

בס"ד

הפעלנו במחשב א' את השרת ובמחשב ב' את ה=client

ה client ביצע התחברות עם השם "moshe" ושלה הודעה אחת עם התוכן: ma kore?

עקבנו אחרי פעולות אלו בעזרת wireshark ניתקנו את ההתקשרות ושמרנו קובץ pcap

פתחנו את קובץ ה pcap וקיבלנו את החלון הבא:

WireShark.pcap [Wireshark 1.12.8 (v1.12.8-0-g5b6e543 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Fortinet_2b:57:d9	Broadcast	ARP	56	who has 172.16.28.83? Tell 172.16.31.254
2	0.001570	172.16.27.163	255.255.255.255	DHCP	345	DHCP Request - Transaction ID 0x4989368a
3	0.001571	172.16.26.21	172.16.31.255	NBNS	92	Name query NB ISATAP<00>
4	0.001572	LgElectr_d8:b7:90	Broadcast	ARP	56	who has 172.16.26.21? Tell 172.16.27.128
5	0.001572	LgElectr_bb:3a:49	Broadcast	ARP	56	who has 172.16.26.21? Tell 172.16.24.122
6	0.102434	172.16.29.137	255.255.255.255	UDP	170	Source port: 60677 Destination port: 10019
7	0.102435	Fortinet_2b:57:d9	Broadcast	ARP	56	who has 172.16.25.240? Tell 172.16.31.254
8	0.205518	MurataMa_2e:a1:e6	Broadcast	0x3600	68	Ethernet II
9	0.205518	172.16.25.222	255.255.255.255	UDP	170	Source port: 51501 Destination port: 10007
10	0.205519	172.16.27.208	172.16.31.255	UDP	86	Source port: 49157 Destination port: 61117
11	0.205519	Fortinet_2b:57:d9	Broadcast	ARP	56	who has 172.16.24.72? Tell 172.16.31.254
12	0.307113	Fortinet_2b:57:d9	Broadcast	ARP	56	who has 172.16.31.33? Tell 172.16.31.254
13	0.307114	Fortinet_2b:57:d9	Broadcast	ARP	56	who has 172.16.26.212? Tell 172.16.31.254
14	0.307683	0.0.0.0	255.255.255.255	DHCP	351	DHCP Discover - Transaction ID 0x1c3f48b0
15	0.408872	0.0.0.0	255.255.255.255	DHCP	363	DHCP Request - Transaction ID 0x1c3f48b0
16	0.409722	JuniperN_17:d8:81	Broadcast	ARP	56	who has 172.16.29.238? Tell 172.16.31.253

<

Frame 1: 56 bytes on wire (448 bits), 56 bytes captured (448 bits)
Ethernet II, Src: Fortinet_2b:57:d9 (08:5b:0e:2b:57:d9), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

0000 ff ff ff ff ff 08 5b 0e 2b 57 d9 08 06 00 01[.+.w.....
0010 08 00 06 04 00 01 08 5b 0e 2b 57 d9 ac 10 1f fe[.+.w.....
0020 00 00 00 00 00 00 ac 10 1c 53 00 00 00 00 00[.S.....
0030 00 00 00 00 00 00 00 00

על מנת לזהות את התעבורה של הצ'אט נסנן את התוצאות לפי הפורט שהשתמשנו בצ'אט- 7777:

Wireshark.pcap [Wireshark 1.12.8 (v1.12.8-0-g5b6e543 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp.port==7777 Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
345	6.452694	172.16.28.147	172.16.29.13	TCP	66	1743->7777 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
346	6.452775	172.16.29.13	172.16.28.147	TCP	66	7777->1743 [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
347	6.455991	172.16.28.147	172.16.29.13	TCP	54	1743->7777 [ACK] Seq=1 Ack=1 win=65536 Len=0
348	6.459752	172.16.28.147	172.16.29.13	TCP	58	1743->7777 [PSH, ACK] Seq=1 Ack=1 win=65536 Len=4
349	6.460928	172.16.29.13	172.16.28.147	TCP	58	7777->1743 [PSH, ACK] Seq=1 Ack=5 win=65536 Len=4
350	6.471571	172.16.28.147	172.16.29.13	TCP	62	1743->7777 [PSH, ACK] Seq=5 Ack=5 win=65536 Len=8
351	6.477131	172.16.29.13	172.16.28.147	TCP	74	7777->1743 [PSH, ACK] Seq=5 Ack=13 win=65536 Len=20
364	6.678479	172.16.28.147	172.16.29.13	TCP	54	1743->7777 [ACK] Seq=13 Ack=25 win=65536 Len=0
1073	20.189863	172.16.28.147	172.16.29.13	TCP	66	1743->7777 [PSH, ACK] Seq=13 Ack=25 win=65536 Len=12
1074	20.190081	172.16.29.13	172.16.28.147	TCP	73	7777->1743 [PSH, ACK] Seq=25 Ack=25 win=65536 Len=19
1085	20.406829	172.16.28.147	172.16.29.13	TCP	54	1743->7777 [ACK] Seq=25 Ack=44 win=65536 Len=0
1319	24.494245	172.16.28.147	172.16.29.13	TCP	60	1743->7777 [PSH, ACK] Seq=25 Ack=44 win=65536 Len=6
1320	24.495157	172.16.29.13	172.16.28.147	TCP	67	7777->1743 [PSH, ACK] Seq=44 Ack=31 win=65536 Len=13
1321	24.495515	172.16.29.13	172.16.28.147	TCP	54	7777->1743 [FIN, ACK] Seq=57 Ack=31 win=65536 Len=0
1322	24.497692	172.16.28.147	172.16.29.13	TCP	54	1743->7777 [ACK] Seq=31 Ack=58 win=65536 Len=0
1556	29.504356	172.16.28.147	172.16.29.13	TCP	54	1743->7777 [RST, ACK] Seq=31 Ack=58 win=0 Len=0

Frame 345: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)

Ethernet II, Src: IntelCor_89:3d:7a (f4:06:69:89:3d:7a), Dst: HonHaiPr_22:63:f7 (80:56:f2:22:63:f7)

Internet Protocol Version 4, Src: 172.16.28.147 (172.16.28.147), Dst: 172.16.29.13 (172.16.29.13)

Transmission Control Protocol, Src Port: 1743 (1743), Dst Port: 7777 (7777), Seq: 0, Len: 0

0000 80 56 f2 22 63 f7 f4 06 69 89 3d 7a 08 00 45 00 .V."c... i.=z..E.
0010 00 34 16 2c 40 00 80 06 52 d7 ac 10 1c 93 ac 10 .4.,@... R.....
0020 1d 0d 06 cf 1e 61 4e 4f bc 45 00 00 00 00 80 02aNO .E.....
0030 20 00 8d 8a 00 00 02 04 05 b4 01 03 03 08 01 01
0040 04 02 ..

זיהינו את ההתחברות של הלקוח עם ה־172.16.28.147

אל השרת עם ה־172.16.29.13

כאן למשל ניתן לראות שהלקוח שולח את ההודעה: ma kore?

Filter: tcp.port==7777 Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
345	6.452694	172.16.28.147	172.16.29.13	TCP	66	1743->7777 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
346	6.452775	172.16.29.13	172.16.28.147	TCP	66	7777->1743 [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
347	6.455991	172.16.28.147	172.16.29.13	TCP	54	1743->7777 [ACK] Seq=1 Ack=1 win=65536 Len=0
348	6.459752	172.16.28.147	172.16.29.13	TCP	58	1743->7777 [PSH, ACK] Seq=1 Ack=1 win=65536 Len=4
349	6.460928	172.16.29.13	172.16.28.147	TCP	58	7777->1743 [PSH, ACK] Seq=1 Ack=5 win=65536 Len=4
350	6.471571	172.16.28.147	172.16.29.13	TCP	62	1743->7777 [PSH, ACK] Seq=5 Ack=5 win=65536 Len=8
351	6.477131	172.16.29.13	172.16.28.147	TCP	74	7777->1743 [PSH, ACK] Seq=5 Ack=13 win=65536 Len=20
364	6.678479	172.16.28.147	172.16.29.13	TCP	54	1743->7777 [ACK] Seq=13 Ack=25 win=65536 Len=0
1073	20.189863	172.16.28.147	172.16.29.13	TCP	66	1743->7777 [PSH, ACK] Seq=13 Ack=25 win=65536 Len=12
1074	20.190081	172.16.29.13	172.16.28.147	TCP	73	7777->1743 [PSH, ACK] Seq=25 Ack=25 win=65536 Len=19
1085	20.406829	172.16.28.147	172.16.29.13	TCP	54	1743->7777 [ACK] Seq=25 Ack=44 win=65536 Len=0
1319	24.494245	172.16.28.147	172.16.29.13	TCP	60	1743->7777 [PSH, ACK] Seq=25 Ack=44 win=65536 Len=6
1320	24.495157	172.16.29.13	172.16.28.147	TCP	67	7777->1743 [PSH, ACK] Seq=44 Ack=31 win=65536 Len=13
1321	24.495515	172.16.29.13	172.16.28.147	TCP	54	7777->1743 [FIN, ACK] Seq=57 Ack=31 win=65536 Len=0
1322	24.497692	172.16.28.147	172.16.29.13	TCP	54	1743->7777 [ACK] Seq=31 Ack=58 win=65536 Len=0
1556	29.504356	172.16.28.147	172.16.29.13	TCP	54	1743->7777 [RST, ACK] Seq=31 Ack=58 win=0 Len=0

Frame 1073: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)

Ethernet II, Src: IntelCor_89:3d:7a (f4:06:69:89:3d:7a), Dst: HonHaiPr_22:63:f7 (80:56:f2:22:63:f7)

Internet Protocol Version 4, Src: 172.16.28.147 (172.16.28.147), Dst: 172.16.29.13 (172.16.29.13)

Transmission Control Protocol, Src Port: 1743 (1743), Dst Port: 7777 (7777), Seq: 13, Ack: 25, Len: 12

Data (12 bytes)

Data: 7400096d61206b6f72653f0a
[Length: 12]

0000 80 56 f2 22 63 f7 f4 06 69 89 3d 7a 08 00 45 00 .V."c... i.=z..E.
0010 00 34 16 2c 40 00 80 06 52 ce ac 10 1c 93 ac 10 .4.5@... R.....
0020 1d 0d 06 cf 1e 61 4e 4f bc 52 9a 5c e6 dd 50 18aNO .R.\..P.
0030 01 00 00 70 86 00 00 74 00 09 6d 61 20 6b 6f 72 65 ...p...E...ma kore
0040 3f 0a

כאן אפשר לראות שהשרת שולח לכל המשתמשים המחוברים את ההודעה שקיבל מהלקוח בצירוף שם השולח:

WireShark.pcap [Wireshark 1.12.8 (v1.12.8-0-g3b6e543 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp.port==7777 Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
345	6.452694	172.16.28.147	172.16.29.13	TCP	66	1743→7777 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SA=172.16.28.147 D=172.16.29.13
346	6.452775	172.16.29.13	172.16.28.147	TCP	66	7777→1743 [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1460 WS=256 SA=172.16.29.13 D=172.16.28.147
347	6.455991	172.16.28.147	172.16.29.13	TCP	54	1743→7777 [ACK] Seq=1 Ack=1 win=65536 Len=0
348	6.459752	172.16.28.147	172.16.29.13	TCP	58	1743→7777 [PSH, ACK] Seq=1 Ack=1 win=65536 Len=4
349	6.460928	172.16.29.13	172.16.28.147	TCP	58	7777→1743 [PSH, ACK] Seq=1 Ack=5 win=65536 Len=4
350	6.471571	172.16.28.147	172.16.29.13	TCP	62	1743→7777 [PSH, ACK] Seq=5 Ack=5 win=65536 Len=8
351	6.477131	172.16.29.13	172.16.28.147	TCP	74	7777→1743 [PSH, ACK] Seq=5 Ack=13 win=65536 Len=20
364	6.678479	172.16.28.147	172.16.29.13	TCP	54	1743→7777 [ACK] Seq=13 Ack=25 win=65536 Len=0
1073	20.189863	172.16.28.147	172.16.29.13	TCP	66	1743→7777 [PSH, ACK] Seq=13 Ack=25 win=65536 Len=12
1074	20.190081	172.16.29.13	172.16.28.147	TCP	73	7777→1743 [PSH, ACK] Seq=25 Ack=25 win=65536 Len=19
1085	20.406829	172.16.28.147	172.16.29.13	TCP	54	1743→7777 [ACK] Seq=25 Ack=44 win=65536 Len=0
1319	24.494245	172.16.28.147	172.16.29.13	TCP	60	1743→7777 [PSH, ACK] Seq=25 Ack=44 win=65536 Len=6
1320	24.495157	172.16.29.13	172.16.28.147	TCP	67	7777→1743 [PSH, ACK] Seq=44 Ack=31 win=65536 Len=13
1321	24.495515	172.16.29.13	172.16.28.147	TCP	54	7777→1743 [FIN, ACK] Seq=57 Ack=31 win=65536 Len=0
1322	24.497692	172.16.28.147	172.16.29.13	TCP	54	1743→7777 [ACK] Seq=31 Ack=58 win=65536 Len=0
1556	29.504356	172.16.28.147	172.16.29.13	TCP	54	1743→7777 [RST, ACK] Seq=31 Ack=58 win=0 Len=0

Frame 1074: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0

Ethernet II, Src: HonHaiPr_22:63:F7 (80:56:f2:22:63:f7), Dst: IntelCor_89:3d:7a (f4:06:69:89:3d:7a)

Internet Protocol Version 4, Src: 172.16.29.13 (172.16.29.13), Dst: 172.16.28.147 (172.16.28.147)

Transmission Control Protocol, Src Port: 7777 (7777), Dst Port: 1743 (1743), Seq: 25, Ack: 25, Len: 19

Data (19 bytes)

Data: 7400104d6f7368653a206d61206b6f72653f0a [Length: 19]

0000 f4 06 69 89 3d 7a 80 56 f2 22 63 f7 08 00 45 00 ..i.=z.v ".c...E.

0010 00 3b 7b 96 40 00 80 06 ed 65 ac 10 1d 0d ac 10 .;{.@... .e.....

0020 1c 93 1e 61 06 cf 9a 5c e6 dd 4e 4f bc 5e 50 18 ...a... \..NO.AP.

0030 01 00 69 1b 00 00 f4 00 10 4d 6f 73 68 65 3a 20 ..i...[.mosine:

0040 6d 61 20 6b 6f 72 65 3f 0a ma kore?.

בתוכנת fiddler נוכל לעקוב אחרי הצ'אט מכיוון שהיא פועלת רק על http ו-https

ואילו הצ'אט עובד על tcp