

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	Puan
190541021	Zeynep DEMİR	88
175541038	Ali Fuat KARAASLAN	83
16541044	Furkan BAŞAN	83
185542003	Burak DEMİRER	95
190541017	Rumeysa KOÇAK	93
175541006	Osman USLU	85
185541094	Alihan EYMİRLİ	90
16541071	Hazel OKTAY	79
15541061	Hidayet Can ULUBAŞ	79
175541611	Mohammad Amin ASLAMI	95
175541009	Alihan KOÇ	87

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, çözümleme, 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?

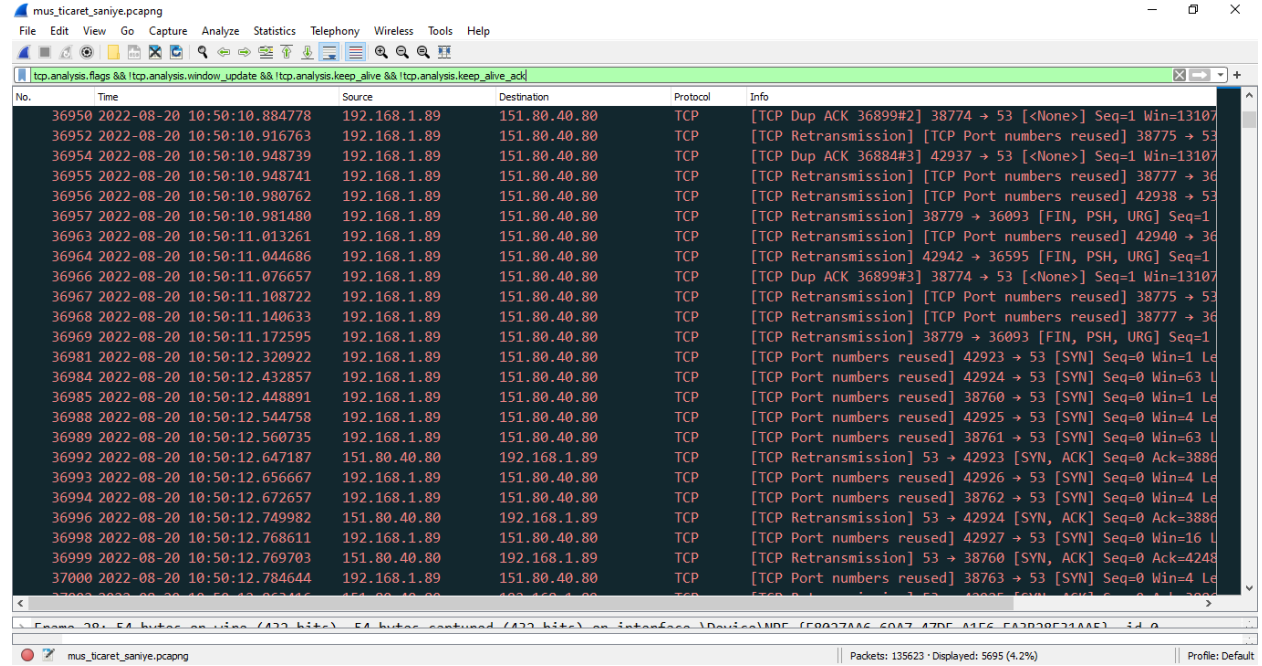
Performans sorunları olan ağlarda sorun giderme de dahil olmak üzere birçok kullanıma sahiptir. Siber güvenlik uzmanları genellikle bağlantıları izlemek, şüpheli ağ işlemlerinin içeriğini görüntülemek ve ağ trafiği patlamalarını belirlemek için bu yazılımı kullanır. Bu yazılım herhangi bir BT uzmanının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



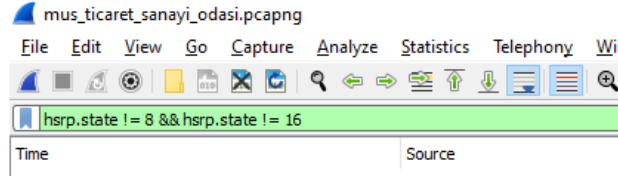
No.	Time	Source	Destination	Protocol	Info
36950	2022-08-20 10:50:10.884778	192.168.1.89	151.80.40.80	TCP	[TCP Dup ACK 36899#2] 38774 → 53 [None] Seq=1 Win=13107
36952	2022-08-20 10:50:10.916763	192.168.1.89	151.80.40.80	TCP	[TCP Retransmission] [TCP Port numbers reused] 38775 → 53
36954	2022-08-20 10:50:10.948739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

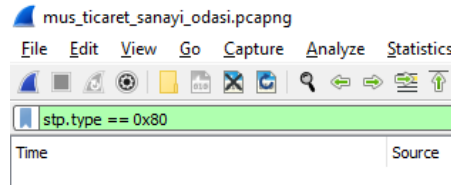
2. HSRP State Change (Hot Standby Redundancy Protocol)

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)

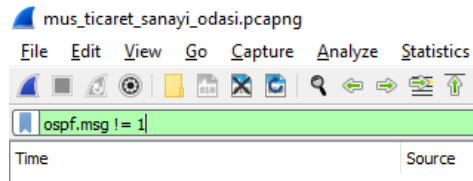
STP paketini **mustso'dan** her hangi bir ağ veya problem yakalamadık. Yani STP ile ilgili herhangi bir düzenleme gerek yoktur.



4. OSPF State Change (open shortest path first)

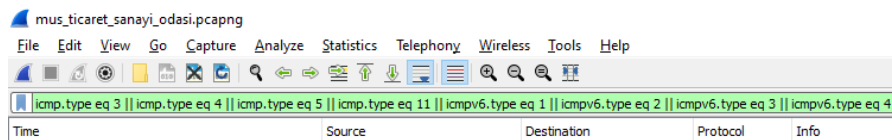
dinamik bir yönlendirme protokolüdür. Bir iç ağ geçidi protokolüdür (IGP). Yönlendiriciler, yönetici müdahalesine gerek kalmadan rotaları otomatik olarak öğrenmek için kullanır.

OSPF ile ilgili herhangi bir düzenleme gerek yoktur.



5. ICMP errors

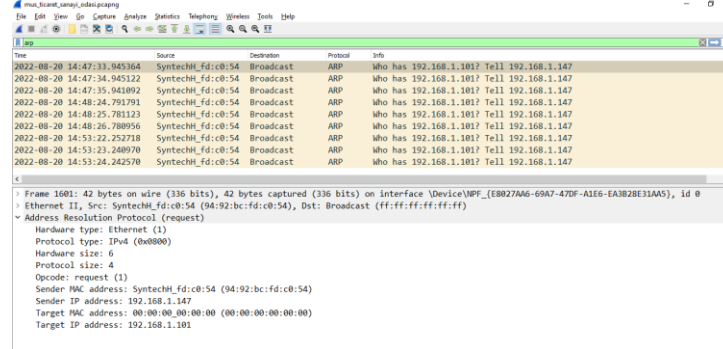
ICMP'deki hata verileri iki değerde taşınır: type ve code. Bir ICMP paketinin tipi, mesajın iletmeyi amaçladığı genel mesajı içerir. **Örneğin, 3 türündeki bir değer, amaçlanan varış noktasına ulaşılamadığı anlamına gelir**, ama bize herhangi bir ağ tarafını vermedi için düzgün çalıştığını bize göstermektedir.



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.



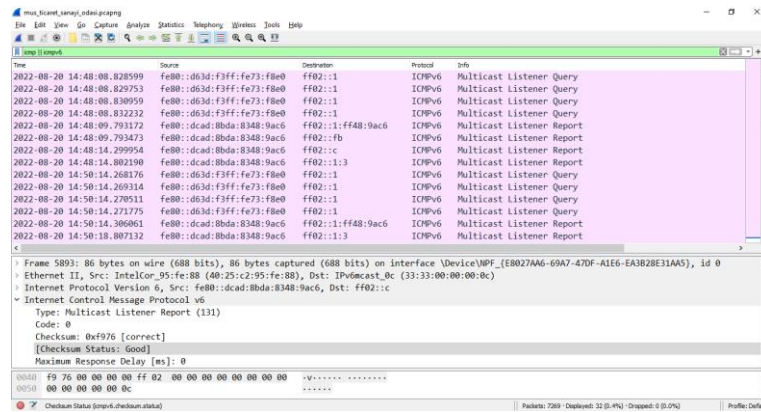
7. ICMP (Internet Control Message Protocol)

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 toplamaları kullanır. Burada açıklandığı gibi sağlama toplamalarının 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\nUser-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	sdh
38130	mustso.org.tr		441 bytes	sdh
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	zdaT0Ex_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_6fc9910770f8f9b1fcadbd0c41c6c3fa8f72.cab
63193	download.windowsupdate.com	application/vnd.ms-cab-compressed	10 kB	37408837_d517de8ffc90af67f2d3107a09a8291a4734ab4.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	37411236_6f631123736115f60600437c0b3c7e4d3370.cab

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

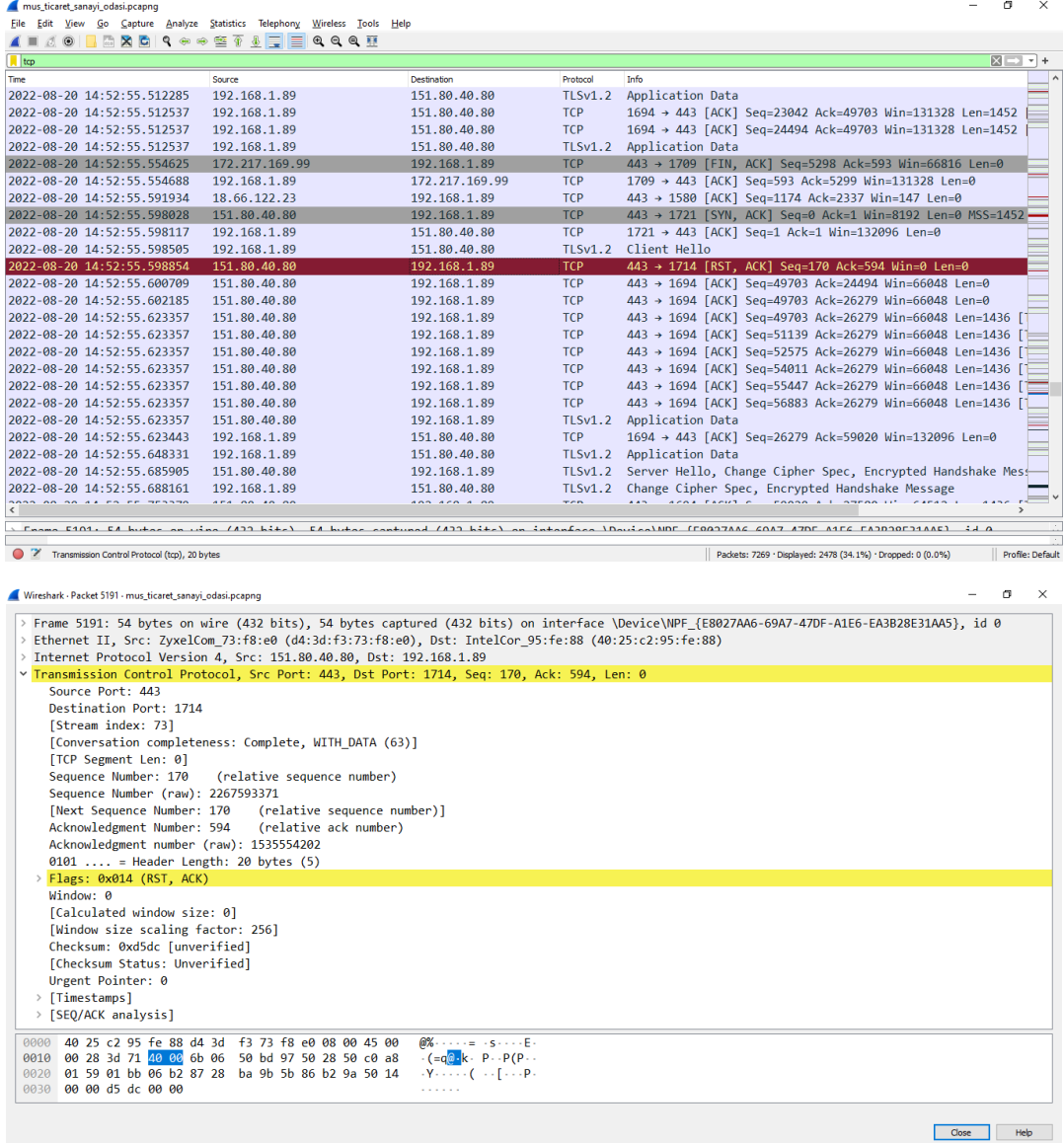
Kötü amaçlı ve yazılım ararken kullandığınız etiket **içerik türü** ve **uygulama türüdür**.

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
<p>> Frame 38555: 363 bytes on wire (2904 bits), 363 bytes captured (2904 bits) on interface \Device\NPF_{E8027AA6-69A7-47DF-A1E6-EA}</p> <p>> Ethernet II, Src: IntelCor_95:fe:88 (40:25:c2:95:fe:88), Dst: ZyxelCom_73:f8:e0 (d4:3d:f3:73:f8:e0)</p> <p>> Internet Protocol Version 4, Src: 192.168.1.89, Dst: 151.80.40.80</p> <p>> Transmission Control Protocol, Src Port: 1363, Dst Port: 80, Seq: 1, Ack: 1, Len: 309</p> <p>> Hypertext Transfer Protocol</p> <p>> POST / HTTP/1.1\r\n</p> <p>User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)\r\n</p> <p>Connection: close\r\n</p> <p>Content-Type: application/x-www-form-urlencoded\r\n</p> <p>> Content-Length: 88\r\n</p> <p>Host: mustso.org.tr\r\n</p> <p>\r\n</p> <p>[Full request URI: http://mustso.org.tr/]</p> <p>[HTTP request 1/1]</p> <p>[Response in frame: 38658]</p> <p>File Data: 88 bytes</p> <p>> HTML Form URL Encoded: application/x-www-form-urlencoded</p>

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.



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.

Wireshark ile ICMP Paket Analizi

ICMP (Internet Control Message Protocol), hata mesajları ve [TCP/IP](#) yazılımının bir takım kendi mesaj trafiği amaçları için kullanılır. Hataları raporlamak için kullanılan, kontrol amaçlı bir protokoldür. Bu şekilde normal kullanımının yanında, uzak sistem hakkında bilgi toplamak için sıkça kullanıldığından çok önemlidir.

IP header	ICMP header	ICMP payload size	MTU (1500)
20 bytes	8 bytes	1472 bytes (maximum)	$20 + 8 + 1472 = 1500$

Network katmanında ICMP paketi

Ethernet header	IP header	ICMP header	ICMP payload size	MTU (1514)
14	20 bytes	8 bytes	1472 bytes (maximum)	$14 + 20 + 8 + 1472 = 1514$

Veri Link katmanında ICMP paketi

ICMP neden kullanılır:

- [TTL](#) süresi dolduğu zaman paketin sahibine bildirim yapmak
- Herhangi bir durumda yok edilen paket hakkında geri bildirim sağlamak
- Parçalanmasın komutu verilmiş paket parçalandığında geri bildirim sağlamak
- Hata oluşumlarında geri bildirim sağlamak
- Paket başka bir yoldan gideceği zaman geri bildirim sağlamak

ICMP hata ve durum raporlama prosedürleri

ICMP tarafından rapor edilen hata ve durum raporlama servisleri aşağıda listelenmiştir.

Tıp Kodu Değeri	ICMP Mesajın Tipi
0	Eko yanıt-ping yanıtı (Echo Reply)
3	Hedefe Erişilemedi (Destination Not Reachable)
4	Kaynak Kapatmak (Source Quench)
5	Yeniden Yönlendirme (Redirection Required)
8	Eko yanıt-ping isteği (Echo Request)
9	Yönlendirici tanıtımı
10	Yönlendirici istemi
11	Zaman aşımı—traceroute kullanır (Time to Live Exceeded)
12	Parametre Problemi (Parameter Problem)
13	Timestamp İstemi (Timestamp Request)
14	Timestamp Yanıtı (Timestamp Reply)
15	Bilgi İstemi (Information Request)
16	Bilgi Yanıtı (Information Reply)
17	Adres Maskesi İstemi (Address Mask Request)
18	Adres Maskesi yanıtı (Address Mask Reply)

ICMP mesaj tipleri ile internet üzerinde kontrol amaçlı birçok program yazılması olasıdır. Örneğin timestamp mesajları kullanılarak internet üzerindeki gecikmeler ölçülebilir.

ICMP sorgulaması

Ping taraması bir ICMP uygulamasıdır ama bir sistem hakkında ICMP sorgulaması yapmak sadece ping paketleri ile yapılmaz. Bir sisteme birçok yoldan ICMP sorgulaması yapılabilir ve çok değerli bilgiler elde edilebilir. Mesela, Unix tabanlı sistemlerde kullanılan "icmpquery" ya da "icmppush" uygulaması sayesinde sistemin saati(hangi zaman bölgesinde olduğu) "ICMP type 13" (TIMESTAMP) ile öğrenilebilir ya da bir hostun hangi ağ maskesinde olduğu "ICMP type 17" (ADDRESS MASK REQUEST) mesajı ile elde edilebilir. [Ağ](#) maskesi(Netmask) bilgisi önemlidir, çünkü saldırgan sadece belli bir alt ağdaki(subnet) sisteme saldırmak isteyebilir. Burada dikkat edilmesi gereken bir nokta da tüm yönlendiricilerin ICMP TIMESTAMP ya da ICMP NETMASK sorgulamasına cevap vermedikleridir.

Önlemler

ICMP sorgulamasını engellemek, ilgili ICMP tiplerini (ICMP TIMESTAMP - type 13 gibi) bloke etmekle yapılabilir. Cisco yönlendiricilerde bu engelleme genişletilmiş erişim listesiyle şöyle yapılır:

```
Access-list 101 deny icmp any any 13
```

Ancak ICMP paketlerini engellemek, ağdaki sorunların çözülmesini geciktirebilir. ICMP sorgulaması saldırı tespit programları ile rahatlıkla gözlemlenebilir.

ICMP uygulamaları

Basit ve sıkça kullanılan 2 tane ICMP uygulaması vardır: [Ping](#) ve [Traceroute](#). Daha çok ağ üzerindeki sorunları tespit edebilmek ya da çözmek için kullanılan bu 2 uygulama aynı zamanda, hacking işleminin başlangıç aşamalarından birini oluşturur. Ağdaki canlı makineleri bulabilmek için ping taramaları ya da ağın haritasını çıkartabilmek için traceroute uygulamaları hacker'ler tarafından sıkça kullanılır.

Ping en basit TCP/IP uygulamasıdır. Bir hosta ulaşmanın ilk adımı ona ping çekmektir. Eğer bir hosta [ping](#) ile ulaşabiliyorsanız, [telnet](#) ya da [FTP](#) ile ulaşmanız (ilgili portlar açıksa) mümkündür. Son yıllarda güvenlik duvarlarının yönlendiricilerdeki "access list"lerin ve diğer güvenlik kontrol mekanizmalarının sıkça kullanılmaya başlanmasıyla bu yargı değişmeye başlamıştır. Yani bir hosta ping çekemiyorsanız, telnet ya da ftp yapamayacağınız anlamına gelmez. Ping uygulaması, ICMP Echo ve ICMP Reply mesajlarını kullanarak bir hostun erişilebilir olup olmadığını belirler. Ping, alıcı bilgisayara "echo request" paketi gönderirken, cevap olarak da "echo reply" paketini bekler. Traceroute programı ise

gönderen bilgisayardan alıcı bilgisayara giden paket ve izlediği yolla ilgili çok önemli bilgiler verir. Bu bilgiler arasında en çok kullanılanı "paketin izlediği yol (path)" bilgisidir. Bu sayede paketin hangi yollardan geçerek alıcı hosta ulaştığı rahatlıkla izlenebilir. Traceroute programı ICMP protokolünün bir parçasıdır. ICMP protokolü, iki host arasında bilgi akışı olurken, bu esnada ortaya çıkan hataları ve diğer bilgileri mesaj yoluyla raporlar.

Wireshark ile ICMP Mesaj Kodu & Paketlerin Açıklanması

ICMP mesajının query ve error olmak üzere iki tipi vardır.

Query:

Sorgu mesajları hedef cihazdan veya router dan aldığımız bilgileri içerir.

Bu yazıda kullanılan ICMP query kodları:

- Type 0 : Echo Reply
- Type 8: Echo Request

Ping komutu hedef cihaza “echo request” gönderir. Eğer hedef cihazdan “echo Reply” cevabı alırsa cihaz ayakta demektir.

Yankı (Echo): Yankı mesajları, bir yönlendirici(Router) veya bilgisayar tarafından diğer bir yönlendirici veya bilgisayara gönderilen mesajlardır. Yankı mesajı kaynaktan hedefe yönelen bir mesaj olup, yankı mesajı olarak hedeften kaynağa Yankı Cevabı (Echo Reply) mesajı döner. Yankı mesajı ile hedef bilgisayarın çalışıp çalışmadığı ve iletişim kurmak için gerekli yolun sağlanıp sağlanamayacağının testi yapılır. TCP / IP protokol grubu yüklü olan bilgisayarlar üzerinde çalıştırılan Ping komutu bu işlevi yerine getirir. Ping isteğini gönderen cihaz (Yankı İsteği) Echo Request'te bulunur. ICMP mesajlarındaki Yankı İsteği Tipi (Echo Request Type) 8 ve Kod(Code) 0'dır.Hedef IP adresi Yankı İsteği (Echo Request)

mesajını aldığı anda gönderen cihaza Yankı Cevabı(Echo Reply) mesajını gönderir. Bu mesajın Tip'i (Type) ve Kod'u (Code) 0'dır.

Önce mustso.org.tr domainimize ping atarak ip adresinin 151.80.40.80 olduğunu öğrendim ve hemen ardından kali üzerinde wiresharkı açarak filter kısmında icmp yi seçtim.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	151.80.40.80	ICMP	98	Echo (ping) request id=0x0ce4, seq=963/49923, ttl=64 (reply in 2)
2	0.000977682	151.80.40.80	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0ce4, seq=963/49923, ttl=108 (request in 1)
5	1.000743935	10.0.2.15	151.80.40.80	ICMP	98	Echo (ping) request id=0x0ce4, seq=964/50179, ttl=64 (reply in 6)
6	1.001075701	151.80.40.80	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0ce4, seq=964/50179, ttl=108 (request in 5)
9	2.002541182	10.0.2.15	151.80.40.80	ICMP	98	Echo (ping) request id=0x0ce4, seq=965/50435, ttl=64 (reply in 10)
10	2.111915903	151.80.40.80	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0ce4, seq=965/50435, ttl=108 (request in 9)
13	3.005112706	10.0.2.15	151.80.40.80	ICMP	98	Echo (ping) request id=0x0ce4, seq=966/50691, ttl=64 (reply in 14)
14	3.101803060	151.80.40.80	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0ce4, seq=966/50691, ttl=108 (request in 13)
17	4.006231791	10.0.2.15	151.80.40.80	ICMP	98	Echo (ping) request id=0x0ce4, seq=967/50947, ttl=64 (reply in 18)
18	4.095924565	151.80.40.80	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0ce4, seq=967/50947, ttl=108 (request in 17)
21	5.008520328	10.0.2.15	151.80.40.80	ICMP	98	Echo (ping) request id=0x0ce4, seq=968/51203, ttl=64 (reply in 22)
22	5.114080623	151.80.40.80	10.0.2.15	ICMP	98	Echo (ping) reply id=0x0ce4, seq=968/51203, ttl=108 (request in 21)
25	6.000485010	10.0.2.15	151.80.40.80	ICMP	98	Echo (ping) request id=0x0ce4, seq=969/51459, ttl=64 (reply in 26)

TTL=64 : Hedef makine Linux işletim sistemine sahiptir.

```
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x6f79 [correct]
[Checksum Status: Good]
Identifier (BE): 3300 (0x0ce4)
Identifier (LE): 58380 (0xe40c)
Sequence Number (BE): 963 (0x03c3)
Sequence Number (LE): 49923 (0xc303)
[Response frame: 2]
Timestamp from icmp data: Aug 26, 2022 14:02:44.000000000 EDT
```

Birinci paket kaynaktan gönderilen ICMP echo request 'dir. Yukarıda çizili olan karede ICMP query kodun "Type 8 echo ping request" olduğunu görüyoruz.

```
Internet Control Message Protocol
Type: 0 (Echo (ping) reply)
Code: 0
Checksum: 0x7779 [correct]
[Checksum Status: Good]
Identifier (BE): 3300 (0x0ce4)
Identifier (LE): 58380 (0xe40c)
Sequence Number (BE): 963 (0x03c3)
```

Benzer şekilde hedef cihazdan dönen ikinci paketin yukarıda belirtilmiş olan "Type 0 echo ping reply" olduğunu görüyoruz.

Teşekkürler: Wireshark Gurubu