

NARZĘDZIA DIAGNOSTYCZNE – badanie ruchu sieciowego za pomocą programu Wireshark

PRZYPOMNIENIE !

Wireshark to program typu „open source” używany do analizy pakietów dostępny na różnych platformach. Narzędzie tego typu potocznie nazywane jest snifferem. Dzięki dużej ilości dodatków potrafi rozpoznać i zdekodować wiele protokołów komunikacyjnych. Wireshark nie jest wyposażony w funkcjonalność MITM (man in the middle) analizowany ruch wymaga przechwycenia za pomocą innych programów np. Ettercap, Cain and Abel czy *arp spoof*.

I a. INSTALACJA WIRESHARK



1. Należy pobrać najnowszą wersję programu ze strony www.wireshark.org
2. Standardowa instalacja, po której narzędzie jest gotowe do pracy.

I b. INSTALACJA WIRESHARK

(w przypadku dystrybucji typu Kali program jest preinstalowany)



1. Należy wejść terminal zaktualizować pakiety komendami:
 - `sudo apt-get update`
 - `sudo apt-get upgrade`
2. Następnie należy zainstalować program komendą:
`sudo apt-get install wireshark`
3. Zgodnie z preferencjami wybierać opcje instalacji. Po zakończeniu aplikacja może być uruchomiona przez komendę `wireshark` bądź odnaleziona na liście programów.
4. Do prawidłowego funkcjonowania aplikacji niezbędne jest przydzielenie uprawnień (w przeciwnym wypadku nie odnajdziemy prawidłowego interfejsu).
5. W przypadku problemów (wprowadzeniu złych parametrów) należy wpisać `sudo dpkg-reconfigure wireshark-common` wybrać prawą opcję.
6. W przypadku potrzeby używania programu „bez roota” należy zmodyfikować uprawnienia pliku komendą `sudo chmod +x /usr/bin/dumpcap`

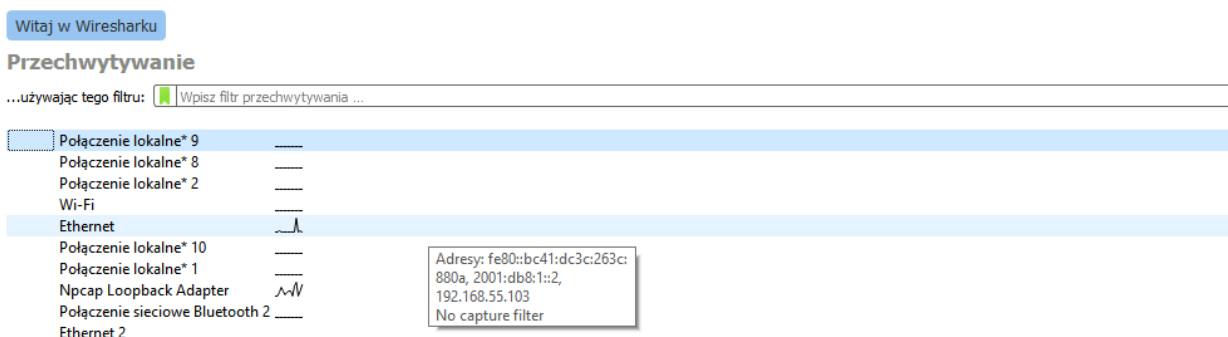
7. Program jest gotowy do pracy.

II. ZAPOZNANIE Z INTERFEJSEM

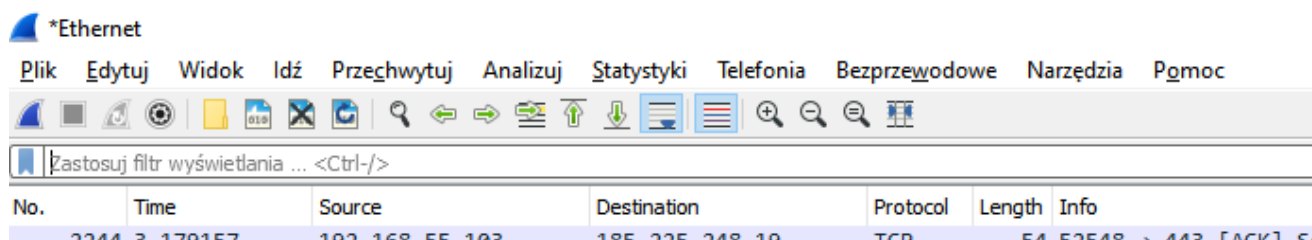
(na przykładzie W10)



Po włączeniu aplikacji ukaże nam się okno wyboru interfejsu z którego będziemy korzystać podczas wyłapywania pakietów.



Specjalnie zaznaczono interfejs Ethernet – daje możliwość zweryfikowania (sprawdzając własny adres IP) czy podłączając się pod ten kanał będziemy analizować pożądaną sieć.



Powyżej widać pasek narzędzi oraz filtr który jest podstawowym narzędziem pracy podczas przeszukiwania informacji przechwyconych z sieci. Wyróżniamy dwa filtry:

- **przechwytywania** – używany do wyboru CO ma być zapisywane w logach
- **wyświetlania** – używany do wyszukiwania informacji wewnątrz przechwyconych danych

WAŻNE!

Definicje filtrów

www.wireshark.org/CaptureFilters

ZADANIA

I ANALIZA PODSTAWOWYCH PROTOKOŁÓW

1. Na podstawie komendy **ping**, przeanalizuj przechwycone dane – protokoły **ICMP, ARP, DNS**.
2. Podczas odczytywania znajdź adres fizyczny urządzenia sieciowego z którego korzystasz oraz nazwę urządzenia które obsługuje połączenie po stronie serwera na dowolnie wybranym przykładzie.
3. Poprzez przeglądarkę internetową przeanalizuj różnice między protokołami **HTTP / HTTPS**.
Znajdź niezabezpieczoną stronę z panelem logowania – przechwyc fikcyjne dane logowania. Dla porównania wykonaj tę samą czynność na zabezpieczonej stronie.
4. Poprzez dowolnego klienta przeanalizuj różnice między protokołami **FTP / FTPS**.
Identycznie jak wyżej.
5. Odnajdź usługi która korzysta z protokołu **UDP**, ukaż przynajmniej 3 różne źródła.

II PRACA W PARZE

1. Wymieńcie się adresami IP.
2. Podczas nasłuchiwania wykonajcie komendę **ping** sprawdźcie czy poprawnie odnaleźliście swoje adresy fizyczne (MAC).
3. Znajdź Panel Sterowania → System i zabezpieczenia → Zapora Windows Defender → Ustawienia zaawansowane.
4. Dodaj regułę przychodzącą która nie pozwala na echo w przypadku komendy **ping**.
5. Spróbujcie wykonać ponownie wzajemny **ping**.
6. Po zakończeniu zadania usuń regułę.

III ANALIZA ZAAWANSOWANA W PARZE

1. Pobierz program arpspoof [www.github.com/alanda/arp spoof](https://github.com/alanda/arp spoof)
2. W razie konieczności doinstaluj www.winpcap.org/install/
3. Pod pierwszym linkiem znajduje się instrukcja w jaki sposób należy korzystać z oprogramowania.
4. Należy wymienić się adresem IP z partnerem.
5. Atakujący wykorzystuje **arpspoof** do zatrucia tablicy ARP ofiary oraz **Wireshark** do przechwycenia pakietów .
6. Ofiara znajduje niezabezpieczony formularz wykorzystujący protokół **HTTP**, dla testów wpisuje tam fikcyjne dane.
7. Atakujący musi odnaleźć login i hasło w logach **Wireshark**.
8. Zamiana ról.
9. **Wymyśl i wykonaj (w parze) nieprzedstawiony w materiale przykład wykorzystania zatrucia tablicy ARP.**