Protokoły komunikacyjne

Analiza i charakterystyka

Zbigniew Bojkiw gr. 11

Zawartość

Wprowadzenie

Praca ta ma na celu charakterystykę i analizę działania wybranych protokołów komunikacyjnych. Aby osiągnąć cel autor pracy analizuje protokoły za pomocą analizatora sieciowego Wireshark umożliwiającego dokładną analizę przesyłanych danych w podsieci, do której jest podłączony komputer.

W kolejnych rozdziałach pracy znajduje się charakterystyka wybranych protokołów sieciowych oraz przykłady zastosowania tych protokołów będące podstawą do analizy ich działania.

Każdy z przykładów posiada własny log z programu Wireshark pokazujący ruch pakietów sieciowych w obrębie danej operacji.

Wszystkie przykłady wykonane zostały w lokalnej sieci domowej składającej się z kilku komputerów połączonych do sieci Internet za pomocą routera posiadającego publiczny, zmienny adres IP

Uwaga: Dane takie jak adresy fizyczne MAC, nazwy użytkowników, hasła oraz inne dane, których autor nie chce lub nie może ujawniać, zostały odpowiednio ocenzurowane.

Charakterystyka wybranych protokołów komunikacyjnych

W niniejszej pracy wykorzystano 4 protokoły internetowe, które są powszechnie wykorzystywane przy komunikacji pomiędzy urządzeniami w sieci i przedstawiono ich działanie na przykładzie kilku, często wykonywanych operacji.

Wykorzystane protokoły to:

1. ARP (ang. Address Resolution Protocol).
2. ICMP (ang. Internet Control Message Protocol).
3. DNS (ang. Domain Name System)
4. FTP (ang. File Transfer Protocol)

Protokół ARP

Warstwa TPC/IP

ARP jest protokołem pracującym na warstwie łącza, która zawiera protokoły obsługujące niskopoziomową transmisję pakietów

Zastosowanie

Protokół ARP poprzez umożliwienie przekształcania 32-*bitowych* adresów *IP* (ustalanych autorytarnie przez użytkownika/administratora) na fizyczne, 48-bitowe adresy *MAC* (przypisane fizycznie m.in. do *kart sieciowych*), pozwala na znajdowania adresu sprzętowego hosta (MAC), gdy dany jest adres warstwy sieciowej.

Protokół ICMP

Warstwa TPC/IP

Protokół ICMP pracuje na warstwie sieciowej. Ramki protokołów warstwy sieciowej są transportowane przez protokoły z warstwy łącza.

Zastosowanie

Protokół ten jest wykorzystywany w diagnostyce sieci oraz trasowaniu i pełni funkcję kontroli transmisji w sieci.

Protokół DNS

Zastosowanie

Protokół DNS umożliwia zamianę adresów znanych użytkownikom Internetu na adresy zrozumiałe dla urządzeń tworzących sieć komputerową.

Protokół FTP

Warstwa TPC/IP

FTP jest protokołem pracującym na warstwie aplikacji. Protokoły tej warstwy zawierają się jako dane w protokołach warstwy transportowej.

Zastosowanie

Protokół FPT jest protokołem typu klient-serwer i umożliwia przesyłanie plików z i na serwer poprzez sieć TCP/IP.

Odnajdywanie adresu MAC bramy sieciowej za pomocą protokołu ARP

Stacja AsustekC_b7:70:8b wykorzystuje protokół ARP (ang. Address Resolution Protocol) by odnaleźć adres sprzętowy karty sieciowej Ethernet (MAC) stacji, która jest bramą sieciową (gateway) dla AsustekC_b7:70:8b.

Log przechwyconych pakietów

L.p.	Czas	Źródło	Przeznaczenie	Protokół	Informacje
8	6.388402	AsustekC_b7:70:8b	Broadcast	ARP	Who has 10.0.0.2? Tell 10.0.0.4
9	6.388914	Pro-Nets_54:40:d4	AsustekC_b7:70:8b	ARP	10.0.0.2 is at XX:XX:XX:54:40:d4

Opis poszczególnych pozycji logu

Frame 8 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

Frame 9 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4), Dst: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b)
Address Resolution Protocol (reply)

8. Stacja AsustekC_b7:70:8b, która posiada w sieci lokalnej adres IP o numerze 10.0.0.4 potrzebuje adresu MAC stacji o adresie IP 10.0.0.2, będącej bramą sieciową dla stacji AsustekC_b7:70:8b. Aby uzyskać te dane, stacja AsustekC_b7:70:8b wysyła ramkę rozgłoszeniową (broadcast) o adresie docelowym MAC w postaci ff:ff:ff:ff:ff:ff, która zawiera adres 10.0.0.2 i dociera do wszystkich stacji w podsieci
9. Z definicji bramy sieciowej wynika, że musi się znajdować w tej samej podsieci co stacja, dla której jest bramą. Dlatego otrzyma ramkę rozgłoszeniową wysłaną przez AsustekC_b7:70:8b

i odpowie na nią przesyłając swój adres MAC. W tym momencie stacja o adresie IP 10.0.04 zna adres MAC swojej bramy, więc może zacząć wysyłać pakiety IP do stacji znajdujących się w innych podsieciach.

Ping

Ping to program używany w sieciach komputerowych TCP/IP, który służy do diagnozowania połączeń sieciowych. Za jego pomocą można sprawdzić czy istnieje połączenie pomiędzy dwiema testowanymi stacjami oraz określić jego jakość. Do tego typu testów wykorzystuje się protokół ICMP (ang. Internet Control Message Protocol). Działanie ping polega na wysyłaniu przez jedną stację pakietów ICMP Echo Request do innej stacji w tej samej, lub innej podsieci i odbieraniu od niej ICMP Echo Reply.

Ping do stacji z tej samej podsieci

Ponieważ stacja do której wysłano ping znajduje się w tej samej podsieci co AsustekC_b7:70:8b, musi on odnaleźć adres sprzętowy karty sieciowej Ethernet (MAC) tej stacji wykorzystując protokół ARP (ang. Address Resolution Protocol).

Logi przechwyconych pakietów

L.p.	Czas	Źródło	Przeznaczenie	Protokół	Informacje
51	60.599810	AsustekC_b7:70:8b	Broadcast	ARP	Who has 10.0.0.8? Tell 10.0.0.4
52	60.603297	XX:XX:XX:2e:58:02	AsustekC_b7:70:8b	ARP	10.0.0.8 is at XX:XX:XX:2e:58:02
53	60.603320	10.0.0.4	10.0.0.8	ICMP	Echo (ping) request
54	60.604477	10.0.0.8	10.0.0.4	ICMP	Echo (ping) reply

Opis poszczególnych pozycji logu

Frame 51 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

Frame 52 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: XX:XX:XX:2e:58:02 (XX:XX:XX:2e:58:02), Dst: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b)
Address Resolution Protocol (reply)

Frame 53 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b), Dst: XX:XX:XX:2e:58:02 (XX:XX:XX:2e:58:02)
Internet Protocol, Src: 10.0.0.4 (10.0.0.4), Dst: 10.0.0.8 (10.0.0.8)
Internet Control Message Protocol

Frame 54 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: XX:XX:XX:2e:58:02 (XX:XX:XX:2e:58:02), Dst: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b)
Internet Protocol, Src: 10.0.0.8 (10.0.0.8), Dst: 10.0.0.4 (10.0.0.4)
Internet Control Message Protocol

51. Aby wysłać pakiet ICMP Echo Request do stacji o adresie IP 10.0.0.8, AsustekC_b7:70:8b posiadający adres IP 10.0.0.4, potrzebuje adresu sprzętowego karty sieciowej Ethernet (MAC) tej stacji, gdyż oba komputery znajdują się w tej samej podsieci. W tym celu, stacja

AsustekC_b7:70:8b korzystając z protokołu ARP (ang. Address Resolution Protocol). wysyła ramkę rozgłoszeniową (broadcast) o adresie docelowym MAC w postaci ff:ff:ff:ff:ff:ff, która zawiera adres 10.0.0.8 i dociera do wszystkich stacji w podsieci.

52. Ponieważ stacja o adresie IP 10.0.0.8 znajduje się w tej samej podsieci co AsustekC_b7:70:8b, otrzyma ramkę rozgłoszeniową wysłaną przez stację o adresie IP 10.0.0.4 i odpowie na nią przesyłając swój adres MAC. W tym momencie AsustekC_b7:70:8b, zna adres MAC stacji o numerze IP 10.0.0.8 i może do niej wysłać pakiet ICMP Echo Request.
53. AsustekC_b7:70:8b wysyła ICMP Echo Request na stację o adresie IP 10.0.0.8.
54. Stacja o adresie IP 10.0.0.8 odbiera pakiet ICMP Echo Request i odpowiada wysyłając pakiety ICMP Echo Reply adres IP 10.0.0.4, czyli na adres stacji AsustekC_b7:70:8b. Dzięki temu możemy wnioskować, że połączenie pomiędzy stacjami działa.

Uwaga: Zwykle ping wysyła kilka zapytań ICMP Echo Request i dla każdego z nich odbiera odpowiedź w postaci pakietu ICMP Echo Reply dlatego punkty 53 i 54 mogą być powtarzane.

Ping dla stacji z innej podsieci przy użyciu adresu domenowego

Ponieważ stacja do której wysłano ping została zaadresowana za pomocą domeny, konieczna będzie zamiana adresu domenowego tejże stacji na adres IP za pomocą protokołu DNS (ang. Domain Name System).

Logi przechwyconych pakietów

L.p.	Czas	Źródło	Przeznaczenie	Protokół	Informacje
40	45.808432	10.0.0.4	10.0.0.2	DNS	Standard query A www.ue.wroc.pl
41	45.820680	10.0.0.2	10.0.0.4	DNS	Standard query response A 156.17.118.245
42	45.825472	10.0.0.4	156.17.118.245	ICMP	Echo (ping) request
43	45.868919	156.17.118.245	10.0.0.4	ICMP	Echo (ping) reply

Opis poszczególnych pozycji logu

Frame 40 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b), Dst: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4)
Internet Protocol, Src: 10.0.0.4 (10.0.0.4), Dst: 10.0.0.2 (10.0.0.2)
User Datagram Protocol, Src Port: 55364 (55364), Dst Port: domain (53)
Domain Name System (query)

Frame 41 (90 bytes on wire, 90 bytes captured)
Ethernet II, Src: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4), Dst: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b)
Internet Protocol, Src: 10.0.0.2 (10.0.0.2), Dst: 10.0.0.4 (10.0.0.4)
User Datagram Protocol, Src Port: domain (53), Dst Port: 55364 (55364)
Domain Name System (response)

Frame 42 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b), Dst: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4)
Internet Protocol, Src: 10.0.0.4 (10.0.0.4), Dst: 156.17.118.245 (156.17.118.245)
Internet Control Message Protocol

Frame 43 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4), Dst: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b)

Internet Protocol, Src: 156.17.118.245 (156.17.118.245), Dst: 10.0.0.4 (10.0.0.4)
Internet Control Message Protocol

40. Aby wysłać pakiet ICMP Echo Request do stacji o adresie domenowym www.ue.wroc.pl, AsustekC_b7:70:8b o adresie IP 10.0.0.4 potrzebuje adres IP tej stacji. Aby go uzyskać, za pomocą protokołu DNS, AsustekC_b7:70:8b wysyła do swojej bramy sieciowej o adresie IP 10.0.0.2 zapytanie o adres IP stacji, dla której zarejestrowano domenę www.ue.wroc.pl.
41. Brama domyślna po otrzymaniu zapytania od AsustekC_b7:70:8b przesyła je do jednego z dwóch serwerów DNS dostawcy usług internetowych (providera), których zadaniem jest dalsze przesyłanie zapytania do jednego z 13 głównych serwerów DNS, które są odpowiedzialne za domeny najwyższego poziomu (TLD – top level domains). Jeżeli wybrany przez nas adres jest rozpoznany za pomocą jednego z tych serwerów, zostanie on zamieniony na adres IP i powróci poprzez serwery providera do bramy sieciowej. W innym wypadku przeszukane zostaną serwery DNS niższego poziomu wskazane przez serwer główny. Gdy do bramy sieciowej powróci już odpowiedź w formie adresu IP stacji o adresie domenowym www.ue.wroc.pl, zostanie ona przesłana do stacji AsustekC_b7:70:8b.
42. Za pomocą protokołu DNS AsustekC_b7:70:8b ustalił, że stacja o adresie domenowym www.ue.wroc.pl posiada adres IP o numerze 156.17.118.245. Dzięki temu może on wysłać na ten adres pakiet ICMP Echo Request.
43. Stacja o adresie IP 156.17.118.245 odbiera pakiet ICMP Echo Request i jeżeli nie została skonfigurowana tak, aby blokować pakiety ICMP Echo Reply, to zostaną one przesłane w ramach odpowiedni na adres IP 10.0.0.4, czyli na adres stacji AsustekC_b7:70:8b.

Uwaga: Zwykle ping wysyła kilka zapytań ICMP Echo Request i dla każdego z nich odbiera odpowiedź w postaci pakietu ICMP Echo Reply dlatego punkty 42 i 43 mogą być powtarzane.

FTP

Logowanie do serwera FTP przy użyciu adresu domenowego

Logi przechwyconych pakietów

L.p.	Czas	Źródło	Przeznaczenie	Protokół	Informacje
2	0.206535	10.0.0.4	10.0.0.2	DNS	Standard query A ftp.60free.ovh.org
3	0.219562	10.0.0.2	10.0.0.4	DNS	Standard query response A 91.121.126.69
7	0.546334	91.121.126.69	10.0.0.4	FTP	Response: 220 Welcome to the OVH free hosting FTP server. Please login...
8	0.561309	10.0.0.4	91.121.126.69	FTP	Request: USER *użytkownik*
10	0.606184	91.121.126.69	10.0.0.4	FTP	Response: 331 Password required for *użytkownik*
11	0.622664	10.0.0.4	91.121.126.69	FTP	Request: PASS *hasło*
13	0.730522	91.121.126.69	10.0.0.4	FTP	Response: 230-Last login from: *publiczny adres ip* at *data*. Login count:*liczba logowań*.
15	0.976516	91.121.126.69	10.0.0.4	FTP	Response: 230 User *użytkownik* logged in
16	0.982649	10.0.0.4	91.121.126.69	FTP	Request: SYST

18	1.026033	91.121.126.69	10.0.0.4	FTP	Response: 215 UNIX Type: L8
19	1.044214	10.0.0.4	91.121.126.69	FTP	Request: FEAT
20	1.087709	91.121.126.69	10.0.0.4	FTP	Response: 211-Features:
22	1.303958	91.121.126.69	10.0.0.4	FTP	Response: 211 End
23	1.340668	10.0.0.4	91.121.126.69	FTP	Request: PWD
24	1.383666	91.121.126.69	10.0.0.4	FTP	Response: 257 / is the current directory
25	1.498263	10.0.0.4	91.121.126.69	FTP	Request: TYPE A
26	1.541055	91.121.126.69	10.0.0.4	FTP	Response: 200 Type set to A
27	1.560414	10.0.0.4	91.121.126.69	FTP	Request: PASV
28	1.603806	91.121.126.69	10.0.0.4	FTP	Response: 227 Entering Passive Mode (91,121,126,69,191,24).
32	1.683436	10.0.0.4	91.121.126.69	FTP	Request: LIST
33	1.727010	91.121.126.69	10.0.0.4	FTP	Response: 150 Opening ASCII mode data connection for file list
40	1.959854	91.121.126.69	10.0.0.4	FTP	Response: 226 Transfer complete

Opis poszczególnych pozycji logu

Frame 2 (78 bytes on wire, 78 bytes captured)
Ethernet II, Src: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b), Dst: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4)
Internet Protocol, Src: 10.0.0.4 (10.0.0.4), Dst: 10.0.0.2 (10.0.0.2)
User Datagram Protocol, Src Port: 64905 (64905), Dst Port: domain (53)
Domain Name System (query)

Frame 3 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4), Dst: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b)
Internet Protocol, Src: 10.0.0.2 (10.0.0.2), Dst: 10.0.0.4 (10.0.0.4)
User Datagram Protocol, Src Port: domain (53), Dst Port: 64905 (64905)
Domain Name System (response)

Frame 7 (119 bytes on wire, 119 bytes captured)
Ethernet II, Src: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4), Dst: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b)
Internet Protocol, Src: 91.121.126.69 (91.121.126.69), Dst: 10.0.0.4 (10.0.0.4)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 1362 (1362), Seq: 1, Ack: 1, Len: 65
File Transfer Protocol (FTP)

Frame 8 (66 bytes on wire, 66 bytes captured)
Ethernet II, Src: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b), Dst: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4)
Internet Protocol, Src: 10.0.0.4 (10.0.0.4), Dst: 91.121.126.69 (91.121.126.69)
Transmission Control Protocol, Src Port: 1362 (1362), Dst Port: ftp (21), Seq: 1, Ack: 66, Len: 12
File Transfer Protocol (FTP)

Frame 10 (87 bytes on wire, 87 bytes captured)
Ethernet II, Src: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4), Dst: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b)
Internet Protocol, Src: 91.121.126.69 (91.121.126.69), Dst: 10.0.0.4 (10.0.0.4)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 1362 (1362), Seq: 66, Ack: 13, Len: 33
File Transfer Protocol (FTP)

Frame 11 (70 bytes on wire, 70 bytes captured)
Ethernet II, Src: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b), Dst: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4)
Internet Protocol, Src: 10.0.0.4 (10.0.0.4), Dst: 91.121.126.69 (91.121.126.69)
Transmission Control Protocol, Src Port: 1362 (1362), Dst Port: ftp (21), Seq: 13, Ack: 99, Len: 16
File Transfer Protocol (FTP)

Frame 13 (131 bytes on wire, 131 bytes captured)
Ethernet II, Src: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4), Dst: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b)
Internet Protocol, Src: 91.121.126.69 (91.121.126.69), Dst: 10.0.0.4 (10.0.0.4)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 1362 (1362), Seq: 99, Ack: 29, Len: 77
File Transfer Protocol (FTP)

Frame 15 (80 bytes on wire, 80 bytes captured)
Ethernet II, Src: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4), Dst: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b)
Internet Protocol, Src: 91.121.126.69 (91.121.126.69), Dst: 10.0.0.4 (10.0.0.4)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 1362 (1362), Seq: 176, Ack: 29, Len: 26
File Transfer Protocol (FTP)

Frame 16 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b), Dst: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4)
Internet Protocol, Src: 10.0.0.4 (10.0.0.4), Dst: 91.121.126.69 (91.121.126.69)
Transmission Control Protocol, Src Port: 1362 (1362), Dst Port: ftp (21), Seq: 29, Ack: 202, Len: 6
File Transfer Protocol (FTP)

Frame 18 (73 bytes on wire, 73 bytes captured)
Ethernet II, Src: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4), Dst: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b)
Internet Protocol, Src: 91.121.126.69 (91.121.126.69), Dst: 10.0.0.4 (10.0.0.4)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 1362 (1362), Seq: 202, Ack: 35, Len: 19
File Transfer Protocol (FTP)

Frame 19 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b), Dst: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4)
Internet Protocol, Src: 10.0.0.4 (10.0.0.4), Dst: 91.121.126.69 (91.121.126.69)
Transmission Control Protocol, Src Port: 1362 (1362), Dst Port: ftp (21), Seq: 35, Ack: 221, Len: 6
File Transfer Protocol (FTP)

Frame 20 (210 bytes on wire, 210 bytes captured)
Ethernet II, Src: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4), Dst: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b)
Internet Protocol, Src: 91.121.126.69 (91.121.126.69), Dst: 10.0.0.4 (10.0.0.4)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 1362 (1362), Seq: 221, Ack: 41, Len: 156
File Transfer Protocol (FTP)

Frame 22 (63 bytes on wire, 63 bytes captured)
Ethernet II, Src: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4), Dst: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b)
Internet Protocol, Src: 91.121.126.69 (91.121.126.69), Dst: 10.0.0.4 (10.0.0.4)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 1362 (1362), Seq: 377, Ack: 41, Len: 9
File Transfer Protocol (FTP)

Frame 23 (59 bytes on wire, 59 bytes captured)
Ethernet II, Src: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b), Dst: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4)
Internet Protocol, Src: 10.0.0.4 (10.0.0.4), Dst: 91.121.126.69 (91.121.126.69)
Transmission Control Protocol, Src Port: 1362 (1362), Dst Port: ftp (21), Seq: 41, Ack: 386, Len: 5
File Transfer Protocol (FTP)

Frame 24 (88 bytes on wire, 88 bytes captured)
Ethernet II, Src: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4), Dst: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b)
Internet Protocol, Src: 91.121.126.69 (91.121.126.69), Dst: 10.0.0.4 (10.0.0.4)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 1362 (1362), Seq: 386, Ack: 46, Len: 34
File Transfer Protocol (FTP)

Frame 25 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b), Dst: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4)
Internet Protocol, Src: 10.0.0.4 (10.0.0.4), Dst: 91.121.126.69 (91.121.126.69)
Transmission Control Protocol, Src Port: 1362 (1362), Dst Port: ftp (21), Seq: 46, Ack: 420, Len: 8
File Transfer Protocol (FTP)

Frame 26 (73 bytes on wire, 73 bytes captured)
Ethernet II, Src: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4), Dst: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b)
Internet Protocol, Src: 91.121.126.69 (91.121.126.69), Dst: 10.0.0.4 (10.0.0.4)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 1362 (1362), Seq: 420, Ack: 54, Len: 19
File Transfer Protocol (FTP)

Frame 27 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b), Dst: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4)
Internet Protocol, Src: 10.0.0.4 (10.0.0.4), Dst: 91.121.126.69 (91.121.126.69)
Transmission Control Protocol, Src Port: 1362 (1362), Dst Port: ftp (21), Seq: 54, Ack: 439, Len: 6
File Transfer Protocol (FTP)

Frame 28 (105 bytes on wire, 105 bytes captured)
Ethernet II, Src: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4), Dst: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b)
Internet Protocol, Src: 91.121.126.69 (91.121.126.69), Dst: 10.0.0.4 (10.0.0.4)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 1362 (1362), Seq: 439, Ack: 60, Len: 51
File Transfer Protocol (FTP)

Frame 32 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b), Dst: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4)
Internet Protocol, Src: 10.0.0.4 (10.0.0.4), Dst: 91.121.126.69 (91.121.126.69)
Transmission Control Protocol, Src Port: 1362 (1362), Dst Port: ftp (21), Seq: 60, Ack: 490, Len: 6
File Transfer Protocol (FTP)

Frame 33 (108 bytes on wire, 108 bytes captured)
Ethernet II, Src: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4), Dst: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b)
Internet Protocol, Src: 91.121.126.69 (91.121.126.69), Dst: 10.0.0.4 (10.0.0.4)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 1362 (1362), Seq: 490, Ack: 66, Len: 54
File Transfer Protocol (FTP)

Frame 40 (77 bytes on wire, 77 bytes captured)
Ethernet II, Src: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4), Dst: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b)
Internet Protocol, Src: 91.121.126.69 (91.121.126.69), Dst: 10.0.0.4 (10.0.0.4)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 1362 (1362), Seq: 544, Ack: 66, Len: 23
File Transfer Protocol (FTP)
Przesyłanie pliku na serwer FTP

2. Aby można było zalogować się na serwer FTPi o adresie domenowym ftp.60free.ovh.org, AsustekC_b7:70:8b o adresie IP 10.0.0.4 potrzebuje adres IP tego serwera. Aby go uzyskać, za pomocą protokołu DNS, AsustekC_b7:70:8b wysyła do swojej bramy sieciowej o adresie IP 10.0.0.2 zapytanie o adres IP serwera, dla którego zarejestrowano domenę ftp.60free.ovh.org.
3. Brama domyślna po otrzymaniu zapytania od AsustekC_b7:70:8b przesyła je do jednego z dwóch serwerów DNS dostawcy usług internetowych (providera), których zadaniem jest dalsze przesyłanie zapytania do jednego z 13 głównych serwerów DNS, które są odpowiedzialne za domeny najwyższego poziomu (TLD – top level domains). Jeżeli wybrany przez nas adres jest rozpoznany za pomocą jednego z tych serwerów, zostanie on zamieniony na adres IP i powróci poprzez serwery providera do bramy sieciowej. W innym wypadku przeszukane zostaną serwery DNS niższego poziomu wskazane przez serwer główny. Gdy do bramy sieciowej powróci już odpowiedź w formie adresu IP serwera o adresie domenowym ftp.60free.ovh.org, zostanie ona przesłana do stacji AsustekC_b7:70:8b.
7. Za pomocą protokołu DNS AsustekC_b7:70:8b ustalił, że serwer o adresie domenowym ftp.60free.ovh.org posiada adres IP o numerze 91.121.126.69. Pierwszym krokiem, jaki wykonuje ten serwer za pomocą protokołu FTP, to przesłanie komunikatu powitalnego na adres IP 10.0.0.4 o treści „Welcome to the OVH free hosting FTP server. Please login...”
8. Po otrzymaniu komunikatu powitalnego AsustekC_b7:70:8b wysyła na adres IP 91.121.126.69 nazwę użytkownika.
10. Jeżeli nazwa użytkownika jest poprawna to serwer FTP wysyła na adres 10.0.0.4 żądanie hasła dla użytkownika.
11. W odpowiedzi na żądanie, AsustekC_b7:70:8b wysyła hasło użytkownika do serwera.
13. Serwer FTP wysyła do stacji o adresie IP 10.0.0.4 informacje na temat daty ostatniego logowania wskazując na to z jakiego Adresu IP zostało dokonane. Poza tymi informacjami podana jest liczba wszystkich zalogowań do Serwera FTP.
15. Z adresu IP o numerze 91.121.126.69 przychodzi wiadomość o tym, że użytkownik został zalogowany do serwera FTP.

[16…22] – Pomiędzy stacją AsustekC_b7:70:8b a serwerem FTP następuje wymiana żądań i odpowiedzi na te żądania. Dotyczą one systemu operacyjnego działającego na serwerze i cech sprzętu.

23. AsustekC_b7:70:8b przesyła do serwera FTP zapytanie PWD (ang. print working directory - wypisz katalog roboczy) – dzięki niemu program do obsługi protokołu FTP dowie się, jaki katalog powinien otworzyć.
24. Serwer FTP odpowiada na zapytanie PWD przesyłając adres katalogu roboczego do AsustekC_b7:70:8b.

[25 i 26] - AsustekC_b7:70:8b przesyła na adres IP 91.121.126.69 prośbę o ustawienie typu transferu plików ASCII na co serwer odpowiada odpowiednim komunikatem.

[27 i 28] - AsustekC_b7:70:8b prosi serwer FTP o przejście do trybu pasywnego. W odpowiedzi serwer zmienia tryb i wysyła odpowiedni komunikat.

32. AsustekC_b7:70:8b przesyła do serwera FTP żądanie, aby ten otworzył połączenie dla listy plików i folderów znajdujących się w katalogu roboczym.
33. Serwer FTP otwiera połączenie dla listy plików używając do tego zadeklarowanego wcześniej typu transferu plików ASCII.
40. Z adresu IP o numerze 91.121.126.69 nadchodzi komunikat o tym, że zakończono transfer.

Przesyłanie pliku na serwer

Logi przechwyconych pakietów

L.p.	Czas	Źródło	Przeznaczenie	Protokół	Informacje
1	0.000000	10.0.0.4	91.121.126.69	FTP	Request: CWD www
2	0.043551	91.121.126.69	10.0.0.4	FTP	Response: 250 CWD command successful
3	0.051735	10.0.0.4	91.121.126.69	FTP	Request: PWD
4	0.094817	91.121.126.69	10.0.0.4	FTP	Response: 257 /www is the current directory
5	0.154766	10.0.0.4	91.121.126.69	FTP	Request: PASV
6	0.198503	91.121.126.69	10.0.0.4	FTP	Response: 227 Entering Passive Mode (91,121,126,69,165,60).
10	0.251297	10.0.0.4	91.121.126.69	FTP	Request: LIST
11	0.294930	91.121.126.69	10.0.0.4	FTP	Response: 150 Opening ASCII mode data connection for file list
18	0.509251	91.121.126.69	10.0.0.4	FTP	Response: 226 Transfer complete
25	36.271951	10.0.0.4	91.121.126.69	FTP	Request: TYPE I
26	36.315982	91.121.126.69	10.0.0.4	FTP	Response: 200 Type set to I
27	36.322647	10.0.0.4	91.121.126.69	FTP	Request: PASV
28	36.366551	91.121.126.69	10.0.0.4	FTP	Response: 227 Entering Passive Mode (91,121,126,69,133,246).
32	36.419227	10.0.0.4	91.121.126.69	FTP	Request: STOR test.htm
34	36.548105	91.121.126.69	10.0.0.4	FTP	Response: 150 Opening BINARY mode data connection for test.htm
297	40.289435	91.121.126.69	10.0.0.4	FTP	Response: 226 Transfer complete
298	40.296359	10.0.0.4	91.121.126.69	FTP	Request: SIZE test.htm
300	40.340245	91.121.126.69	10.0.0.4	FTP	Response: 213 117640
302	40.549734	10.0.0.4	91.121.126.69	FTP	Request: TYPE A
303	40.592986	91.121.126.69	10.0.0.4	FTP	Response: 200 Type set to A
304	40.614740	10.0.0.4	91.121.126.69	FTP	Request: PASV
305	40.658530	91.121.126.69	10.0.0.4	FTP	Response: 227 Entering Passive Mode (91,121,126,69,166,50).
309	40.711884	10.0.0.4	91.121.126.69	FTP	Request: LIST
310	40.755161	91.121.126.69	10.0.0.4	FTP	Response: 150 Opening ASCII mode data connection for file list
317	40.944206	91.121.126.69	10.0.0.4	FTP	Response: 226 Transfer complete

Opis poszczególnych pozycji logu

Frame 1 (63 bytes on wire, 63 bytes captured)
Ethernet II, Src: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b), Dst: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4)
Internet Protocol, Src: 10.0.0.4 (10.0.0.4), Dst: 91.121.126.69 (91.121.126.69)
Transmission Control Protocol, Src Port: 1503 (1503), Dst Port: ftp (21), Seq: 0, Ack: 0, Len: 9
File Transfer Protocol (FTP)

Frame 2 (82 bytes on wire, 82 bytes captured)
Ethernet II, Src: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4), Dst: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b)
Internet Protocol, Src: 91.121.126.69 (91.121.126.69), Dst: 10.0.0.4 (10.0.0.4)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 1503 (1503), Seq: 0, Ack: 9, Len: 28
File Transfer Protocol (FTP)

Frame 3 (59 bytes on wire, 59 bytes captured)
Ethernet II, Src: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b), Dst: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4)
Internet Protocol, Src: 10.0.0.4 (10.0.0.4), Dst: 91.121.126.69 (91.121.126.69)
Transmission Control Protocol, Src Port: 1503 (1503), Dst Port: ftp (21), Seq: 9, Ack: 28, Len: 5
File Transfer Protocol (FTP)

Frame 4 (91 bytes on wire, 91 bytes captured)
Ethernet II, Src: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4), Dst: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b)
Internet Protocol, Src: 91.121.126.69 (91.121.126.69), Dst: 10.0.0.4 (10.0.0.4)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 1503 (1503), Seq: 28, Ack: 14, Len: 37
File Transfer Protocol (FTP)

Frame 5 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b), Dst: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4)
Internet Protocol, Src: 10.0.0.4 (10.0.0.4), Dst: 91.121.126.69 (91.121.126.69)
Transmission Control Protocol, Src Port: 1503 (1503), Dst Port: ftp (21), Seq: 14, Ack: 65, Len: 6
File Transfer Protocol (FTP)

Frame 6 (105 bytes on wire, 105 bytes captured)
Ethernet II, Src: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4), Dst: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b)
Internet Protocol, Src: 91.121.126.69 (91.121.126.69), Dst: 10.0.0.4 (10.0.0.4)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 1503 (1503), Seq: 65, Ack: 20, Len: 51
File Transfer Protocol (FTP)

Frame 10 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b), Dst: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4)
Internet Protocol, Src: 10.0.0.4 (10.0.0.4), Dst: 91.121.126.69 (91.121.126.69)
Transmission Control Protocol, Src Port: 1503 (1503), Dst Port: ftp (21), Seq: 20, Ack: 116, Len: 6
File Transfer Protocol (FTP)

Frame 11 (108 bytes on wire, 108 bytes captured)
Ethernet II, Src: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4), Dst: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b)
Internet Protocol, Src: 91.121.126.69 (91.121.126.69), Dst: 10.0.0.4 (10.0.0.4)

Transmission Control Protocol, Src Port: ftp (21), Dst Port: 1503 (1503), Seq: 116, Ack: 26, Len: 54
File Transfer Protocol (FTP)

Frame 18 (77 bytes on wire, 77 bytes captured)
Ethernet II, Src: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4), Dst: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b)
Internet Protocol, Src: 91.121.126.69 (91.121.126.69), Dst: 10.0.0.4 (10.0.0.4)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 1503 (1503), Seq: 170, Ack: 26, Len: 23
File Transfer Protocol (FTP)

Frame 25 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b), Dst: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4)
Internet Protocol, Src: 10.0.0.4 (10.0.0.4), Dst: 91.121.126.69 (91.121.126.69)
Transmission Control Protocol, Src Port: 1503 (1503), Dst Port: ftp (21), Seq: 26, Ack: 193, Len: 8
File Transfer Protocol (FTP)

Frame 26 (73 bytes on wire, 73 bytes captured)
Ethernet II, Src: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4), Dst: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b)
Internet Protocol, Src: 91.121.126.69 (91.121.126.69), Dst: 10.0.0.4 (10.0.0.4)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 1503 (1503), Seq: 193, Ack: 34, Len: 19
File Transfer Protocol (FTP)

Frame 27 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b), Dst: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4)
Internet Protocol, Src: 10.0.0.4 (10.0.0.4), Dst: 91.121.126.69 (91.121.126.69)
Transmission Control Protocol, Src Port: 1503 (1503), Dst Port: ftp (21), Seq: 34, Ack: 212, Len: 6
File Transfer Protocol (FTP)

Frame 28 (106 bytes on wire, 106 bytes captured)
Ethernet II, Src: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4), Dst: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b)
Internet Protocol, Src: 91.121.126.69 (91.121.126.69), Dst: 10.0.0.4 (10.0.0.4)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 1503 (1503), Seq: 212, Ack: 40, Len: 52
File Transfer Protocol (FTP)

Frame 32 (69 bytes on wire, 69 bytes captured)
Ethernet II, Src: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b), Dst: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4)
Internet Protocol, Src: 10.0.0.4 (10.0.0.4), Dst: 91.121.126.69 (91.121.126.69)
Transmission Control Protocol, Src Port: 1503 (1503), Dst Port: ftp (21), Seq: 40, Ack: 264, Len: 15
File Transfer Protocol (FTP)

Frame 34 (108 bytes on wire, 108 bytes captured)
Ethernet II, Src: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4), Dst: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b)
Internet Protocol, Src: 91.121.126.69 (91.121.126.69), Dst: 10.0.0.4 (10.0.0.4)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 1503 (1503), Seq: 264, Ack: 55, Len: 54
File Transfer Protocol (FTP)

Frame 297 (77 bytes on wire, 77 bytes captured)
Ethernet II, Src: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4), Dst: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b)
Internet Protocol, Src: 91.121.126.69 (91.121.126.69), Dst: 10.0.0.4 (10.0.0.4)

Transmission Control Protocol, Src Port: ftp (21), Dst Port: 1503 (1503), Seq: 318, Ack: 55, Len: 23
File Transfer Protocol (FTP)

Frame 298 (69 bytes on wire, 69 bytes captured)
Ethernet II, Src: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b), Dst: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4)
Internet Protocol, Src: 10.0.0.4 (10.0.0.4), Dst: 91.121.126.69 (91.121.126.69)
Transmission Control Protocol, Src Port: 1503 (1503), Dst Port: ftp (21), Seq: 55, Ack: 341, Len: 15
File Transfer Protocol (FTP)

Frame 300 (66 bytes on wire, 66 bytes captured)
Ethernet II, Src: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4), Dst: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b)
Internet Protocol, Src: 91.121.126.69 (91.121.126.69), Dst: 10.0.0.4 (10.0.0.4)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 1503 (1503), Seq: 341, Ack: 70, Len: 12
File Transfer Protocol (FTP)

Frame 302 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b), Dst: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4)
Internet Protocol, Src: 10.0.0.4 (10.0.0.4), Dst: 91.121.126.69 (91.121.126.69)
Transmission Control Protocol, Src Port: 1503 (1503), Dst Port: ftp (21), Seq: 70, Ack: 353, Len: 8
File Transfer Protocol (FTP)

Frame 303 (73 bytes on wire, 73 bytes captured)
Ethernet II, Src: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4), Dst: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b)
Internet Protocol, Src: 91.121.126.69 (91.121.126.69), Dst: 10.0.0.4 (10.0.0.4)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 1503 (1503), Seq: 353, Ack: 78, Len: 19
File Transfer Protocol (FTP)

Frame 304 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b), Dst: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4)
Internet Protocol, Src: 10.0.0.4 (10.0.0.4), Dst: 91.121.126.69 (91.121.126.69)
Transmission Control Protocol, Src Port: 1503 (1503), Dst Port: ftp (21), Seq: 78, Ack: 372, Len: 6
File Transfer Protocol (FTP)

Frame 305 (105 bytes on wire, 105 bytes captured)
Ethernet II, Src: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4), Dst: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b)
Internet Protocol, Src: 91.121.126.69 (91.121.126.69), Dst: 10.0.0.4 (10.0.0.4)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 1503 (1503), Seq: 372, Ack: 84, Len: 51
File Transfer Protocol (FTP)

Frame 309 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b), Dst: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4)
Internet Protocol, Src: 10.0.0.4 (10.0.0.4), Dst: 91.121.126.69 (91.121.126.69)
Transmission Control Protocol, Src Port: 1503 (1503), Dst Port: ftp (21), Seq: 84, Ack: 423, Len: 6
File Transfer Protocol (FTP)

Frame 310 (108 bytes on wire, 108 bytes captured)
Ethernet II, Src: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4), Dst: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b)
Internet Protocol, Src: 91.121.126.69 (91.121.126.69), Dst: 10.0.0.4 (10.0.0.4)

Transmission Control Protocol, Src Port: ftp (21), Dst Port: 1503 (1503), Seq: 423, Ack: 90, Len: 54
File Transfer Protocol (FTP)

Frame 317 (77 bytes on wire, 77 bytes captured)
Ethernet II, Src: Pro-Nets_54:40:d4 (XX:XX:XX:54:40:d4), Dst: AsustekC_b7:70:8b (XX:XX:XX:b7:70:8b)
Internet Protocol, Src: 91.121.126.69 (91.121.126.69), Dst: 10.0.0.4 (10.0.0.4)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 1503 (1503), Seq: 477, Ack: 90, Len: 23
File Transfer Protocol (FTP)

1. AsustekC_b7:70:8b przesyła do serwera FTP żądanie CWD (ang. change working directory - zmień katalog roboczy), aby zmienić katalog na „WWW".
2. Serwer przesyła na adres IP 10.0.0.4 odpowiedź, że zmiana katalogu zakończyła się sukcesem.
3. AsustekC_b7:70:8b przesyła do serwera FTP zapytanie PWD (ang. print working directory - wypisz katalog roboczy) – dzięki niemu program do obsługi protokołu FTP zapisze pliki w zmienionym katalogu.
4. Serwer FTP odpowiada na zapytanie PWD przesyłając adres zmienionego katalogu roboczego do AsustekC_b7:70:8b.

[5 i 6] - AsustekC_b7:70:8b prosi serwer FTP o przejście do trybu pasywnego. W odpowiedzi serwer zmienia tryb i wysyła odpowiedni komunikat.

10. AsustekC_b7:70:8b przesyła do serwera FTP żądanie, aby ten otworzył połączenie dla listy plików i folderów znajdujących się w katalogu roboczym.
11. Serwer FTP otwiera połączenie dla listy plików używając do tego transferu plików typu ASCII, który zadeklarowano przy logowaniu.
18. Z adresu IP o numerze 91.121.126.69 nadchodzi komunikat o tym, że zakończono transfer.

[25 i 26] - AsustekC_b7:70:8b przesyła na adres IP 91.121.126.69 prośbę o ustawienie typu transferu plików images (dane binarne) na co serwer odpowiada odpowiednim komunikatem.

[27 i 28] - AsustekC_b7:70:8b prosi serwer FTP o przejście do trybu pasywnego. W odpowiedzi serwer zmienia tryb i wysyła odpowiedni komunikat.

32. Stacja o adresie IP 10.0.0.4 wysyła do serwera FTP żądanie STOR, które oznacza, że AsustekC_b7:70:8b chce zapisać plik na serwerze.
34. Serwer FTP otwiera połączenie dla pliku używając do tego zadeklarowanego wcześniej typu transferu plików images (dane binarne).

[następuje przesłanie pliku]

297. Z adresu IP o numerze 91.121.126.69 nadchodzi komunikat o tym, że zakończono transfer.

[298 i 300] - AsustekC_b7:70:8b wysyła do serwera FTP zapytanie SIZE, aby uzyskać wiadomość o wielkości przesłanego pliku. Serwer odpowiada wysyłając na adres 10.0.0.4 dane o wielkości pliku.

[302 i 303] - AsustekC_b7:70:8b przesyła na adres IP 91.121.126.69 prośbę o ustawienie typu transferu plików ASCII na co serwer odpowiada odpowiednim komunikatem.

[304 i 305] - AsustekC_b7:70:8b prosi serwer FTP o przejście do trybu pasywnego. W odpowiedzi serwer zmienia tryb i wysyła odpowiedni komunikat.

309. AsustekC_b7:70:8b przesyła do serwera FTP żądanie, aby ten otworzył połączenie dla listy plików i folderów znajdujących się w katalogu roboczym.
310. Serwer FTP otwiera połączenie dla listy plików używając do tego zadeklarowanego wcześniej typu transferu plików ASCII.
317. Z adresu IP o numerze 91.121.126.69 nadchodzi komunikat o tym, że zakończono transfer.

Wnioski

Jak łatwo można zauważyć analizując logi z programu Wireshark, komputer komunikując się w ramach sieci z innymi komputerami, wysyła do nich bardzo wiele pojedynczych zapytań (pakietów), a każde kolejne zapytanie zwykle musi być poprzedzone odpowiedzią ze stacji do której ma być wysłane. Zapytania te są opisane za pomocą protokołów komunikacyjnych, które odpowiadają za różne funkcje w obrębie sieci.

Niewielki rozmiar pakietów pozwala na wykonywanie bardzo wielu operacji w krótkim czasie i pozwala na obsługę kilku stacji roboczych przez jedno urządzenie na raz.

Przy analizie protokołu FTP można zauważyć, iż jeżeli dane takie jak nazwa użytkownika i hasło nie są odpowiednio zaszyfrowane, to można je bardzo łatwo przechwycić korzystając chociażby z analizatora sieciowego Wireshark