

1. Úloha

qualification2018.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns && ip.addr == 10.20.30.2 && frame.cap_len == 130 or frame.cap_len == 80

No.	Time	Source	Destination	Protocol	Length	Info
47342	8624.093007	10.10.10.2	10.20.30.2	DNS	130	Standard query response 0x9d0a A smtprelay.testang.eu A 172.16.10.9 NS dns.testang.eu A 172.16.10.2
28111	8587.678946	10.10.10.2	10.20.30.2	DNS	130	Standard query response 0x9e2f A smtprelay.testang.eu A 172.16.10.9 NS dns.testang.eu A 172.16.10.2
24765	8587.489215	10.10.10.2	10.20.30.2	DNS	130	Standard query response 0x9e9f A smtprelay.testang.eu A 172.16.10.9 NS dns.testang.eu A 172.16.10.2
35478	8588.137225	10.10.10.2	10.20.30.2	DNS	130	Standard query response 0x9f2c A smtprelay.testang.eu A 172.16.10.9 NS dns.testang.eu A 172.16.10.2
36884	8588.227390	10.10.10.2	10.20.30.2	DNS	130	Standard query response 0x9fd6 A smtprelay.testang.eu A 172.16.10.9 NS dns.testang.eu A 172.16.10.2
53155	8684.897124	10.10.10.2	10.20.30.2	DNS	130	Standard query response 0xa00f A smtprelay.testang.eu A 172.16.10.9 NS dns.testang.eu A 172.16.10.2
33465	8588.020700	10.10.10.2	10.20.30.2	DNS	130	Standard query response 0xa0ad A smtprelay.testang.eu A 172.16.10.9 NS dns.testang.eu A 172.16.10.2
60250	8744.482195	10.10.10.2	10.20.30.2	DNS	130	Standard query response 0xa2d9 A smtprelay.testang.eu A 172.16.10.9 NS dns.testang.eu A 172.16.10.2
60042	8744.409979	10.10.10.2	10.20.30.2	DNS	130	Standard query response 0xa36d A smtprelay.testang.eu A 172.16.10.9 NS dns.testang.eu A 172.16.10.2
29274	8587.744198	10.10.10.2	10.20.30.2	DNS	130	Standard query response 0xa3e8 A smtprelay.testang.eu A 172.16.10.9 NS dns.testang.eu A 172.16.10.2
61662	8757.238609	10.10.10.2	10.20.30.2	DNS	130	Standard query response 0xa47b A smtprelay.testang.eu A 172.16.10.9 NS dns.testang.eu A 172.16.10.2
31194	8587.868432	10.10.10.2	10.20.30.2	DNS	130	Standard query response 0xa49f A smtprelay.testang.eu A 172.16.10.9 NS dns.testang.eu A 172.16.10.2

> Frame 16662: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits)
> Ethernet II, Src: Microsof_19:8a:29 (00:15:5d:19:8a:29), Dst: Microsof_19:8a:31 (00:15:5d:19:8a:31)
> Internet Protocol Version 4, Src: 10.10.10.2, Dst: 10.20.30.2
> User Datagram Protocol, Src Port: 53, Dst Port: 43483
> Domain Name System (response)

0000 00 15 5d 19 8a 31 00 15 5d 19 8a 29 08 00 45 00 ...]...1...]...E-
0010 00 74 1b 6a 00 00 40 11 22 ee 0a 0a 0a 02 0a 14 ...t.j. @ ".....
0020 1e 02 00 35 a9 db 00 60 97 8a a4 7b 85 80 00 01 ...5... ..(
0030 00 01 00 01 00 01 09 73 6d 74 70 72 65 6c 61 79s mtprelay
0040 07 74 65 73 74 61 6e 67 02 65 75 00 00 01 00 01testang.eu.....
0050 c0 0c 00 01 00 01 00 01 2c 00 04 ac 10 0a 09
0060 c0 16 00 02 00 01 00 00 01 2c 00 06 03 64 6e 73 dns
0070 c0 16 c0 42 00 01 00 01 00 00 01 2c 00 04 ac 10 ...B.....
0080 0a 02

qualification2018.pcap Packets: 138088 - Displayed: 1660 (1.2%) Profile: Default

dns && ip.addr == 10.20.30.2 && frame.cap_len == 130 or frame.cap_len == 80

2. úloha

qualification2018.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http && ip.dst == 10.10.5.17 && http.request.uri contains "secret.php"

No.	Time	Source	Destination	Protocol	Length	Info
1313...	-34288833.47...	10.20.90.218	10.10.5.17	HTTP	202	HEAD /secret/secret.php HTTP/1.0
1313...	-34288833.47...	10.20.90.218	10.10.5.17	HTTP	202	HEAD /secret/secret.php HTTP/1.0
1313...	-34288833.47...	10.20.90.218	10.10.5.17	HTTP	202	HEAD /secret/secret.php HTTP/1.0
1313...	-34288833.47...	10.20.90.218	10.10.5.17	HTTP	206	HEAD /secret/secret.php HTTP/1.0
1313...	-34288833.47...	10.20.90.218	10.10.5.17	HTTP	206	HEAD /secret/secret.php HTTP/1.0
1313...	-34288833.47...	10.20.90.218	10.10.5.17	HTTP	202	HEAD /secret/secret.php HTTP/1.0
1313...	-34288833.47...	10.20.90.218	10.10.5.17	HTTP	206	HEAD /secret/secret.php HTTP/1.0
1313...	-34288833.47...	10.20.90.218	10.10.5.17	HTTP	206	HEAD /secret/secret.php HTTP/1.0
1313...	-34288833.47...	10.20.90.218	10.10.5.17	HTTP	206	HEAD /secret/secret.php HTTP/1.0
1313...	-34288833.47...	10.20.90.218	10.10.5.17	HTTP	206	HEAD /secret/secret.php HTTP/1.0
1313...	-34288833.47...	10.20.90.218	10.10.5.17	HTTP	202	HEAD /secret/secret.php HTTP/1.0
1313...	-34288833.47...	10.20.90.218	10.10.5.17	HTTP	202	HEAD /secret/secret.php HTTP/1.0
1313...	-34288833.47...	10.20.90.218	10.10.5.17	HTTP	206	HEAD /secret/secret.php HTTP/1.0

> Frame 131342: 206 bytes on wire (1648 bits), 206 bytes captured (1648 bits)
> Ethernet II, Src: Routerbo_e7:53:1c (4c:5e:0c:e7:53:1c), Dst: Microsof_b3:1a:3a (00:15:5d:b3:1a:3a)
> Internet Protocol Version 4, Src: 10.20.90.218, Dst: 10.10.5.17
> Transmission Control Protocol, Src Port: 1031, Dst Port: 80, Seq: 1, Ack: 1, Len: 140
> Hypertext Transfer Protocol

http && ip.dst == 10.10.5.17 && http.request.uri contains "secret.php"

3. úloha BONUS

1) IP adresa útočníka je 10.20.90.218

- 2)
 - ✓ Authorization: Basic YWRtaW46ZmFtaWx5\r\n
 - Credentials: admin:family
 - ✓ Authorization: Basic YWRtaW46d2hhdGV2ZXI=\r\n
 - Credentials: admin:whatever
 - ✓ Authorization: Basic YWRtaW46bmFydXRv\r\n
 - Credentials: admin:naruto

Čiže napríklad, meno: admin ; heslo: naruto