

Wireshark - Mustso Final Raporu

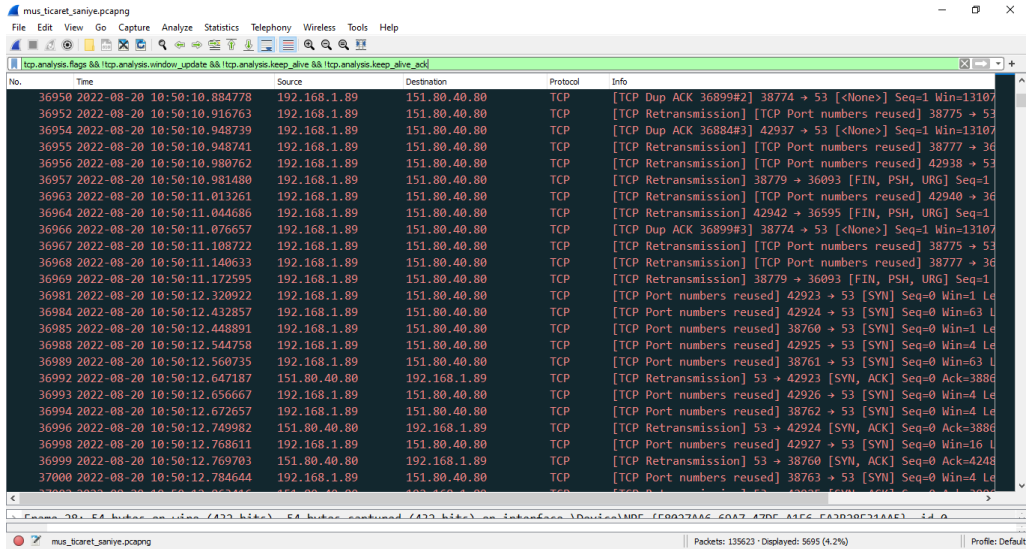
175541611 Mohammad Amin ASLAMI - Kişisel Rapor

Wireshark

Wireshark bir ağ paket analiz aracıdır. Mustso ip adresini buldum ve wireshark'ta bir kaç tane filter yazdım, bir kaç tane sonuç buldum, ama en önemlilerinden bir tanesi Bad TCP'di 54 tane yakın Bad TCP 151.80.40.80 id adresinide vardı, zaten uzaktan tarama yaptım için sadece kısıtlı bilgiler elde edebildim, toplu olarak Genel rapor halinde daha ayrıntılı bir şekilde gurup olarak verdik.

Bad TCP (Yakalama)

Varsayılan Wireshark yüklemesi, siyah bir arka plan üzerinde kırmızı metin kullanan "Hatalı TCP" adlı bir renklendirme kuralına sahiptir. Bu renklendirme kuralı "tcp" koşuluyla eşleşir.analiz.bayraklar". Muhtemelen gördüğün şey budur. Kendi başına, bu bilgi muazzam derecede yararlı değildir, çünkü tcp.analiz.bayraklar birkaç farklı TCP koşuluyla eşleşir.



| No. | Time | Source | Destination | Protocol | Info |
|-------|----------------------------|--------------|--------------|----------|---|
| 36950 | 2022-08-20 10:50:10.884778 | 192.168.1.89 | 151.80.40.80 | TCP | [TCP Dup ACK 36899#2] 38774 → 53 [⟨None⟩] Seq=1 Win=13107 |
| 36952 | 2022-08-20 10:50:10.916763 | 192.168.1.89 | 151.80.40.80 | TCP | [TCP Retransmission] [TCP Port numbers reused] 38775 → 53 |
| 36954 | 2022-08-20 10:50:10.948739 | 192.168.1.89 | 151.80.40.80 | TCP | [TCP Dup ACK 36884#3] 42937 → 53 [⟨None⟩] Seq=1 Win=13107 |
| 36955 | 2022-08-20 10:50:10.948741 | 192.168.1.89 | 151.80.40.80 | TCP | [TCP Retransmission] [TCP Port numbers reused] 38777 → 36 |
| 36956 | 2022-08-20 10:50:10.980762 | 192.168.1.89 | 151.80.40.80 | TCP | [TCP Retransmission] [TCP Port numbers reused] 42938 → 53 |
| 36957 | 2022-08-20 10:50:10.981480 | 192.168.1.89 | 151.80.40.80 | TCP | [TCP Retransmission] 38779 → 36093 [FIN, PSH, URG] Seq=1 |
| 36963 | 2022-08-20 10:50:11.013261 | 192.168.1.89 | 151.80.40.80 | TCP | [TCP Retransmission] [TCP Port numbers reused] 42940 → 36 |
| 36964 | 2022-08-20 10:50:11.044686 | 192.168.1.89 | 151.80.40.80 | TCP | [TCP Retransmission] 42942 → 36595 [FIN, PSH, URG] Seq=1 |
| 36966 | 2022-08-20 10:50:11.076657 | 192.168.1.89 | 151.80.40.80 | TCP | [TCP Dup ACK 36899#3] 38774 → 53 [⟨None⟩] Seq=1 Win=13107 |
| 36967 | 2022-08-20 10:50:11.108722 | 192.168.1.89 | 151.80.40.80 | TCP | [TCP Retransmission] [TCP Port numbers reused] 38775 → 53 |
| 36968 | 2022-08-20 10:50:11.140633 | 192.168.1.89 | 151.80.40.80 | TCP | [TCP Retransmission] [TCP Port numbers reused] 38777 → 36 |
| 36969 | 2022-08-20 10:50:11.172595 | 192.168.1.89 | 151.80.40.80 | TCP | [TCP Retransmission] 38779 → 36093 [FIN, PSH, URG] Seq=1 |
| 36981 | 2022-08-20 10:50:12.320922 | 192.168.1.89 | 151.80.40.80 | TCP | [TCP Port numbers reused] 42923 → 53 [SYN] Seq=0 Win=1 Le |
| 36984 | 2022-08-20 10:50:12.432857 | 192.168.1.89 | 151.80.40.80 | TCP | [TCP Port numbers reused] 42924 → 53 [SYN] Seq=0 Win=63 L |
| 36985 | 2022-08-20 10:50:12.448891 | 192.168.1.89 | 151.80.40.80 | TCP | [TCP Port numbers reused] 38760 → 53 [SYN] Seq=0 Win=1 Le |
| 36988 | 2022-08-20 10:50:12.544758 | 192.168.1.89 | 151.80.40.80 | TCP | [TCP Port numbers reused] 42925 → 53 [SYN] Seq=0 Win=4 Le |
| 36989 | 2022-08-20 10:50:12.560735 | 192.168.1.89 | 151.80.40.80 | TCP | [TCP Port numbers reused] 38761 → 53 [SYN] Seq=0 Win=63 L |
| 36992 | 2022-08-20 10:50:12.647187 | 151.80.40.80 | 192.168.1.89 | TCP | [TCP Retransmission] 53 → 42923 [SYN, ACK] Seq=0 Ack=3886 |
| 36993 | 2022-08-20 10:50:12.656667 | 192.168.1.89 | 151.80.40.80 | TCP | [TCP Port numbers reused] 42926 → 53 [SYN] Seq=0 Win=4 Le |
| 36994 | 2022-08-20 10:50:12.672657 | 192.168.1.89 | 151.80.40.80 | TCP | [TCP Port numbers reused] 38762 → 53 [SYN] Seq=0 Win=4 Le |
| 36996 | 2022-08-20 10:50:12.749982 | 151.80.40.80 | 192.168.1.89 | TCP | [TCP Retransmission] 53 → 42924 [SYN, ACK] Seq=0 Ack=3886 |
| 36998 | 2022-08-20 10:50:12.768611 | 192.168.1.89 | 151.80.40.80 | TCP | [TCP Port numbers reused] 42927 → 53 [SYN] Seq=0 Win=16 L |
| 36999 | 2022-08-20 10:50:12.769703 | 151.80.40.80 | 192.168.1.89 | TCP | [TCP Retransmission] 53 → 38760 [SYN, ACK] Seq=0 Ack=4248 |
| 37000 | 2022-08-20 10:50:12.784644 | 192.168.1.89 | 151.80.40.80 | TCP | [TCP Port numbers reused] 38763 → 53 [SYN] Seq=0 Win=4 Le |

Bad TCP 54 tane taradımız ağ'da buldum.

HTTP (Hypertext Transfer Protocol):

Genellikle **application** ile başlayanları kötü amaçlı olarak kullanabiliriz, onları indirip ondan sonra deneyebiliriz ve eğer o uygulama çalışırsa hack ve kötü amaçlı olarak kullanabilir, o yüzden http protokolü çok önemli bir protokoldür.