

Wireshark - Mustso Final Raporu

Ders Hakkında:

Ders: Bilgi Sistemleri ve Güvenliği [YMH321]

Danışman: Doç.Dr.Fatih ÖZKAYNAK

Fakülte/Bölüm: Teknoloji Fakültesi/Yazılım Mühendisliği

Üniversite: Fırat Üniversitesi/Elazığ

Github:

https://github.com/burakd81/bsvg/blob/5c329a2ab0cf42a2fa91cd2bb035b25d4d8caa43/mus_ticaret_s_anayi_odasi.pcapng

Çalışma Ekibi:

Öğrenci No	Ad ve Soyadı
190541021	Zeynep DEMİR
175541038	Ali Fuat KARAASLAN
16541044	Furkan BAŞAN
185542003	Burak DEMİRER
190541017	Rumeysa KOÇAK
175541006	Osman USLU
185541094	Alihan EYMİRLİ
16541071	Hazel OKTAY
15541061	Hidayet Can ULUBAŞ
175541611	Mohammad Amin ASLAMI
175541009	Alihan KOÇ

Wireshark Nedir?

Wireshark bir ağ paket analiz aracıdır. Bir ağ paket analiz aracı, yakalanan paketlerin verilerini mümkün olduğunca ayrıntılı sunar. **Wireshark özgür ve açık kaynaklı bir paket çözümleyicisidir.** Ağ sorunlarını giderme, çözümüleme, yazılım ve iletişim protokolü geliştirme ve eğitim amaçlı olarak kullanılır.

Wireshark'ın Özellikleri

Windows,Unix,OS X,Solaris,FreeBSD,NetBSD ve birçok işletim sistemleri için uygundur.

Wireshark ne için kullanılır?

Performans sorunları olan ağlarda sorun giderme de dahil olmak üzere birçok kullanıma sahiptir. Siber güvenlik uzmanları genellikle bağlantıları izlemek, şüpheli ağ işlemlerinin içeriğini görüntülemek ve ağ trafiği patlamalarını belirlemek için bu yazılımı kullanır. Bu yazılım herhangi bir BT uzmanının araç setinin önemli bir parçasıdır.

1. 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.

Bunlardan bazıları kendiliğinden kötü değildir ve sorun gidermeye çalıştığınız sorunla doğrudan ilgili olmayabilir. Aşağıda bir kaç tane (Bad TCP) paketini **mustso'dan** yakaladık.

Bad TCP (Komutu) - tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive && !tcp.analysis.keep_alive_ack

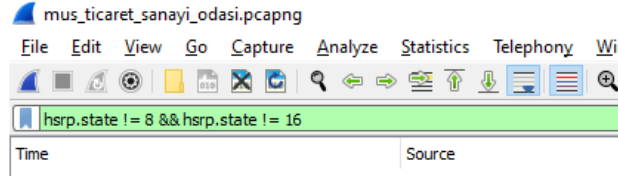
No.	Time	Source	Destination	Protocol	Info
36950	2022-08-20 10:50:10.884778	192.168.1.89	151.80.40.80	TCP	[TCP Dup ACK 36899#2] 38774 → 53 [None] Seq=1 Win=13107
36952	2022-08-20 10:50:10.916763	192.168.1.89	151.80.40.80	TCP	[TCP Retransmission] [TCP Port numbers reused] 38775 → 53
36954	2022-08-20 10:50:10.948739	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 10:50:10.988762	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

Mustso IP Adresi - 151.80.40.80

Bad TCP 54 tane taradımız ağ'da bulduk, bunları görmek için github linkin'den ulaşabilirsiniz.

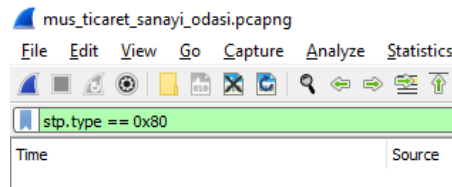
2. HSRP State Change (Hot Standby Redundancy Protocol)

HSRP paketini **mustso'dan** her hangi bir ağ veya problem yakalamadık. Yani HSRP ile ilgili her hangi bir düzenleme gerek yoktur.



3. Spanning Tree Topology Change (STP)

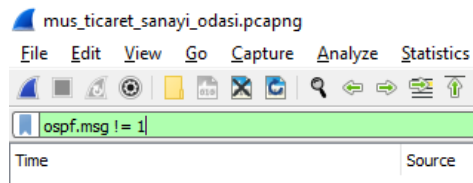
STP paketini **mustso'dan** her hangi bir ağ veya problem yakalamadık. Yani STP ile ilgili herhangi bir düzenleme gerek yoktur.



4. OSPF State Change (open shortest path first)

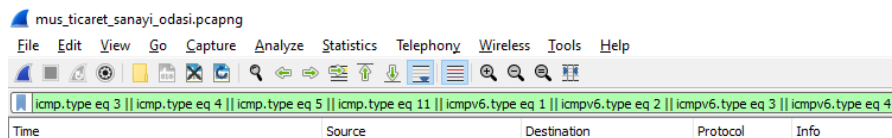
dinamik bir yönlendirme protokolüdür. Bir iç ağ geçidi protokolüdür (IGP). Yönlendiriciler, yönetici müdahalesine gerek kalmadan rotaları otomatik olarak öğrenmek için kullanır.

OSPF ile ilgili herhangi bir düzenleme gerek yoktur.



5. ICMP errors

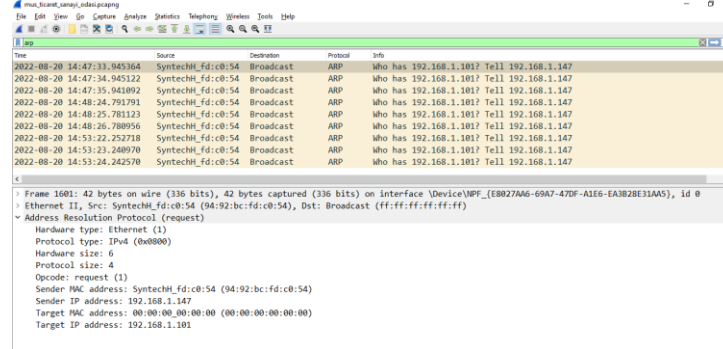
ICMP'deki hata verileri iki değerde taşınır: type ve code. Bir ICMP paketinin tipi, mesajın iletmeyi amaçladığı genel mesajı içerir. **Örneğin, 3 türündeki bir değer, amaçlanan varış noktasına ulaşılamadığı anlamına gelir**, ama bize herhangi bir ağ tarafını vermedi için düzgün çalıştığını bize göstermektedir.



6. ARP (Address Resulation Protocol)

Adres Çözümleme Protokolü, katman 3 (protokol) ve katman 2 (donanım) adresi arasındaki eşlemeyi dinamik olarak keşfetmek için kullanılır. Tipik bir kullanım, bir IP adresinin (ör. 192.168.0.10) temel Ethernet adresine (ör. 01:02:03:04:05:06) eşlenmesidir. ARP bu adreslerin keşfedilme şekli olduğundan, genellikle bir konuşmanın başında ARP paketlerini görürsünüz.

Aşağıda 9 tane (ARP) paketini **mustso'dan** yakaladık. ARP bizim için önemli bir bilgidir.



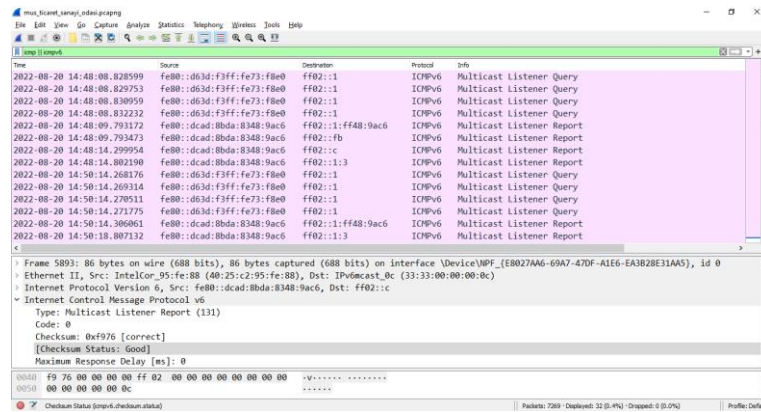
7. ICMP (Internet Control Message Protocol)

ICMP trafiği esas olarak hata mesajlarını taşımaya yöneliktir, bu nedenle ağdaki herhangi bir ICMP trafiği ilgi çekici olabilir. Ancak ICMP, bir saldırgan tarafından kasıtlı olarak kötüye kullanılabilir ve tarama ve veri hırsızlığı için kullanılabilir.

[Checksum Status: **Good**]

Birkaç ağ protokolü, veri bütünlüğünü sağlamak için sağlama toplamları kullanır. Burada açıklandığı gibi sağlama toplamlarının uygulanması, artıklık denetimi olarak da bilinir.

[**Good**], durumu iyi olduğu için bu bilgileri saldırgan kötü amaçlı olarak kullanılamıyor.



8. TCP RST

9. SCTP ABORT

10. TTL low or unexpected

11. Checksum Errors

12. SMB

8 - 12'ye kadar bir şey yakalamadık.

12. HTTP (Hypertext Transfer Protocol)

The image shows a Wireshark capture of HTTP traffic. The top pane displays a list of packets, with the selected packet (38555) highlighted. The middle pane shows the details of the selected packet, including the Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol layers. The bottom pane shows the raw data of the packet in hexadecimal and ASCII.

Time	Source	Destination	Protocol	Info
2022-08-20 10:50:26.169276	192.168.1.89	151.80.40.80	HTTP	OPTIONS / HTTP/1.1
2022-08-20 10:50:26.169361	192.168.1.89	151.80.40.80	HTTP	PROPFIND / HTTP/1.1
2022-08-20 10:50:26.169452	192.168.1.89	151.80.40.80	HTTP	GET /HNAP1 HTTP/1.1
2022-08-20 10:50:26.209584	192.168.1.89	151.80.40.80	HTTP	OPTIONS / HTTP/1.1
2022-08-20 10:50:26.209677	192.168.1.89	151.80.40.80	HTTP	GET /evox/about HTTP/1.1
2022-08-20 10:50:26.221960	192.168.1.89	151.80.40.80	HTTP	GET /evox/about HTTP/1.1
2022-08-20 10:50:26.222052	192.168.1.89	151.80.40.80	HTTP	PROPFIND / HTTP/1.1
2022-08-20 10:50:26.245562	151.80.40.80	192.168.1.89	HTTP	HTTP/1.1 301 Moved Permanently (text/html)
2022-08-20 10:50:26.249680	151.80.40.80	192.168.1.89	HTTP	HTTP/1.1 301 Moved Permanently (text/html)
2022-08-20 10:50:26.252764	151.80.40.80	192.168.1.89	HTTP	HTTP/1.1 301 Moved Permanently (text/html)
2022-08-20 10:50:26.253003	151.80.40.80	192.168.1.89	HTTP	HTTP/1.1 301 Moved Permanently (text/html)
2022-08-20 10:50:26.254408	151.80.40.80	192.168.1.89	HTTP	HTTP/1.1 301 Moved Permanently (text/html)
2022-08-20 10:50:26.263162	192.168.1.89	151.80.40.80	HTTP	GET /HNAP1 HTTP/1.1
2022-08-20 10:50:26.263258	192.168.1.89	151.80.40.80	HTTP	GET /.git/HEAD HTTP/1.1
2022-08-20 10:50:26.274004	192.168.1.89	151.80.40.80	HTTP	POST / HTTP/1.1 (application/x-www-form-urlencoded)

Frame 38555: 363 bytes on wire (2904 bits), 363 bytes captured (2904 bits) on interface \Device\NPF_{E8027AA6-69A7-47DF-A1E6-EA3B28E31AA5}, id 0
Ethernet II, Src: IntelCor_95:fe:88 (40:25:c2:95:fe:88), Dst: ZyxeCom_73:f8:e0 (d4:3d:f3:73:f8:e0)
Internet Protocol Version 4, Src: 192.168.1.89, Dst: 151.80.40.80
Transmission Control Protocol, Src Port: 1363, Dst Port: 80, Seq: 1, Ack: 1, Len: 309
Hypertext Transfer Protocol
POST / HTTP/1.1\r\n
User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)\r\n

0000 d4 3d f3 73 f8 e0 40 25 c2 95 fe 88 08 00 45 00 -.-s- @%E-
0010 01 5d 3f c5 40 00 80 06 38 34 c0 a8 01 59 97 50 -.]? @... 84...Y.P
0020 28 50 05 53 00 50 56 a8 5b 94 8c c8 e4 a2 50 18 (P-S-PV- [.....P-

Buradan tüm dosya isteklerini görebilirsiniz ama isterseniniz dosyaya gitmeniz gereken asıl dosya ve bu seçenek denir.

Nesneleri dışa aktarır ve tüm HTTP'yi görebilirsiniz

The image shows a Wireshark capture of HTTP traffic. The top pane displays a list of packets, with the selected packet (38142) highlighted. The middle pane shows the details of the selected packet, including the Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol layers. The bottom pane shows the raw data of the packet in hexadecimal and ASCII.

Time	Source	Destination	Protocol	Info
38139	2022-08-20 10:50:25.813619	192.168.1.89	151.80.40.80	HTTP GET /nmaplowercheck1660981825 HTTP/1.1
38140	2022-08-20 10:50:25.813721	192.168.1.89	151.80.40.80	HTTP GET / HTTP/1.1 , NTLMSSP_NEGOTIATE
38142	2022-08-20 10:50:25.837129	151.80.40.80	192.168.1.89	HTTP HTTP/1.1 301 Moved Permanently (text/html)

Window: 516
[Calculated window size: 132096]
[Window size scaling factor: 256]
Checksum: 0x1cfc [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[SEQ/ACK analysis]
TCP payload (217 bytes)

[Checksum Status: **Unverified**]

Packet	Hostname	Content Type	Size	Filename
38121	mustso.org.tr		441 bytes	sdik
38130	mustso.org.tr		441 bytes	sdik
38411			152 bytes	
38760			152 bytes	
72344	emdl.ws.microsoft.com	application/json	361 bytes	am_delta_patch_1.373.615.0_55dc2bd433f910f74a802aa20298f671c70d6862.exe.json
11957	ocsp.sectigo.com	application/ocsp-response	766 bytes	MFlwUDBOMewwSjAlBgUrDgMCgGUABBSmEJ7sDLVqQ%2FaFKR54j1BHqdkgQUGqH4YRkgD8NBd0UojtE1xwYSBFUCEQCMd6AAj%2FTRsMY9nzplg
7443	edgedl.me.gvt1.com	application/octet-stream	1120 bytes	hfnkpmilhgieaddgfemhofmblmnib_7529_all_ealbfmk5twdcj3wommi5jzwc4m.crx3
11165	edgedl.me.gvt1.com	application/octet-stream	172 bytes	hfnkpmilhgieaddgfemhofmblmnib_7529_all_ealbfmk5twdcj3wommi5jzwc4m.crx3
31917	edgedl.me.gvt1.com	application/octet-stream	2235 bytes	hfnkpmilhgieaddgfemhofmblmnib_7529_all_ealbfmk5twdcj3wommi5jzwc4m.crx3
32120	edgedl.me.gvt1.com	application/octet-stream	4023 bytes	hfnkpmilhgieaddgfemhofmblmnib_7529_all_ealbfmk5twdcj3wommi5jzwc4m.crx3
32144	edgedl.me.gvt1.com	application/octet-stream	10 kB	hfnkpmilhgieaddgfemhofmblmnib_7529_all_ealbfmk5twdcj3wommi5jzwc4m.crx3
32235	edgedl.me.gvt1.com	application/octet-stream	7352 bytes	hfnkpmilhgieaddgfemhofmblmnib_7529_all_ealbfmk5twdcj3wommi5jzwc4m.crx3
72358	au.download.windowsupdate.com	application/octet-stream	2 bytes	am_delta_patch_1.373.615.0_55dc2bd433f910f74a802aa20298f671c70d6862.exe
73040	au.download.windowsupdate.com	application/octet-stream	312 kB	am_delta_patch_1.373.615.0_55dc2bd433f910f74a802aa20298f671c70d6862.exe
74066	au.download.windowsupdate.com	application/octet-stream	1048 kB	am_delta_patch_1.373.615.0_55dc2bd433f910f74a802aa20298f671c70d6862.exe
74708	au.download.windowsupdate.com	application/octet-stream	1048 kB	am_delta_patch_1.373.615.0_55dc2bd433f910f74a802aa20298f671c70d6862.exe
7407	crfs.pki.goog	application/pkix-crl	11 kB	zdaT0Ev_Fk.crl
35895	crl.comodoca.com	application/pkix-crl	506 bytes	AAAACertificateServices.crl
62669	download.windowsupdate.com	application/vnd.ms-cab-compressed	7309 bytes	37410186_75cc048935ef30263eafda180efedd6bc8fa801c.cab
62693	download.windowsupdate.com	application/vnd.ms-cab-compressed	7319 bytes	37408720_1aeef9d3c5f388f392d2626d9ab180cf211bc18.cab
62751	download.windowsupdate.com	application/vnd.ms-cab-compressed	7317 bytes	37408721_60036ff5b5b1f24d5638f31110b6a180d3b29e98.cab
62822	download.windowsupdate.com	application/vnd.ms-cab-compressed	7313 bytes	37407254_7a93d465795c5a426a53d58ee0b8e4d6934fc08.cab
62863	download.windowsupdate.com	application/vnd.ms-cab-compressed	7313 bytes	37407253_2e7d0661d858b6c545e3d283554d96c8ef27a7cf.cab
62907	download.windowsupdate.com	application/vnd.ms-cab-compressed	10 kB	37413180_ce1e43cc02b9bfaab0f6804b58dc3db2c142b720.cab
62960	download.windowsupdate.com	application/vnd.ms-cab-compressed	10 kB	37412469_4a270de84a35257179cd7a270b6e8e2c5c65630.cab
62992	download.windowsupdate.com	application/vnd.ms-cab-compressed	10 kB	37412321_21f8064aca1a9b75fcd07e5c883ed6691c503e12.cab
63061	download.windowsupdate.com	application/vnd.ms-cab-compressed	10 kB	37411521_7e5592c79ca643fb72f022fec53741993fe81604.cab
63095	download.windowsupdate.com	application/vnd.ms-cab-compressed	10 kB	37411353_a39a34af973532e27e9bc8003b94876df1d8eb1.cab
63137	download.windowsupdate.com	application/vnd.ms-cab-compressed	10 kB	37410444_a49a0c25e282a57230a4e619b6f8e4f731e13ff6.cab
63164	download.windowsupdate.com	application/vnd.ms-cab-compressed	10 kB	37410302_6fc9910770ff8f9b1fcadbd0c41c6c3fa8f72.cab
63193	download.windowsupdate.com	application/vnd.ms-cab-compressed	10 kB	37408837_d517de8ffc9c0af67f2d3107a09a8291a4734ab4.cab
63210	download.windowsupdate.com	application/vnd.ms-cab-compressed	10 kB	37407370_9d385f648b6eebf9de6612f80eae7d06096148b.cab
64460	download.windowsupdate.com	application/vnd.ms-cab-compressed	7399 bytes	37411404_e32891188d29528f4da867b73b80cd28e2b777e.cab
64502	download.windowsupdate.com	application/vnd.ms-cab-compressed	7323 bytes	37411237_7eab953df624a7bea67993d1ef5a3beb48503744.cab
64546	download.windowsupdate.com	application/vnd.ms-cab-compressed	7315 bytes	37411235_66f31123736115f60600437c0b3c7e3e3d3370.cab

Çok fazla içerik türü(**content types**) En kiritik buldumuz kısımda **Application** buldundu kısımdır.

Kötü amaçlı ve yazılım ararken kullandığınız etiket **içerik türü** ve **uygulama türüdür**.

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.

Wireshark · Packet 38555 · mus_ticaret_saniye.pcapng
<ul style="list-style-type: none"> > Frame 38555: 363 bytes on wire (2904 bits), 363 bytes captured (2904 bits) on interface \Device\NPF_{E8027AA6-69A7-47DF-A1E6-EA} > Ethernet II, Src: IntelCor_95:fe:88 (40:25:c2:95:fe:88), Dst: ZyxelCom_73:f8:e0 (d4:3d:f3:73:f8:e0) > Internet Protocol Version 4, Src: 192.168.1.89, Dst: 151.80.40.80 > Transmission Control Protocol, Src Port: 1363, Dst Port: 80, Seq: 1, Ack: 1, Len: 309 > Hypertext Transfer Protocol <ul style="list-style-type: none"> > POST / HTTP/1.1\r\n <ul style="list-style-type: none"> User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)\r\n Connection: close\r\n Content-Type: application/x-www-form-urlencoded\r\n > Content-Length: 88\r\n Host: mustso.org.tr\r\n \r\n [Full request URI: http://mustso.org.tr/] [HTTP request 1/1] [Response in frame: 38658] File Data: 88 bytes > HTML Form URL Encoded: application/x-www-form-urlencoded

13. TCP (Transmission Control Protocol)

Varsayılan olarak, Wireshark'ın TCP ayırıcısı her TCP oturumunun durumunu izler ve sorunlar veya olası sorunlar algılandığında ek bilgi sağlar. Bir yakalama dosyası ilk açıldığında analiz her TCP paketi için bir kez yapılır. Paketler, paket listesinde görüldükleri sırayla işlenir.

The image displays two screenshots from the Wireshark network protocol analyzer. The top screenshot shows a packet capture of a TCP connection. The packet list on the left shows a sequence of packets, with packet 5191 highlighted in red, indicating a Reset (RST) packet. The packet details pane on the right shows the structure of this packet: Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The TCP section shows the source port as 443, destination port as 1714, sequence number as 170, and acknowledgment number as 594. The flags field is set to RST, ACK. The bottom screenshot shows the packet details pane for packet 5191, highlighting the 'Flags: 0x014 (RST, ACK)' field. The 'Sequence Number: 170' and 'Acknowledgment Number: 594' are also visible. The packet bytes pane at the bottom shows the raw data of the packet.

Yukardaki bilgileri heme iyi amaç ile ve hem kötü amaç ile kullanabiliriz, hack kavramını bildiğiniz gibi beyaz şapkalı ve siyah şapkalı hacker iki'sde bilgileri toplar, ama birisi iyi niyet ve birisi kötü niyet ile kullanabilir.

1. Bad TCP

Kısımında [Checksum Status: **Unverified**] olduğundan dolayı bu kısımları mustso'nun düzeltmesi gerekiyor.

12. HTTP

Kısımında [Checksum Status: **Unverified**] olduğundan dolayı bu kısımları mustso'nun düzeltmesi gerekiyor.