (duplicate use of 192.168.122.57 detected!)

Παρατηρούμε ότι το ssh λειτουργά κανονικά.

Μάριος Γαβριήλ ΑΜ:4244 Μηνάς Ελευθερίου ΑΜ:4245

8. Παρατηρούμε στο τερματικό του mye007 να εμφανίζεται ο κωδικός που ο c1 εισάγει για να συνδεθεί με ssh στον c2. Επίσης ελέγχουμε την κυκλοφορία της συνεδρίας ssh μεταξύ των c1 και c2 που είναι αποθηκευμένη στον καταλόγο /usr/local/var/log/mitm-ssh με τις πληροφορίες ταυτοποίησης και το συνθηματικό.