

1110111011011

1001100

110011001100

10101010101010

00011001001

Ekspert Wiresharka

Analiza ruchu sieciowego

Hacking i Cyberbezpieczeństwo | Giganci Programowania

Opracowanie: Michał Suchoń

Przypomnienie

1. Do czego służy Keylogger?
2. Jak się nazywa system operacyjny (distro Linuxa), posiadający narzędzia do hackingu?
3. Co to SSH?
4. Do czego służy DeepWeb?
5. Czym jest Phishing?

Przypomnienie

1. Do czego służy Keylogger?
oprogramowanie bądź urządzenie (także jako wirus), służące do rejestrowania klawiszy bądź kliknięć myszki, np. celem kradzieży danych bądź badania zachowań użytkowników
2. Jak się nazywa system operacyjny (distro Linuxa), posiadający narzędzia do hackingu?
3. Co to SSH?
4. Do czego służy DeepWeb?
5. Czym jest Phishing?

Przypomnienie

1. Do czego służy Keylogger?
oprogramowanie bądź urządzenie (także jako wirus), służące do rejestrowania klawiszy bądź kliknięć myszki, np. celem kradzieży danych bądź badania zachowań użytkowników
2. Jak się nazywa system operacyjny (distro Linuxa), posiadający narzędzia do hackingu?
Kali Linux
3. Co to SSH?
4. Do czego służy DeepWeb?
5. Czym jest Phishing?

Przypomnienie

1. Do czego służy Keylogger?
oprogramowanie bądź urządzenie (także jako wirus), służące do rejestrowania klawiszy bądź kliknięć myszki, np. celem kradzieży danych bądź badania zachowań użytkowników
2. Jak się nazywa system operacyjny (distro Linuxa), posiadający narzędzia do hackingu?
Kali Linux
3. Co to SSH?
ang. Secure Shell; protokół komunikacyjny, umożliwiający zdalne połączenie z innym komputerem (serwerem) z możliwością wydawania poleceń i konfigurowania. Protokół SSH (w odróżnieniu od przodka – Telnetu) jest zabezpieczony szyfrowanym połączeniem dwustronnym
4. Do czego służy DeepWeb?
5. Czym jest Phishing?

Przypomnienie

1. Do czego służy Keylogger?
oprogramowanie bądź urządzenie (także jako wirus), służące do rejestrowania klawiszy bądź kliknięć myszki, np. celem kradzieży danych bądź badania zachowań użytkowników
2. Jak się nazywa system operacyjny (distro Linuxa), posiadający narzędzia do hackingu?
Kali Linux
3. Co to SSH?
ang. Secure Shell; protokół komunikacyjny, umożliwiający zdalne połączenie z innym komputerem (serwerem) z możliwością wydawania poleceń i konfigurowania. Protokół SSH (w odróżnieniu od przodka – Telnetu) jest zabezpieczony szyfrowanym połączeniem dwustronnym
4. Do czego służy DeepWeb?
rodzaj sieci, która jest niedostępna poprzez klasyczną przeglądarkę, a wymaga podłączenia do sieci Tor, np. przez Tor Browser
5. Czym jest Phishing?

Przypomnienie

1. Do czego służy Keylogger?
oprogramowanie bądź urządzenie (także jako wirus), służące do rejestrowania klawiszy bądź kliknięć myszki, np. celem kradzieży danych bądź badania zachowań użytkowników
2. Jak się nazywa system operacyjny (distro Linuxa), posiadający narzędzia do hackingu?
Kali Linux
3. Co to SSH?
ang. Secure Shell; protokół komunikacyjny, umożliwiający zdalne połączenie z innym komputerem (serwerem) z możliwością wydawania poleceń i konfigurowania. Protokół SSH (w odróżnieniu od przodka – Telnetu) jest zabezpieczony szyfrowanym połączeniem dwustronnym
4. Do czego służy DeepWeb?
rodzaj sieci, która jest niedostępna poprzez klasyczną przeglądarkę, a wymaga podłączenia do sieci Tor, np. przez Tor Browser
5. Czym jest Phishing?
rodzaj ataku, w którym wykorzystuje się elementy socjotechniki po to, aby uzyskać poufne dane

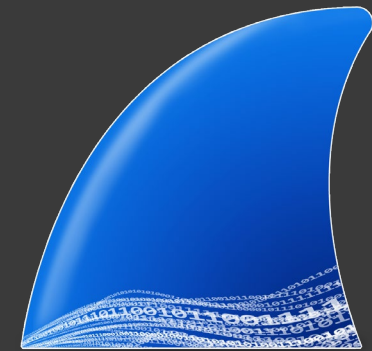
*Do czego używa się
Wiresharka?*



Wireshark

wire – drut / przewód; shark – rekin

program przeznaczony do analizowania ruchu sieciowego

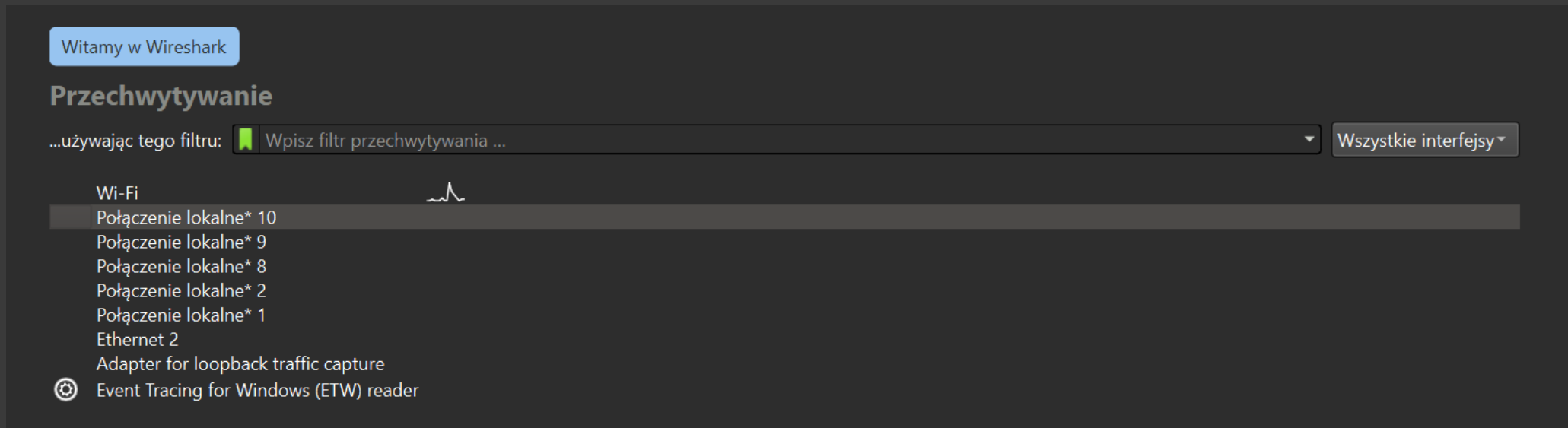


*Co można zrobić za
pomocą Wiresharka?*

- Wireshark analizuje i wyświetla ruch sieciowy w czasie rzeczywistym.
- Pozwala na zapis i odczyt zebranego ruchu sieciowego tak, aby można było zabezpieczyć dane.
- Jest dostępny na wszystkie platformy (Windows, Linux, MacOS)
- Ma dużo wbudowanych funkcji np. do wydobywania plików z ruchu sieciowego czy przeglądania pakietów pojedynczych w prosty sposób.
- Pozwala na deszyfrowanie ruchu sieciowego.
- pierwotnie był tylko do analizy ruchu sieciowego przewodowego, jednak nie strasze mu są sieci wifi.
- Pozwala na dodawanie pluginów oficjalnych i mniej oficjalnych, które łamią prawo), dzięki czemu potrafi wspierać bluetooth, sieci LoraWan, GSM – Wymaga to dodatkowych modułów.
- Jest rozwijany na licencji open source

Interfejs Wiresharka

Ekran startowy - interfejsy



Umożliwia prześledzenie ruchu sieciowego na interfejsach (kartach sieciowych), dostępnych w komputerze oraz ewentualnych maszynach wirtualnych

Ruch sieciowy na interfejsie

Przechwytywanie z Wi-Fi

Plik Edycja Widok Przejdź Przechwytywanie Analiza Statystyki Telefonia Bezprzewodowe Narzędzia Pomoc

Zastosuj filtr wyświetlania ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1900	118.707710	52.123.129.14	192.168.1.167	TCP	1514	443 → 51013 [ACK] Seq=12606 Ack=2024 Win=4194304 Len=1460 [TCP PDU reassembled in 1904]
1901	118.707710	52.123.129.14	192.168.1.167	TCP	1514	443 → 51013 [ACK] Seq=14066 Ack=2024 Win=4194304 Len=1460 [TCP PDU reassembled in 1904]
1902	118.707710	52.123.129.14	192.168.1.167	TCP	1514	443 → 51013 [ACK] Seq=15526 Ack=2024 Win=4194304 Len=1460 [TCP PDU reassembled in 1904]
1903	118.707710	52.123.129.14	192.168.1.167	TCP	1514	443 → 51013 [ACK] Seq=16986 Ack=2024 Win=4194304 Len=1460 [TCP PDU reassembled in 1904]
1904	118.707710	52.123.129.14	192.168.1.167	TLSv1.2	975	Application Data
1905	118.707710	52.123.129.14	192.168.1.167	TCP	1514	443 → 51013 [ACK] Seq=19367 Ack=2024 Win=4194304 Len=1460 [TCP PDU reassembled in 1907]
1906	118.707710	52.123.129.14	192.168.1.167	TCP	1514	443 → 51013 [ACK] Seq=20827 Ack=2024 Win=4194304 Len=1460 [TCP PDU reassembled in 1907]
1907	118.707710	52.123.129.14	192.168.1.167	TLSv1.2	685	Application Data
1908	118.707710	52.123.129.14	192.168.1.167	TCP	1514	443 → 51013 [ACK] Seq=22918 Ack=2024 Win=4194304 Len=1460 [TCP PDU reassembled in 1913]
1909	118.707710	52.123.129.14	192.168.1.167	TCP	1514	443 → 51013 [ACK] Seq=24378 Ack=2024 Win=4194304 Len=1460 [TCP PDU reassembled in 1913]
1910	118.707710	52.123.129.14	192.168.1.167	TCP	1514	443 → 51013 [ACK] Seq=25838 Ack=2024 Win=4194304 Len=1460 [TCP PDU reassembled in 1913]
1911	118.707710	52.123.129.14	192.168.1.167	TCP	1514	443 → 51013 [ACK] Seq=27298 Ack=2024 Win=4194304 Len=1460 [TCP PDU reassembled in 1913]
1912	118.707710	52.123.129.14	192.168.1.167	TCP	1514	443 → 51013 [ACK] Seq=28758 Ack=2024 Win=4194304 Len=1460 [TCP PDU reassembled in 1913]
1913	118.707710	52.123.129.14	192.168.1.167	TLSv1.2	975	Application Data
1914	118.707710	52.123.129.14	192.168.1.167	TCP	1514	443 → 51013 [ACK] Seq=31139 Ack=2024 Win=4194304 Len=1460 [TCP PDU reassembled in 1921]
1915	118.707710	52.123.129.14	192.168.1.167	TCP	1514	443 → 51013 [ACK] Seq=32599 Ack=2024 Win=4194304 Len=1460 [TCP PDU reassembled in 1921]
1916	118.707710	52.123.129.14	192.168.1.167	TCP	1514	443 → 51013 [ACK] Seq=34059 Ack=2024 Win=4194304 Len=1460 [TCP PDU reassembled in 1921]
1917	118.707992	192.168.1.167	52.123.129.14	TCP	54	51013 → 443 [ACK] Seq=2024 Ack=35519 Win=65280 Len=0

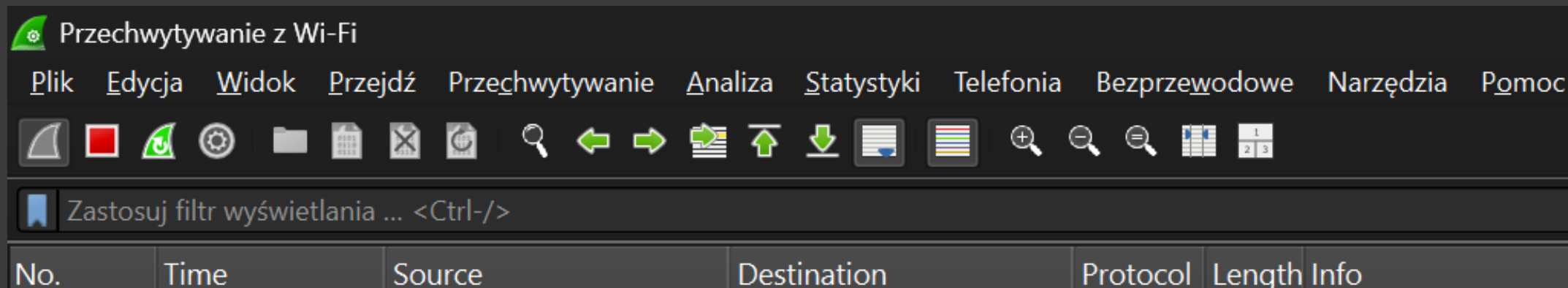
Frame 1913: 975 bytes on wire (7800 bits), 975 bytes captured (7800 bits) on interface
Ethernet II, Src: Commscope_1d:82:09 (e8:82:5b:1d:82:09), Dst: LiteonTechno_47:53:59 (08:00:27:47:53:59)
Internet Protocol Version 4, Src: 52.123.129.14, Dst: 192.168.1.167
Transmission Control Protocol, Src Port: 443, Dst Port: 51013, Seq: 30218, Ack: 2024, Len: 975
[6 Reassembled TCP Segments (8221 bytes): #1908(1460), #1909(1460), #1910(1460), #1911(1460), #1912(1460), #1913(975)]
Transport Layer Security

0000 c0 35 32 47 53 59 e8 82 5b 1d 82 09 08 00 00 00 52GSY... [.....E
0010 03 c1 cf 5b 40 00 76 06 ba 02 34 7b 81 0e c0 a8 ...[@.v...4{...
0020 01 a7 01 bb c7 45 77 90 c1 0e 0f 60 71 d7 50 18Ew...q.P.
0030 40 00 eb b6 00 00 33 b8 fc 9b 59 99 7c d2 39 43 @.....3...Y...9C
0040 c6 d4 33 84 45 39 05 38 89 b2 b2 85 d4 98 a6 c5 ..3.E9.8
0050 db 3d 7b bf 2c 05 79 a1 12 7d 60 c3 ba 85 a0 96 .={.,y.}.....
0060 78 26 91 b3 e1 e9 71 89 4c 91 57 24 0e 02 a3 b2 x&.....q.L.W\$.
0070 61 79 71 50 6b ba 16 b8 9b 7c c6 68 1b 95 e2 ad ayqPk...|h....
0080 4b eb e1 dd 88 06 04 ef 92 81 1e 39 23 51 4b 23 K.....9#QK#
0090 59 6a 8a c3 0f 0d 4d 4b 66 1e 1a 9c 93 e5 dc f7 Yj....MK f.....
00a0 13 ca 07 f1 a1 df 58 7f b3 39 7a e9 2c 34 5d f7X..9z.,4].
00b0 6b 37 9d 2b d4 38 4b e1 19 df 61 b5 e0 e3 cb aa k7+.8K...a.....
00c0 53 01 e9 99 63 79 1d 54 35 42 63 50 28 f4 c0 b8 S...cy.T 5BcP(...
00d0 82 92 5b e4 13 7b f0 ea d3 53 cb e1 82 45 7c 0d ..[...{...S...E|.
00e0 74 4a a8 75 da 86 da d6 77 4f 39 1f 86 7a 57 3d tJ.u....w09...zW=
00f0 b1 83 8c 42 bb f9 ca 01 50 9d 2e 3e c4 cd e5 9c ...B....P.,>....
0100 d1 49 7f 6d 6f 97 22 ab de f6 f5 b7 da a3 9d 55 .I.mo"...U
0110 e8 f6 a6 76 6f 72 5a 2c 23 1b 61 0e af 49 9e d7 ...vorZ, #.a..I..

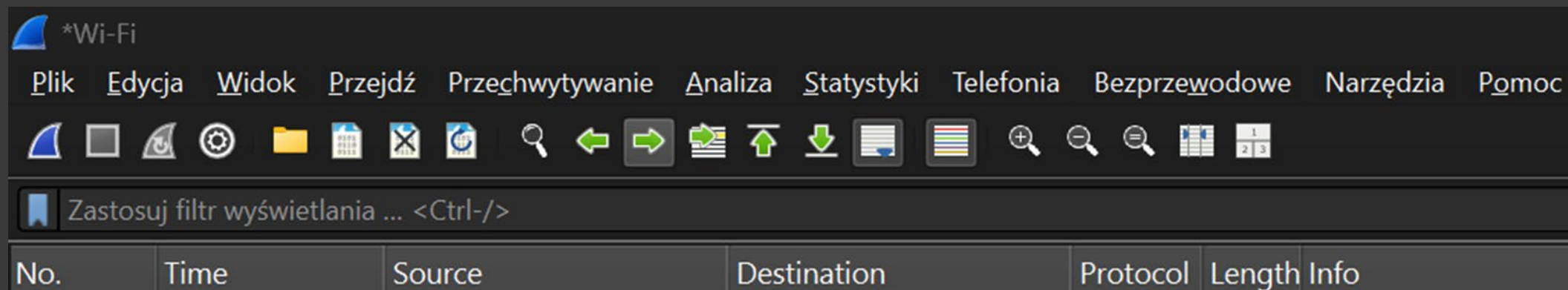
Frame (975 bytes) Reassembled TCP (8221 bytes)

Wi-Fi: <live capture in progress> Pakiety: 2301 Profil: Default

Statusy nasłuchiwania (on/off)

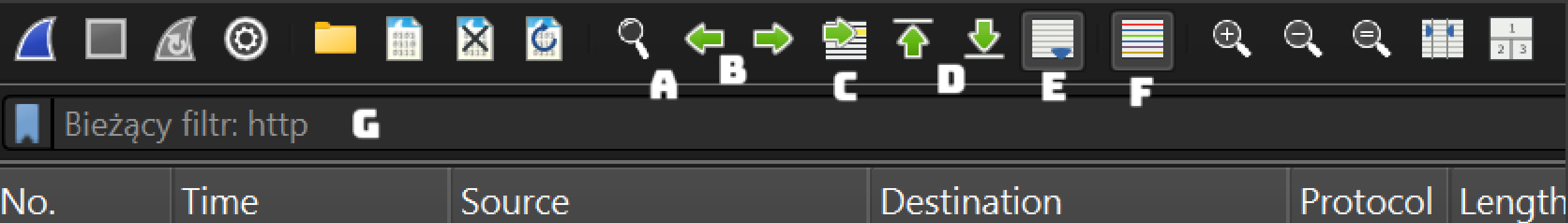


AKTYWNE NASŁUCHIWANIE (CZERWONY KWADRAT „STOP” PODŚWIETLONY)



**WYŁĄCZONE NASŁUCHIWANIE
(CZERWONY KWADRAT „STOP” SZARY, START – NIEBIESKA PŁETWA)**

Narzędzia filtrowania



- **A** – wyszukiwanie konkretnego rodzaju pakietów
- **B** – przełączanie następny/poprzedni pakiet
- **C** – przejście do wybranego pakietu
- **D** – przejście do pierwszego/ostatniego pakietu
- **E** – automatyczne przewijanie, gdy nasłuchiwanie jest aktywne
- **F** – przełączanie formatowania pakietów (kolorowanie wybranych danego rodzaju)
- **G** – tożsame z A

*HTTP filtruje pakiety
nieszyfrowane. W jaki
sposób więc można wyszukać
szyfrowane pakiety HTTPS?
(wyszukiwanie https nie działa!)*

*HTTP filtruje pakiety
nieszyfrowane. W jaki
sposób więc można wyszukać
szyfrowane pakiety HTTPS?*

*Podpowiedź: protokół, dzięki któremu
połączenia są szyfrowane (certyfikaty)*

*HTTP filtruje pakiety
nieszyfrowane. W jaki
sposób więc można wyszukać
szyfrowane pakiety HTTPS?*

ROZWIĄZANIE:

Należy zastosować protokół SSL
(lub następca: TLS)

ĆWICZENIE 1 | Przejmowanie danych przez FTP

1. Uruchamiamy Filezillę i logujemy się do serwera FTP:

adres serwera: **ftp.cytr.us**

login: **gigant1 ... (do) gigant15**

hasło: **Q=%k#ababmqOLtv**

2. Przechodzimy do Wiresharka, resetujemy nasłuchiwanie i wyszukujemy pakiety, filtrując po **ftp**.
3. Szukamy informacji na temat hasła w szczegółach o pakiecie

Przechwytywanie z Wi-Fi

Plik Edycja Widok Przejdź Przechwytywanie Analiza Statystyki Telefonía Bezprzewodowe Narzędzia Pomoc



ftp

No.	Time	Source	Destination	Protocol	Length	Info
33	4.828060	192.168.1.167	135.181.95.85	FTP	62	Request: TYPE I
36	4.905659	135.181.95.85	192.168.1.167	FTP	73	Response: 200 Type set to I
130	17.193344	135.181.95.85	192.168.1.167	FTP	107	Response: 220 ProFTPD Server (CYTR.US) [::ffff:135.181.95.85]
131	17.194253	192.168.1.167	135.181.95.85	FTP	68	Request: USER gigant1
133	17.295827	135.181.95.85	192.168.1.167	FTP	89	Response: 331 Password required for gigant1
182	26.800522	192.168.1.167	135.181.95.85	FTP	76	Request: PASS Q=%k#ababmqOLtv
187	28.767968	135.181.95.85	192.168.1.167	FTP	82	Response: 230 User gigant1 logged in
188	28.768492	192.168.1.167	135.181.95.85	FTP	60	Request: SYST
190	28.868572	135.181.95.85	192.168.1.167	FTP	73	Response: 215 UNIX Type: L8
191	28.869178	192.168.1.167	135.181.95.85	FTP	60	Request: FEAT
193	28.970827	135.181.95.85	192.168.1.167	FTP	69	Response: 211-Features:
194	28.970961	135.181.95.85	192.168.1.167	FTP	74	Response: 211-CLNT
195	28.970961	135.181.95.85	192.168.1.167	FTP	337	Response: 211-EPSV
196	28.970961	135.181.95.85	192.168.1.167	FTP	108	Response: 211-SITE SYMLINK
197	28.970961	135.181.95.85	192.168.1.167	FTP	73	Response: 211-UTF8
199	28.971895	192.168.1.167	135.181.95.85	FTP	81	Request: CLNT WinSCP-release-6.5.3
200	29.073275	135.181.95.85	192.168.1.167	FTP	62	Response: 200 OK

ĆWICZENIE 2 | Pliki *.pcap

Spróbuj przechwycić dowolne pakiety ze swojej karty sieciowej (możesz np. wejść na jakąś stronę i spróbować się zalogować bądź wrzucić plik, np. na chmurze Dysk Google lub podobnej). Następnie, przefiltruj po wybranym protokole, np. http/ssl lub ftp / ssh (w zależności od tego, jakiego rodzaju połączenia nawiązujesz).

Rezultaty zapisz do pliku: File/Plik -> Export Specified Packets/Zapisz wybrane pakiety

1. *Jakie protokoły zostały użyte podczas komunikacji?*
2. *Z jakich adresów komunikacja się odbywała?*
3. *Co to jest za adres 127.0.0.1?*
4. *Jeżeli podczas komunikacji http była próba przestania plików, w jaki sposób możemy je odszukać i wyciągnąć?*

ĆWICZENIE 3 | Przesyłanie pliku i wyciąganie go z komunikacji FTP

Ponownie łączymy się z serwerem FTP za pomocą danych z ćwiczenia 1. Przesyłamy plik, np. obrazek przy uruchomionym nasłuchiwanie w Wireshark'u. **Filtrujemy po FTP.**

Jakie są rezultaty? Czy udało się odnaleźć przesyłany plik?

ĆWICZENIE 3 | Przesyłanie pliku i wyciąganie go z komunikacji FTP

Ponownie łączymy się z serwerem FTP za pomocą danych z ćwiczenia 1. Przesyłamy plik, np. obrazek przy uruchomionym nasłuchiwanie w Wireshark'u. **Filtrujemy po FTP.**

Jakie są rezultaty? Czy udało się odnaleźć przesyłany plik?

Podpowiedź: **Musimy połączyć dwa różne filtry: ftp oraz ftp-data. W celu zastosowania wspólnego filtra dla dwóch rodzajów, musimy zastosować operację logiczną (AND / OR).**

Którą z nich zastosujemy i dlaczego? Jak to zapisać, jeśli jest to analogiczne do języków programowania?

ĆWICZENIE 3 | Przesyłanie pliku i wyciąganie go z komunikacji FTP

Ponownie łączymy się z serwerem FTP za pomocą danych z ćwiczenia 1. Przesyłamy plik, np. obrazek przy uruchomionym nasłuchiwanie w Wireshark'u. **Filtrujemy po FTP.**

Jakie są rezultaty? Czy udało się odnaleźć przesyłany plik?

Rozwiązanie: **Stosujemy operację LUB (OR) – AND spowodowałby, że oczekiwaliśmy dwóch osobnych rodzajów pakietów jednocześnie!**

Zapisujemy więc:

ftp || ftp-data

Na koniec, eksportujemy:

Plik > Eksportuj obiekty > FTP-DATA

Wybieramy plik i zapisujemy na naszym komputerze.

Podsumowanie

1. Jakiego znaku trzeba użyć w filtrze wiresharka aby 2 różne filtry zastosować?
2. Co się nam wyświetli jeżeli użyjemy filtra ftp-data?
3. Co to jest plik o rozszerzeniu PCAP?



ZADANIE EXTRA | Własna analiza

Sprawdź swoje ulubione strony internetowe, jak wygląda ruch sieciowy i czy da się coś z nich wyciągnąć stosując filtr **ip.addr = ip strony ulubionej**

- Zobacz jak wygląda ruch sieciowy podczas grania w grę sieciową.
- Połącz się z kimś przez komunikator głosowy i zobacz jak wygląda takie połączenie.
- Spróbuj tak ustawić wireshark aby przechwytywał ruch sieciowy tylko z maszyny wirtualnej np z kali linuxa, bez ruchu sieciowego z windowsa.

Polecam!



ŹRÓDŁO:

<https://www.youtube.com/watch?v=5qecyZHL-GU>

Polecam!



ŹRÓDŁO:

<https://www.youtube.com/watch?v=C4Gtq5anlyc>