Wprowadzenie do sniffingu pakietów

Wprowadzenie

Witamy w przewodniku dla początkujących dotyczącym sniffingu pakietów. Sniffing pakietów to metoda przechwytywania pakietów danych przesyłanych przez sieć komputerową. Omówimy podstawy sniffingu pakietów i jak rozpocząć korzystanie z sniffingu pakietów za pomocą programu Wireshark. Omówimy, jak wybrać interfejs sieciowy, który chcesz podsłuchać, i jak przeprowadzić przechwytywanie pakietów. Omówimy również, jak podsłuchiwać pakiety sieciowe ze zdalnej lokalizacji oraz jak używać filtrów wyświetlania i przechwytywania, aby zawęzić zakres przechwytywanych pakietów. Ponadto omówimy sposoby maksymalizacji wydajności przechwytywania pakietów oraz jak zatrzymać podsłuchiwanie, zapisywać i eksportować pakiety do dalszej analizy. Po przeczytaniu tego rozdziału powinieneś dobrze rozumieć, jak rozpocząć korzystanie z sniffingu pakietów i potrafić korzystać z narzędzia do podsłuchiwania pakietów, takiego jak Wireshark.

Cele

Celem jest wyposażenie Cię w wiedzę i umiejętności niezbędne do efektywnego wykorzystania technik i narzędzi sniffingu pakietów w rzeczywistych sytuacjach. Załóżmy, że jesteś administratorem sieci i chcesz rozwiązać problemy z łącznością w sieci swojej firmy. Wiedząc, jak wykonać sniffing i użyć filtrów wyświetlania i przechwytywania, możesz zawęzić zakres pakietów do tych związanych z problemami z łącznością i zbadać je pod kątem wskazówek dotyczących przyczyny problemu. Alternatywnie, załóżmy, że jesteś analitykiem bezpieczeństwa i chcesz monitorować ruch sieciowy pod kątem potencjalnych zagrożeń. Wiedząc, jak sniffować pakiety sieciowe ze zdalnej lokalizacji i używając filtrów przechwytywania, aby skupić się na określonych typach ruchu, możesz łatwiej identyfikować podejrzane działania i podejmować odpowiednie działania w celu ochrony sieci. W obu tych przykładach maksymalizacja wydajności przechwytywania pakietów i skuteczne zatrzymanie podsłuchiwania, zapisywania i eksportowania pakietów ma kluczowe znaczenie dla efektywnego wykorzystania przechwyconych danych do analizy i rozwiązywania problemów. Do końca tego rozdziału powinieneś umieć zastosować swoją wiedzę na temat podsłuchiwania pakietów w różnych scenariuszach i skutecznie wykorzystywać techniki i narzędzia do przechwytywania i rejestrowania ruchu sieciowego w różnych celach.

Określ cele podsłuchu

Ważne jest, aby dokładnie wiedzieć, co chcesz podsłuchiwać, korzystając z technik i narzędzi do podsłuchiwania pakietów. Podsłuchiwanie pakietów umożliwia przechwytywanie i rejestrowanie ruchu sieciowego, a ilość danych, które można przechwycić, może być ogromna. Wiedza o tym, co chcesz podsłuchiwać, pomoże Ci zawęzić zakres pakietów, które chcesz przechwycić, i ułatwi analizę danych. Istnieje wiele powodów, dla których warto podsłuchiwać pakiety. Na przykład, możesz chcieć rozwiązywać problemy z łącznością, monitorować ruch sieciowy ze względów bezpieczeństwa lub analizować wydajność. Zanim zaczniesz podsłuchiwać pakiety, zastanów się, co chcesz osiągnąć i jakich konkretnych informacji szukasz. Pomoże Ci to określić najlepsze podejście do podsłuchiwania pakietów i zwiększyć jego skuteczność. Na przykład, jeśli chcesz rozwiązywać problemy z łącznością, możesz filtrować pakiety na podstawie określonych adresów IP lub numerów portów. Jeśli interesuje Cię bezpieczeństwo, możesz użyć filtrów przechwytywania, aby skupić się na określonych typach ruchu, takich jak HTTP lub FTP. Oto kilka przykładów scenariuszy, w których wiedza o tym, co chcesz monitorować, może być pomocna:

Przykład 1: Monitorowanie ruchu sieciowego w celach bezpieczeństwa

Jeśli jesteś analitykiem bezpieczeństwa i chcesz monitorować ruch sieciowy pod kątem potencjalnych zagrożeń, użycie filtrów przechwytywania, aby skupić się na określonych typach ruchu, może być przydatnym podejściem. Na przykład możesz użyć filtrów przechwytywania, aby skupić się na ruchu HTTP, który jest protokołem używanym do przesyłania danych w sieci WWW. Przechwytując tylko ruch HTTP, możesz łatwiej identyfikować podejrzane działania lub próby dostępu do nieautoryzowanych zasobów w sieci. Możesz również użyć filtrów przechwytywania, aby skupić się na ruchu FTP, który jest protokołem używanym do przesyłania plików w sieci. Przechwytując tylko ruch FTP, możesz monitorować transfery plików w sieci i identyfikować wszelkie podejrzane działania, takie jak próby przesyłania poufnych danych do nieautoryzowanych lokalizacji. Użycie filtrów przechwytywania, aby skupić się na określonych typach ruchu, może pomóc Ci łatwiej identyfikować podejrzane działania i podejmować odpowiednie działania w celu ochrony sieci. Może również pomóc Ci zmniejszyć ilość danych, które musisz analizować, co usprawni monitorowanie ruchu sieciowego pod kątem bezpieczeństwa.

Przykład 2: Hacking/etyczne hakowanie

Niezbędne jest precyzyjne określenie, co chcesz przechwycić, aby skoncentrować swoje wysiłki i skutecznie zebrać potrzebne informacje. Załóżmy, że jesteś hakerem lub hakerem etycznym przeprowadzającym test podatności/test penetracyjny sieci. Twoim celem jest zidentyfikowanie wszelkich luk lub słabości w sieci, które mogłyby zostać wykorzystane. W tym scenariuszu kluczowe jest określenie, co chcesz przechwycić, aby ukierunkować swoje wysiłki i zoptymalizować czas. Możesz użyć filtrów przechwytywania, aby skupić się na określonych typach ruchu, takich jak HTTP lub FTP, i filtrów wyświetlania, aby zawęzić zakres pakietów na podstawie określonych kryteriów, takich jak adresy IP lub numery portów. Wiedza o tym, co chcesz przechwycić i użycie odpowiednich filtrów może pomóc w łatwej identyfikacji luk lub słabości w sieci. Co więcej, jako atakujący możesz to wykorzystać, a jako etyczny haker możesz przedstawić klientowi praktyczne zalecenia dotyczące poprawy bezpieczeństwa.

Przykład 3: Analiza wydajności

Jeśli interesuje Cię analiza wydajności sieci, użycie filtrów przechwytywania, aby skupić się na określonych protokołach lub aplikacjach, może być użytecznym podejściem. Na przykład, możesz użyć filtrów przechwytywania, aby skupić się na konkretnym protokole, takim jak TCP lub UDP, aby zrozumieć, jak protokół jest używany w sieci. Następnie możesz przeanalizować pakiety, aby sprawdzić, jak działa protokół i zidentyfikować wszelkie potencjalne wąskie gardła lub inne problemy, które mogą wpływać na wydajność. Możesz również użyć filtrów przechwytywania, aby skupić się na konkretnych aplikacjach, takich jak poczta e-mail czy przeglądanie stron internetowych, i zrozumieć, w jaki sposób korzystają one z sieci. Może to pomóc w zidentyfikowaniu problemów z wydajnością, które mogą być specyficzne dla danej aplikacji i podjęciu kroków w celu poprawy wydajności. Użycie filtrów przechwytywania, aby skupić się na określonych protokołach lub aplikacjach, może pomóc w zrozumieniu sposobu korzystania z sieci i zidentyfikowaniu potencjalnych problemów z wydajnością. Może to również pomóc w zmniejszeniu ilości danych, które trzeba analizować, co usprawnia analizę wydajności sieci.

Przykład 4: Rozwiązywanie problemów z łącznością

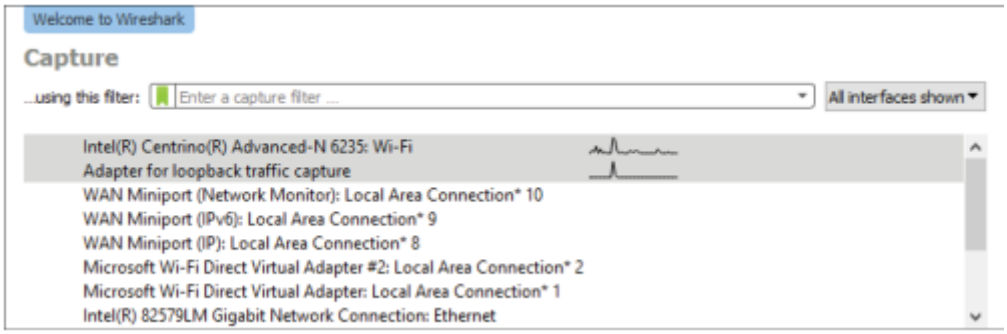
Jeśli jesteś administratorem sieci i próbujesz rozwiązać problemy z łącznością, możesz filtrować pakiety na podstawie określonych adresów IP lub numerów portów, aby skupić się na pakietach związanych z problemem z łącznością. Załóżmy, że próbujesz rozwiązać problem z łącznością między dwoma serwerami w sieci. Możesz użyć narzędzia do podsłuchiwania pakietów, aby przechwycić wszystkie pakiety między dwoma serwerami i poszukać wszelkich problemów lub błędów, które mogą

powodować problem z łącznością. Możesz również użyć filtrów wyświetlania, aby zawęzić wyszukiwanie pakietów na podstawie określonych kryteriów, takich jak adresy IP lub numery portów serwerów. Pozwoli Ci to skupić się na pakietach najbardziej istotnych dla problemu z łącznością i ułatwi znalezienie jego przyczyny. Po przechwyceniu i odfiltrowaniu pakietów możesz użyć graficznego interfejsu narzędzia do podsłuchiwania pakietów, aby je przeanalizować i sprawdzić, co dzieje się w sieci. Pomoże Ci to zidentyfikować wszelkie problemy, które mogą powodować problemy z łącznością i podjąć kroki w celu ich rozwiązania.

Wybór interfejsów sieciowych

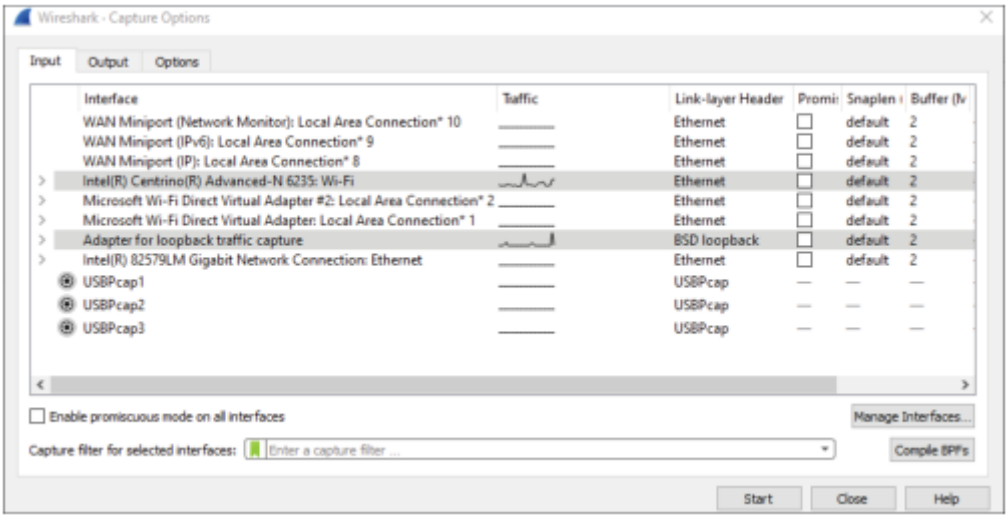
Prawidłowy wybór interfejsu sieciowego w programie Wireshark jest ważny, ponieważ decyduje o tym, które pakiety program będzie przechwytywać i wyświetlać. Wybór niewłaściwego interfejsu może uniemożliwić wyświetlenie interesującego ruchu lub może spowodować jego nadmierne natężenie i uniemożliwić skuteczne filtrowanie. Wybór właściwego interfejsu sieciowego może być również istotny ze względu na wydajność. Jeśli przechwytujesz pakiety w obciążonej sieci, użycie szybkiego interfejsu może pomóc zapewnić, że Wireshark będzie w stanie nadążać za ruchem i unikać gubienia pakietów. Z drugiej strony, jeśli przechwytujesz pakiety w wolnej lub przeciążonej sieci, użycie wolniejszego interfejsu może pomóc uniknąć przeciążenia interfejsu i utraty pakietów. Ogólnie rzecz biorąc, warto dokładnie rozważyć, którego interfejsu używać podczas przechwytywania pakietów w programie Wireshark i wybrać ten, który najlepiej odpowiada Twoim potrzebom. Teraz pytanie brzmi: Jak wybrać konkretny interfejs sieciowy lub wiele interfejsów?

1. Jednym ze sposobów jest wybranie konkretnego interfejsu sieciowego z ekranu startowego programu Wireshark. Ekran startowy wyświetli listę dostępnych interfejsów sieciowych, jak pokazano na rysunku .



Kliknij interfejs, którego chcesz użyć, i kliknij przycisk Start, aby rozpocząć przechwytywanie pakietów na tym interfejsie. Aby zaznaczyć wiele interfejsów, użyj kombinacji klawiszy Shift i lewego przycisku myszy. Po zaznaczeniu rozpocznij przechwytywanie.

2. Innym sposobem jest wybranie interfejsu poprzez kliknięcie opcji „Przechwyć” w menu, wybranie opcji „Opcje” i wybranie odpowiedniego interfejsu z listy dostępnych interfejsów na karcie „Wejście”, klikając go, lub zaznaczenie wielu interfejsów za pomocą kombinacji klawiszy Shift i lewego przycisku myszy, jak pokazano na rysunku 2. Następnie kliknij przycisk „Start”.



3. Alternatywnie, możesz również wybrać interfejs sieciowy z wiersza poleceń, używając opcji -i, a następnie nazwy lub numeru interfejsu, którego chcesz użyć. Na przykład:

wireshark -i eth0

Spowoduje to otwarcie programu Wireshark i wybranie interfejsu eth0. Możesz również określić wiele interfejsów, rozdzielając je przecinkami, w następujący sposób:

wireshark -i eth0,eth1

Spowoduje to przechwycenie pakietów zarówno na interfejsie eth0, jak i eth1. Pamiętaj, że do przechwytywania pakietów na danym interfejsie wymagane są uprawnienia roota lub odpowiednie uprawnienia.

Uwaga: Jeśli nie masz pewności, jakie interfejsy są dostępne w Twoim systemie, możesz użyć polecenia netsh, aby wyświetlić i zarządzać interfejsami sieciowymi w systemie. Na przykład poniższe polecenie wyświetli listę wszystkich dostępnych interfejsów sieciowych.

netsh interface show interface

Rysunek 3 przedstawia listę interfejsów sieciowych, które są obecnie dostępne.

```
c:\Program Files\Wireshark>netsh interface show interface

Admin State    State          Type             Interface Name
-------------------------------------------------------------------------
Enabled        Connected      Dedicated        Wi-Fi
Enabled        Disconnected   Dedicated        Ethernet
```

4. Po potwierdzeniu interfejsu, uruchom wiersz poleceń Wiresharka, używając opcji -i, a następnie naciśnij Enter, jak pokazano na rysunku 4.

```
c:\Program Files\Wireshark>wireshark -i Wi-Fi

c:\Program Files\Wireshark>

** (wireshark:84548) 15:44:48.454393 [Capture MESSAGE] -- Capture Start ...
** (wireshark:84548) 15:44:48.679591 [Capture MESSAGE] -- Capture started
** (wireshark:84548) 15:44:48.682456 [Capture MESSAGE] -- File: "C:\Users\OUCARA~1\AppData\Local\Temp\wireshark_Wi-FI8
4JY1.pcapng"
** (wireshark:84548) 15:45:01.159508 [Capture MESSAGE] -- Capture Stop ...
** (wireshark:84548) 15:45:01.382173 [Capture MESSAGE] -- Capture stopped.
```

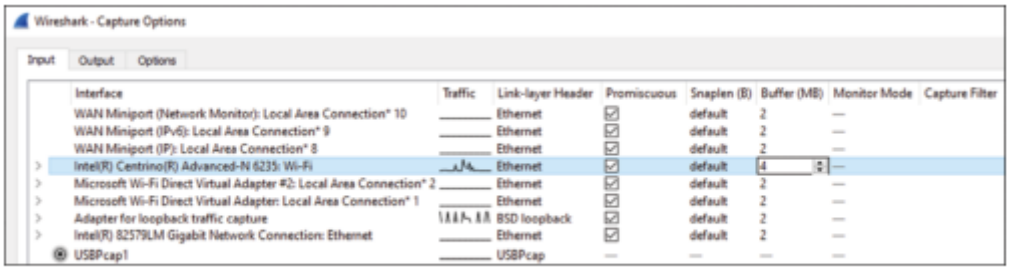
Wireshark zostanie otwarty i rozpocznie przechwytywanie pakietów z głównego paska narzędzi. Rozpocznie się przechwytywanie, a szczegóły będą widoczne również w wierszu poleceń.

Uwaga: Jeśli nie wybrano żadnego interfejsu, na pasku stanu pojawi się komunikat ostrzegawczy o treści „Nie wybrano żadnego interfejsu”, jak pokazano na rysunku 5:

Jeśli wybierzesz niewłaściwy interfejs w programie Wireshark, przechwytywanie pakietów nie pokaże żadnego ruchu, ponieważ Wireshark nie może odebrać żadnych pakietów na wybranym interfejsie. Może się tak zdarzyć, jeśli interfejs nie jest podłączony do sieci lub nie jest poprawnie skonfigurowany. Aby rozwiązać ten problem, spróbuj wybrać inny interfejs lub sprawdź konfigurację interfejsu, aby upewnić się, że jest on poprawnie podłączony i skonfigurowany.

Przeprowadzanie sniffingu pakietów

Po wybraniu interfejsu lub kilku interfejsów, zgodnie z wymaganiami, możesz rozpocząć sniffing i przechwytywanie pakietów na wybranych interfejsach. Domyślnie Wireshark będzie kontynuował przechwytywanie i wyświetlanie pakietów do momentu zapełnienia bufora przechwytywania. Bufor przechwytywania to część pamięci używana do przechowywania pakietów podczas ich przechwytywania i analizy. Gdy bufor przechwytywania się zapełni, Wireshark zatrzyma przechwytywanie pakietów i wyświetli komunikat na pasku stanu informujący o zatrzymaniu przechwytywania. Rozmiar bufora przechwytywania można zmienić, przechodząc do menu Przechwytywanie, a następnie wybierając Opcje. Tutaj możesz dostosować rozmiar bufora przechwytywania z zakładki Wejście, a także inne ustawienia związane z przechwytywaniem pakietów, jak pokazano na rysunku 6:



Należy pamiętać, że zwiększenie rozmiaru bufora przechwytywania pozwoli programowi Wireshark przechowywać więcej pakietów przed zatrzymaniem przechwytywania, ale spowoduje to również większe zużycie pamięci i może wpłynąć na wydajność systemu.

Opcje przechwytywania: Karta Wejściowa

Rysunek 7 przedstawia kartę Wejściową okna dialogowego Opcje przechwytywania w programie Wireshark. Możemy zapoznać się z dodatkowymi opcjami dostępnymi na tej karcie.

Zawiera kilka opcji, których można użyć do konfiguracji przechwytywania:

Interfejs: To menu rozwijane umożliwia wybór interfejsu sieciowego, na którym Wireshark ma przechwytywać pakiety.

Ruch: Ta opcja pozwala określić, czy Wireshark ma przechwytywać cały ruch na interfejsie, czy tylko ruch wysyłany lub odbierany przez hosta.

Nagłówek warstwy łącza: Ta opcja pozwala określić typ nagłówka warstwy łącza, który ma być używany podczas przechwytywania pakietów. Nagłówek warstwy łącza to część pakietu zawierająca informacje o warstwie fizycznej sieci, takie jak adresy MAC nadawcy i odbiorcy.

Promiscuous: To pole wyboru umożliwia włączenie lub wyłączenie trybu promiscuous na interfejsie. W trybie promiscuous interfejs przechwytuje wszystkie pakiety przesyłane w sieci, niezależnie od tego, czy są przeznaczone dla interfejsu, czy nie.

Snaplen (B): To pole pozwala określić długość migawki, czyli maksymalną liczbę bajtów, które powinny być przechwytywane dla każdego pakietu.

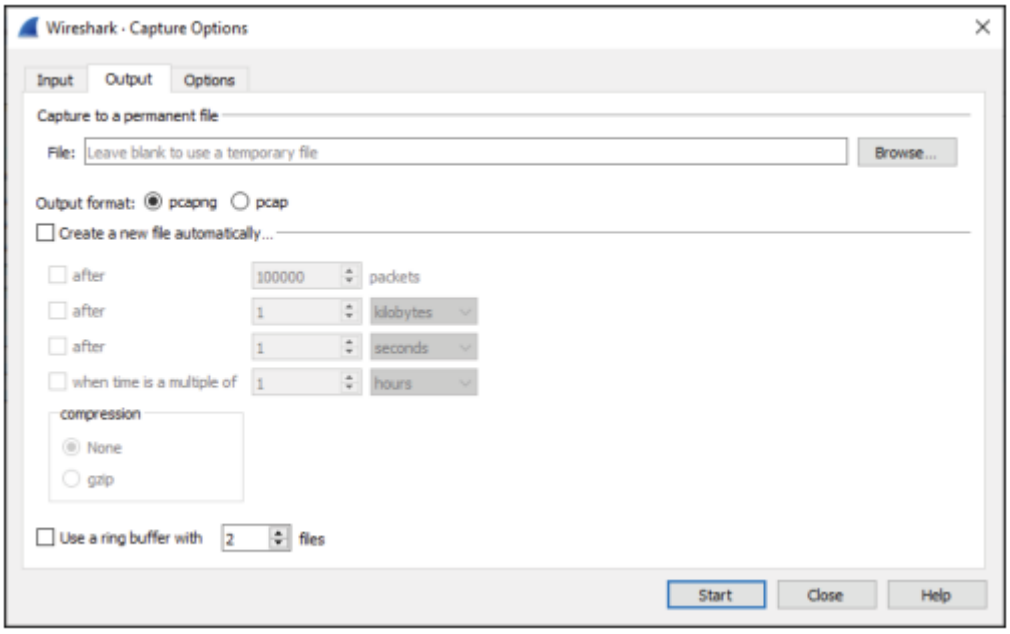
Bufor (MB): To pole umożliwia określenie rozmiaru bufora przechwytywania, czyli ilości pamięci używanej do przechowywania pakietów podczas ich przechwytywania i analizowania.

Tryb monitorowania: To pole wyboru umożliwia włączenie lub wyłączenie trybu monitorowania w interfejsie bezprzewodowym. W trybie monitorowania interfejs może przechwytywać wszystkie pakiety przesyłane bezprzewodowo, w tym pakiety nieprzeznaczone dla tego interfejsu.

Filtr przechwytywania: To pole umożliwia określenie wyrażenia filtra przechwytywania, które będzie używane do wybierania przechwytywanych pakietów. Filtry przechwytywania wykorzystują składnię filtru pakietów Berkeley (BPF) i pozwalają określić kryteria, które pakiet musi spełniać, aby został przechwycony.

Opcje przechwytywania: Karta Wyjście

Karta Wyjście w oknie dialogowym Opcje przechwytywania w programie Wireshark umożliwia określenie miejsca i sposobu zapisywania przechwyconych pakietów, jak pokazano na rysunku 8. Dostęp do tej karty można uzyskać, przechodząc do menu Przechwytywanie, wybierając Opcje i klikając kartę Wyjście.



Pole „Przechwyć do” pozwala określić miejsce, w którym przechwycone pakiety mają być zapisywane. Możesz wybrać zapisanie pakietów do pliku, klikając przycisk „Przeglądaj”, aby wybrać lokalizację, w której plik ma zostać zapisany.

Pole „Format wyjściowy” pozwala określić format, w którym pakiety mają być zapisywane. Wireshark obsługuje formaty wyjściowe „pcapng” i „pcap”. Możesz wybrać format, który najlepiej odpowiada Twoim potrzebom.

Opcja „Utwórz nowy plik automatycznie” pozwala określić, że nowy plik ma być tworzony automatycznie w określonych odstępach czasu lub gdy rozmiar pliku osiągnie określony limit.

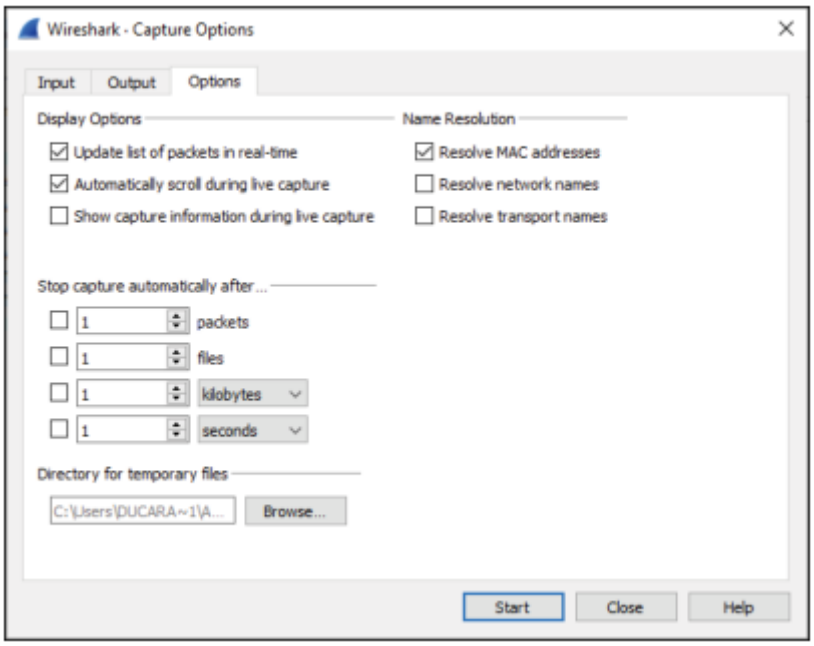
Opcja „Kompresja” pozwala określić poziom kompresji, który ma być używany podczas zapisywania przechwyconego ruchu do pliku.

Opcja „Użyj bufora pierścieniowego z” pozwala określić, że przechwycone pakiety mają być zapisywane w serii plików o stałej maksymalnej liczbie plików.

Za pomocą opcji na karcie Wyjście można określić miejsce i sposób zapisywania przechwyconych pakietów. Może to być przydatne do przechowywania przechwyconych pakietów do późniejszej analizy lub udostępniania ich innym osobom.

Opcje przechwytywania: Karta Opcje

Na rysunku 9 widoczna jest karta Opcje, która przedstawia dodatkowe konfiguracje, które można dostosować podczas przechwytywania ruchu sieciowego.



Opcje dostępne na tej karcie obejmują:

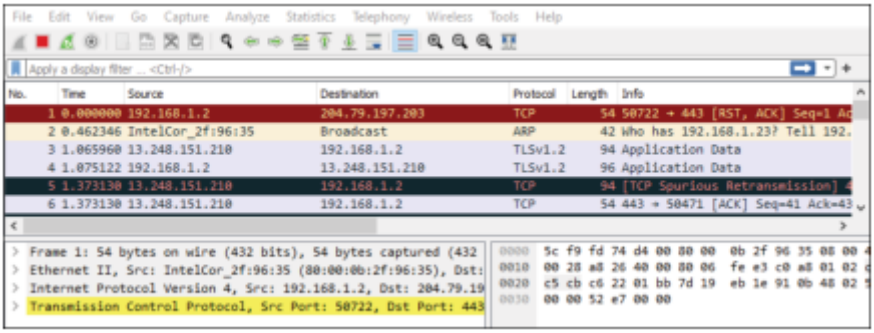
Opcje wyświetlania: Umożliwia określenie opcji wyświetlania przechwyconych pakietów, takich jak aktualizowanie listy pakietów w czasie rzeczywistym, automatyczne przewijanie podczas przechwytywania na żywo oraz wyświetlanie informacji o przechwytywaniu podczas przechwytywania na żywo.

Rozpoznawanie nazw: Pozwala określić, czy Wireshark ma rozwiązywać adresy sieciowe na nazwy hostów podczas przechwytywania ruchu sieciowego. Oferuje również opcje rozwiązywania adresów MAC, nazw sieciowych i nazw transportowych.

Zatrzymaj przechwytywanie automatycznie po: Pozwala określić, że przechwytywanie ma zostać zatrzymane po określonej liczbie pakietów lub po określonym czasie.

Katalog plików tymczasowych: Pozwala określić katalog, w którym mają być zapisywane tymczasowe pliki przechwytywania podczas procesu przechwytywania.

Opcje te umożliwiają precyzyjne dostrojenie procesu przechwytywania, zwiększają wydajność przechwytywania ruchu sieciowego i ułatwiają zarządzanie plikami tymczasowymi. Opcje wyświetlania ułatwiają nawigację i analizę przechwyconych pakietów podczas przechwytywania na żywo. Opcje rozpoznawania nazw mogą dostarczyć bardziej znaczących informacji, a opcja automatycznego zatrzymania przechwytywania po określonej liczbie pakietów lub po upływie określonego czasu może zapobiec niekończącemu się działaniu procesu przechwytywania. Kliknij przycisk Start, aby rozpocząć podsłuchiwanie/przechwytywanie pakietów na wybranym interfejsie sieciowym lub wielu interfejsach, jak pokazano na rysunku 10.



Przechwycone pakiety zostaną wyświetlone w panelu „Lista pakietów” w oknie programu Wireshark. Więcej szczegółów można znaleźć w panelach „Szczegóły pakietu” i „Bajty pakietu”. Panele te umożliwiają analizę szczegółów pakietu i zrozumienie jego konstrukcji oraz roli w ogólnej komunikacji sieciowej.

Zdalny pakiet sieciowy

Podsłuchiwanie pakietów sieciowych ze zdalnej lokalizacji polega na przechwytywaniu ruchu sieciowego w sieci zdalnej, a następnie przesyłaniu przechwyconych danych z powrotem do komputera lokalnego w celu analizy. Można to osiągnąć za pomocą różnych narzędzi i technik, takich jak:

Zdalne przechwytywanie pakietów: Niektóre urządzenia sieciowe, takie jak routery i przełączniki, posiadają wbudowane funkcje przechwytywania pakietów, do których można uzyskać zdalny dostęp. Pozwala to na skonfigurowanie urządzenia do przechwytywania pakietów, a następnie pobierania przechwyconych danych ze zdalnej lokalizacji.

Zdalny sniffer: Niektóre programy do podsłuchiwania pakietów, takie jak Wireshark, mogą działać w trybie zdalnego sniffera, co pozwala na przechwytywanie pakietów na komputerze zdalnym i przesyłanie przechwyconych danych z powrotem do komputera lokalnego w celu analizy. Można to zrobić za pomocą funkcji zdalnego przechwytywania Wireshark. Wymaga to, aby komputer zdalny miał zainstalowany Wireshark i skonfigurowaną funkcję zdalnego przechwytywania.

Tunelowanie: Tunelowanie to technika umożliwiająca enkapsulację jednego protokołu sieciowego w innym. Można go użyć do przesyłania ruchu sieciowego przez niezabezpieczoną sieć, taką jak Internet, a następnie przechwytywania ruchu na odległym końcu tunelu. Na przykład, można użyć protokołu Secure Shell (SSH) do utworzenia bezpiecznego połączenia między komputerem zdalnym a lokalnym, a następnie użyć programu Wireshark do przechwytywania ruchu sieciowego przez tunel SSH.

VPN: Wirtualne sieci prywatne (VPN) umożliwiają utworzenie bezpiecznego połączenia między dwoma urządzeniami sieciowymi. Można ich używać do przechwytywania ruchu sieciowego w sieci zdalnej i przesyłania przechwyconych danych z powrotem do komputera lokalnego w celu analizy. Wireshark może być używany do przechwytywania ruchu sieciowego w sieci zdalnej, a następnie przechwycone dane mogą być przesyłane z powrotem do komputera lokalnego za pośrednictwem połączenia VPN.

Należy pamiętać, że działania te mogą być nielegalne lub nieetyczne, w zależności od sytuacji. Zawsze warto uzyskać pozwolenie lub mieć ku temu podstawy prawne przed rozpoczęciem procesu sniffingu. W tym przypadku, aby sniffować pakiety sieciowe ze zdalnej lokalizacji, potrzebujemy:

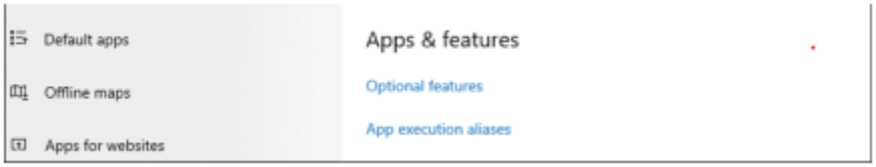
Zdalnego komputera z serwerem SSH i zainstalowanym programem tshark; Dostępu do konta root komputera zdalnego; Usług generujących ruch sieciowy na komputerze zdalnym; Komputera lokalnego z klientem SSH i zainstalowanym programem Wireshark;

Instalacji SSH na zdalnym komputerze z systemem Windows

Komponenty OpenSSH można zainstalować za pomocą Ustawień systemu Windows na urządzeniach z systemem Windows Server 2019 i Windows 10.

Aby zainstalować komponenty OpenSSH:

1. Otwórz Ustawienia systemu Windows, wybierz Aplikacje, a następnie wybierz Funkcje opcjonalne w obszarze Aplikacje i funkcje, jak pokazano na rysunku 11:



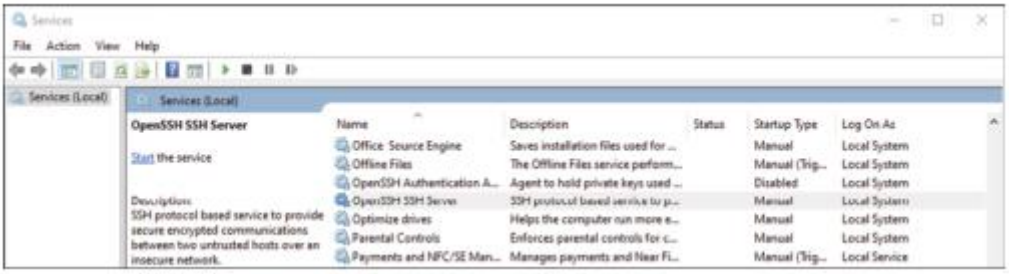
2. Sprawdź na liście, czy serwer OpenSSH jest już zainstalowany. Jeśli nie, u góry strony wybierz opcję „Dodaj funkcję opcjonalną”, a następnie znajdź serwer OpenSSH, wybierz go i kliknij „Zainstaluj”, jak pokazano na rysunku 12:

3. Po zakończeniu instalacji sprawdź listę zainstalowanych funkcji w sekcji Funkcje opcjonalne i upewnij się, że serwer OpenSSH znajduje się na liście na komputerze zdalnym.

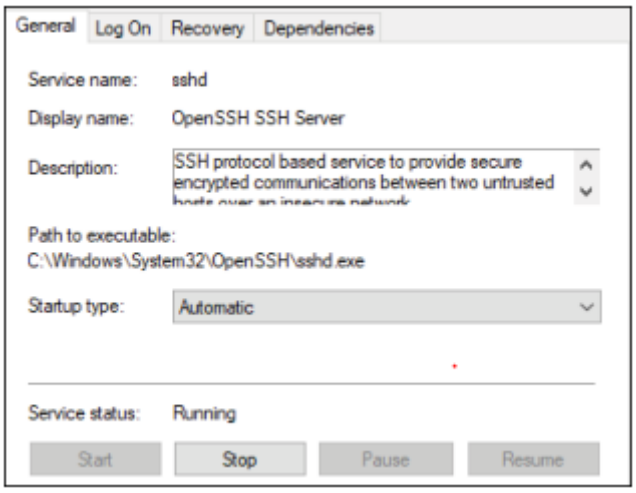
Uwaga: Wykonaj tę samą procedurę, aby zainstalować klienta OpenSSH na komputerze lokalnym z systemem Windows.

4. Otwórz aplikację pulpitu Usługi. (Wybierz Start, wpisz services.msc w polu wyszukiwania, a następnie wybierz aplikację Usługi lub naciśnij Enter).

5. Aby znaleźć serwer OpenSSH SSH, wyszukaj go i kliknij dwukrotnie, jak pokazano na rysunku 13. Spowoduje to otwarcie karty Właściwości.



6. Na karcie Ogólne znajdź menu rozwijane „Typ uruchomienia” i wybierz „Automatyczny” z dostępnych opcji, jak pokazano na rysunku 14. Następnie wybierz opcję „Uruchom”, aby zainicjować usługę. Możesz teraz obserwować aktualny stan usługi.



Instalacja SSH na zdalnym komputerze z systemem Linux

Aby zainstalować serwer SSH na komputerze z systemem Linux:

1. Wpisz polecenie:

sudo apt-get install openssh-server

Uwaga: Używając tej samej procedury, możesz zainstalować klienta OpenSSH na lokalnym komputerze z systemem Linux.

2. Skonfiguruj usługę SSH tak, aby uruchamiała się automatycznie podczas rozruchu, używając następującego polecenia:

sudo systemctl enable ssh

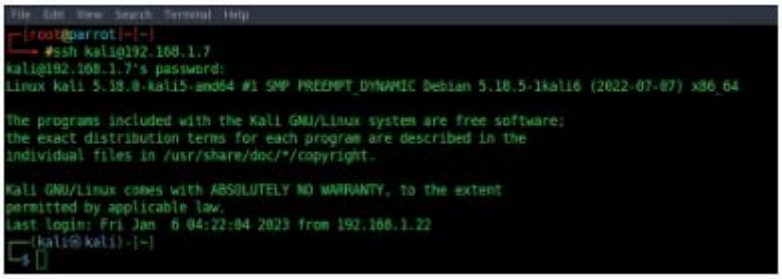
3. Uruchom usługę SSH za pomocą następującego polecenia:

sudo systemctl start ssh

Po pomyślnej instalacji serwera SSH na komputerze zdalnym i klienta SSH na komputerze lokalnym, naszym celem jest użycie poleceń tshark na komputerze zdalnym, przez SSH, do przechwytywania ruchu sieciowego. Następnie przechwycony ruch można skopiować na komputer lokalny w celu analizy za pomocą Wiresharka. Jest to przydatne, gdy nie masz fizycznego dostępu do komputera zdalnego lub uruchamiasz go „bezgłowie”, czyli bez klawiatury i monitora.

1. Krok 1 to zdalne przechwytywanie pakietów za pomocą tshark przez SSH. Aby przechwycić ruch za pomocą polecenia tshark, najpierw musimy połączyć się ze zdalnym komputerem przez SSH. Aby zdalnie przechwytywać pakiety za pomocą tshark przez SSH, możesz użyć następującego polecenia, jak pokazano na rysunku 15:

ssh user@remote_host



To polecenie łączy się ze zdalnym hostem za pomocą protokołu SSH z określoną nazwą użytkownika (user) i uruchamia polecenie tshark na komputerze zdalnym.

Uwaga: Wymagane będą również uprawnienia użytkownika root lub sudo na komputerze zdalnym. W przeciwnym razie tshark nie będzie mógł przechwytywać ruchu i pojawi się komunikat o błędzie: „Nie masz uprawnień do przechwytywania na tym urządzeniu”.

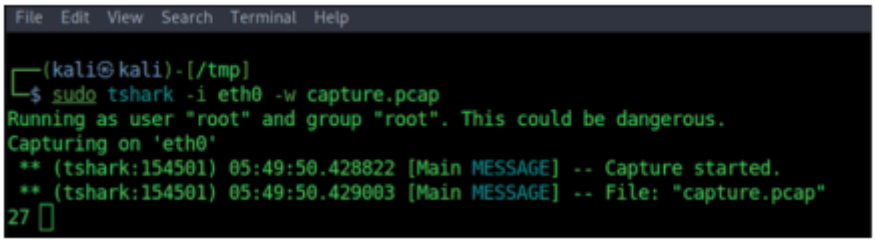
Po nawiązaniu połączenia ze zdalnym hostem za pomocą protokołu SSH uruchom następujące polecenie, aby rozpocząć przechwytywanie ruchu za pomocą tshark:

tshark -i interface -w capture_file

Opcja -i określa interfejs sieciowy, na którym mają być przechwytywane pakiety. Możesz określić nazwę interfejsu (na przykład eth0) lub użyć słowa kluczowego any, aby przechwytywać pakiety ze wszystkich interfejsów. Opcja -w określa plik, w którym mają być zapisywane przechwycone pakiety. Możesz określić ścieżkę i nazwę pliku przechwytywania. Na przykład, aby zapisać pakiety do pliku o nazwie „capture.pcap” w katalogu domowym bieżącego użytkownika,

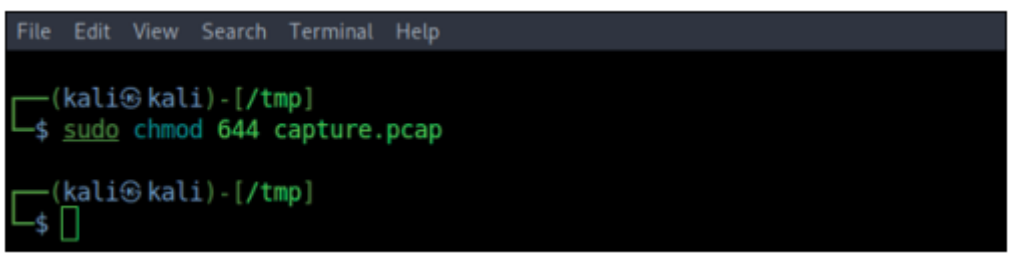
użyj następującego polecenia, jak pokazano na rysunku 16:

tshark -i eth0 -w capture.pcap



Zanim będzie można skopiować przechwycony plik z komputera zdalnego na komputer lokalny w celu analizy za pomocą Wiresharka, należy zmienić uprawnienia pliku. Domyślnie sesje tshark przechwycone przez użytkownika root nie mogą być kopiowane. Aby zmienić uprawnienia pliku, można użyć polecenia chmod, jak pokazano na rysunku 17. Oto przykładowe polecenie:

sudo chmod 644 capture.pcap



To polecenie nada uprawnienia do odczytu i zapisu właścicielowi pliku, a uprawnienia tylko do odczytu pozostałym użytkownikom. Oznacza to, że właściciel pliku może go odczytywać i zapisywać, podczas gdy inni użytkownicy mogą go tylko odczytywać. Teraz możesz skopiować plik na komputer lokalny za pomocą protokołu SCP, jak opisano w następnym kroku.

2. Drugim krokiem jest skopiowanie sesji tshark do analizy. Bezpieczna kopia (SCP) to wygodny sposób na przeniesienie pliku przechwytywania z komputera, na którym uruchomiono TShark, na komputer, na którym zainstalowano Wireshark do analizy. Użytkownicy systemu Windows muszą pobrać plik wykonywalny pscp i dodać go do ścieżki systemowej PATH, ale nie jest konieczne kopiowanie go do C:\Windows\System32. Zamiast tego można dodać katalog, w którym znajduje się plik pscp.exe, do zmiennej środowiskowej PATH, aby można było go uruchomić z dowolnego katalogu. Aby użyć narzędzia pscp.exe w systemie Windows, należy otworzyć program PowerShell i uruchomić następujące polecenie:

pscp.exe kali@192.168.1.7:/ścieżka/do/pliku.

To polecenie skopiuje plik znajdujący się w katalogu „/ścieżka/do/pliku" na komputerze o adresie IP „192.168.1.7" (w tym przykładzie komputer ma nazwę „kali") i skopiuje go do bieżącego katalogu na komputerze lokalnym. Przecinek „." na końcu polecenia określa bieżący katalog jako docelowy. Zostaniesz poproszony o podanie hasła dla komputera zdalnego. Po wprowadzeniu prawidłowego hasła plik zostanie skopiowany na komputer lokalny.

Ponadto użytkownicy komputerów Mac i Linux nie muszą pobierać żadnego dodatkowego oprogramowania, ponieważ SCP jest zazwyczaj domyślnie zawarty w systemie operacyjnym. Polecenie „scp" jest wbudowane i gotowe do użycia. Aby użyć polecenia SCP na komputerze Mac lub Linux, można otworzyć okno terminala i uruchomić następujące polecenie, aby skopiować plik przechwytywania:

scp kali@192.168.1.7:/tmp/capture.pcap.

To polecenie skopiuje plik „capture.pcap" znajdujący się w katalogu „/tmp" na komputerze o adresie IP „192.168.1.7" (w tym przykładzie komputer ma nazwę kali) i skopiuje go do bieżącego katalogu na komputerze lokalnym. Przecinek „." na końcu polecenia określa bieżący katalog jako docelowy. Zostaniesz poproszony o podanie hasła dla komputera zdalnego. Po wprowadzeniu prawidłowego hasła plik zostanie skopiowany na komputer lokalny. Należy pamiętać, że folder docelowy musi istnieć. W przeciwnym razie transfer się nie powiedzie.

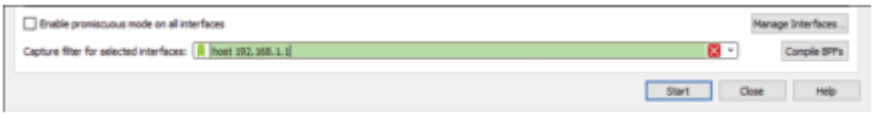
Filtry wyświetlania i przechwytywania

Jedną z potężnych funkcji programu Wireshark jest możliwość filtrowania wyświetlanych i przechwytywanych pakietów. W programie Wireshark dostępne są dwa rodzaje filtrów: filtry przechwytywania i filtry wyświetlania.

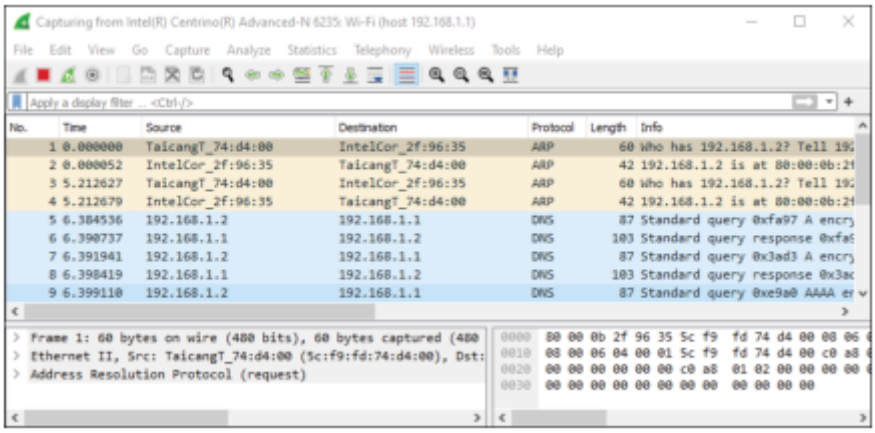
Filtry przechwytywania

Filtry przechwytywania są stosowane przed przechwyceniem pakietów i pozwalają określić, które pakiety mają zostać zapisane w pliku przechwytywania. Może to być przydatne w celu zmniejszenia ilości danych do analizy i przechwytywania tylko określonych typów ruchu. Filtry przechwytywania można ustawić w programie Wireshark za pomocą opcji Przechwytywanie z menu. Wybierz „Opcje" z menu rozwijanego. W oknie dialogowym Opcje przechwytywania wybierz interfejs, na którym chcesz przechwytywać pakiety. W polu „Filtr przechwytywania dla wybranych interfejsów" wpisz żądane wyrażenie filtru. Aby przechwycić wszystkie pakiety wysyłane do lub z określonego adresu IP, można

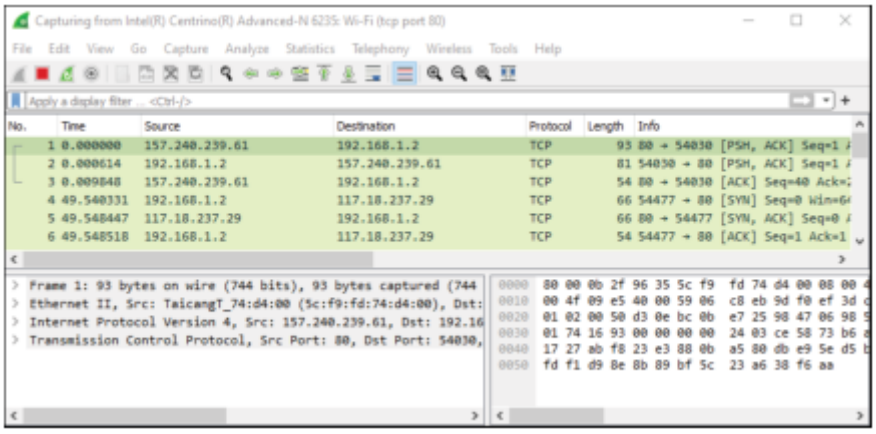
zastosować filtr „host 192.168.1.1”, jak pokazano na rysunku 18. Filtr ten przechwyci wszystkie pakiety wysyłane do lub z adresu IP 192.168.1.1.



Rysunek 19 przedstawia wyniki zastosowania filtru „host 192.168.1.1”. Na rysunku tym można zaobserwować przechwycone pakiety, które są ściśle powiązane z adresem IP 192.168.1.1.



W ten sposób możemy ograniczyć ilość danych rejestrowanych i zapisywanych w pliku przechwytywania, co może zwiększyć efektywność i celowość analizy. Rejestrując tylko pakiety spełniające określone kryteria, można zmniejszyć ilość nieistotnych danych, które trzeba przeszukiwać. Innym przykładem jest sytuacja, gdy chcesz przechwytywać tylko pakiety TCP wysyłane do lub z portu 80 (HTTP), możesz użyć filtru „tcp port 80”. Po zastosowaniu filtru „tcp port 80”, jak pokazano na rysunku 20, przechwytywane będą tylko pakiety TCP wysyłane do lub z portu 80 (HTTP). Rysunek ilustruje wynik przechwytywania pakietów po zastosowaniu tego filtru, umożliwiając obserwację konkretnego ruchu TCP związanego z portem 80.

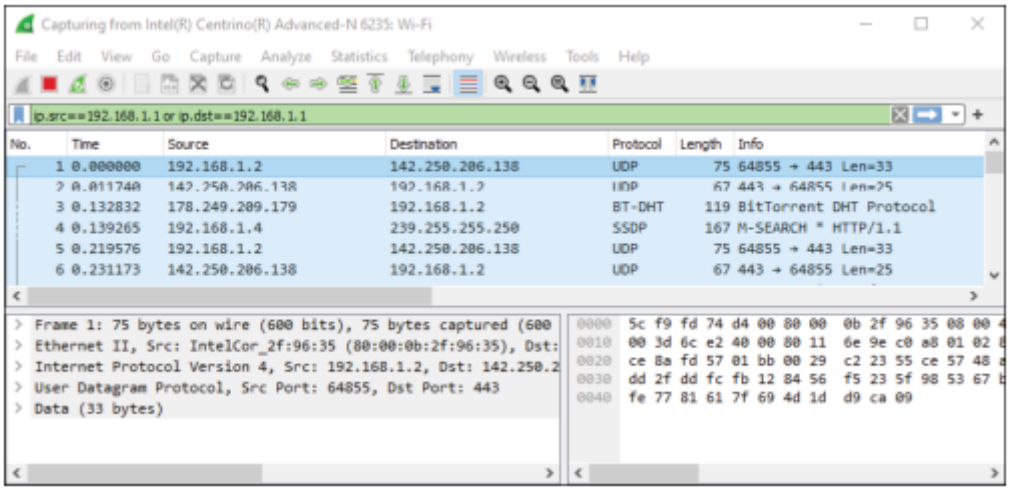


Teraz możesz zobaczyć, że przechwycone pakiety obejmują TYLKO pakiety TCP, których port docelowy lub źródłowy wynosi 80. Podczas pracy z filtrami przechwytywania należy pamiętać, że filtr jest stosowany przed przechwyceniem pakietów, więc tylko pakiety spełniające określone kryteria zostaną zapisane w pliku przechwytywania. Oznacza to, że jeśli później zechcesz przeanalizować pakiety, które nie spełniają kryteriów filtrowania, nie znajdą się one w pliku przechwytywania i nie będziesz mógł ich wyświetlić w Wireshark. Warto również zauważyć, że filtry przechwytywania mają bardziej

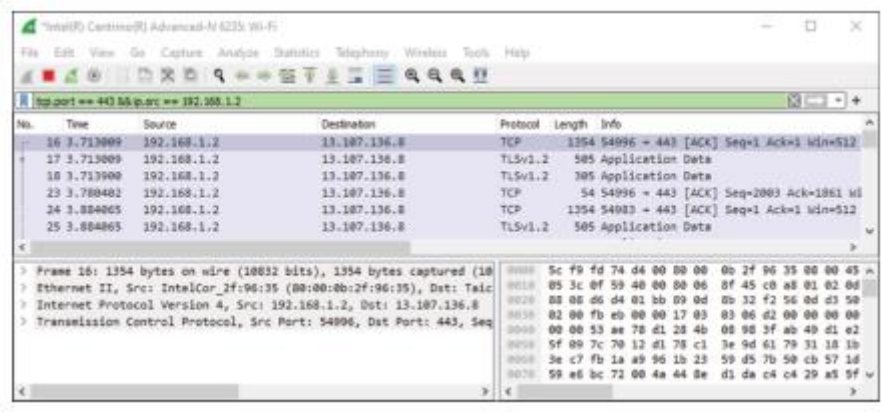
rozbudowaną składnię niż filtry wyświetlania, dzięki czemu możesz użyć bardziej złożonych wyrażeń, aby dopasować pakiety, które chcesz przechwycić.

Filtry wyświetlania

Filtry wyświetlania pozwalają skupić się na konkretnych pakietach, odfiltrowując pakiety niespełniające określonych kryteriów. Filtry te są stosowane po przechwyceniu pakietów i pozwalają wyświetlić tylko interesujące Cię pakiety. Na przykład, jeśli rozwiązujesz problem z określonym adresem IP, możesz użyć filtra wyświetlania, aby wyświetlić tylko pakiety zawierające ten adres IP. Wyrażenie filtru w tym przypadku wyglądałoby następująco: „ip.src == 192.168.1.1 lub ip.dst == 192.168.1.1”. Spowoduje to wyświetlenie wszystkich pakietów wysłanych z lub do adresu IP 192.168.1.1, jak pokazano na rysunku 21:



Innym przykładem jest filtr „tcp.port == 443 && ip.src == 192.168.1.2” w Wireshark, który wyświetli tylko pakiety TCP o adresie IP źródłowym 192.168.1.2 i porcie docelowym 443, jak pokazano na rysunku 22.



Filtr sprawdza określony warunek w dwóch polach: tcp.port i ip.src. Pierwszy warunek to wartość pola tcp.port równa 443. Drugi warunek to wartość pola ip.src równa 192.168.1.2. Operator && służy do połączenia tych dwóch warunków i dopasowania tylko pakietów spełniających oba warunki.

Niektóre z operatorów w Wireshark to:

"==" (równe): Dopasowuje pakiety, w których wartość określonego pola jest równa określonej wartości. Na przykład "tcp.port == 443" dopasowuje pakiety z portem docelowym 443.

"!=" (nierówne): Dopasowuje pakiety, w których wartość określonego pola nie jest równa określonej wartości. Na przykład "tcp.port != 80" dopasowuje pakiety z portem docelowym innym niż 80.

">" (większe niż): Dopasowuje pakiety, w których wartość określonego pola jest większa niż określona wartość. Na przykład "tcp.window_size > 1000" dopasowuje pakiety z rozmiarem okna większym niż 1000 bajtów.

"<" (mniejsze niż): Dopasowuje pakiety, w których wartość określonego pola jest mniejsza niż określona wartość. Na przykład „tcp.window_size < 1000” dopasowuje pakiety o rozmiarze okna mniejszym niż 1000 bajtów.

„>=" (większy lub równy): dopasowuje pakiety, w których wartość określonego pola jest większa lub równa określonej wartości.

„<=" (mniejszy lub równy): dopasowuje pakiety, w których wartość określonego pola jest mniejsza lub równa określonej wartości.

„&&” (i): dopasowuje pakiety, w których oba warunki są spełnione. Na przykład „tcp.port == 80 && ip.src == 10.0.0.1” dopasowuje pakiety z portem docelowym 80 i źródłowym adresem IP 10.0.0.1.

„||” (lub): dopasowuje pakiety, w których co najmniej jeden warunek jest spełniony. Na przykład „tcp.port == 80 || tcp.port == 443” dopasowuje pakiety z portem docelowym 80 lub 443.

„!” (not): neguje warunek. Na przykład „!(tcp.port == 80)” dopasowuje pakiety z portem docelowym innym niż 80.

Są to podstawowe operatory; Wireshark obsługuje również bardziej złożone i zaawansowane operatory do tworzenia niestandardowych filtrów. Należy pamiętać, że składnia pola filtru rozróżnia wielkość liter, a użycie spacji i znaków specjalnych, takich jak „=” i „!”, musi być przestrzegane.

Maksymalizacja wydajności przechwytywania pakietów

Narzędzia do przechwytywania pakietów mogą mieć problemy z wydajnością w przypadku szybkich sieci i dużego natężenia ruchu. Trzy zadania: odczyt pakietów z interfejsów sieciowych, przetwarzanie ich oraz przechowywanie lub wyświetlanie wyników, mogą stać się wąskim gardłem w przypadku milionów pakietów na sekundę. Aby rozwiązać te problemy z wydajnością, można zastosować kilka podejść:

Pomiar problemu: Aby dokładnie zmierzyć wydajność narzędzia do przechwytywania pakietów, należy zrozumieć wzorce ruchu sieciowego i natężenie ruchu, które narzędzie ma obsługiwać. Można użyć narzędzi do monitorowania sieci, aby zmierzyć ruch wsieci i określić liczbę pakietów na sekundę (PPS), które narzędzie musi obsłużyć. Na przykład, za pomocą statystyk programu Wireshark można ustalić średni rozmiar pakietu i liczbę pakietów PPS wysyłanych w sieci. Możesz również użyć opcji „Przechwytywanie | Opcje” w programie Wireshark, aby ustawić filtr przechwytywania, ograniczając liczbę pakietów do przechwycenia i analizy.

Wejście: Aby przechwycić pakiety, narzędzie musi mieć dostęp do ruchu sieciowego. Można to zrobić, podłączając narzędzie do interfejsu sieciowego w systemie przechwytywania lub używając interfejsu sieciowego (TAP) lub portu Span, aby dostarczyć kopię ruchu do narzędzia.

Uwaga: Odczep sieciowy, często nazywany „odczepem” lub „odczepem sieciowym”, to urządzenie sprzętowe służące do przechwytywania ruchu sieciowego poprzez monitorowanie danych przepływających między urządzeniami sieciowymi. Odbywa się to poprzez fizyczne przechwytywanie i kopiowanie danych z łącza sieciowego oraz wysyłanie ich do narzędzi monitorujących lub

analitycznych. Odczepy sieciowe są powszechnie używane do rozwiązywania problemów sieciowych, monitorowania, analizy bezpieczeństwa i optymalizacji wydajności. Zapewniają one przechwytywanie ruchu sieciowego bez wpływu na przepływ lub integralność danych. Port SPAN, znany również jako „port lustrzany" lub „port monitora", to funkcja powszechnie spotykana w przełącznikach sieciowych. Umożliwia ona administratorom sieci skonfigurowanie określonego portu przełącznika w celu duplikowania ruchu przechodzącego przez inne porty. Ten lustrzany ruch może być następnie wysyłany do urządzenia monitorującego lub narzędzia analitycznego w różnych celach, w tym do monitorowania sieci, analizy ruchu i oceny bezpieczeństwa. Porty SPAN to programowa metoda przechwytywania ruchu sieciowego w zakresie możliwości przełącznika.

Na przykład, możesz podłączyć port sieciowy (tap) lub port rozszerzeń (span) do przełącznika lub routera w swojej sieci, aby dostarczyć kopię ruchu do programu Wireshark. Zamiast przechwytywać ruch bezpośrednio z interfejsu sieciowego w systemie przechwytywania, możesz użyć portu sieciowego (tap) lub portu rozszerzeń (span), aby dostarczyć kopię ruchu do programu Wireshark. Może to pomóc w poprawie wydajności poprzez zmniejszenie obciążenia systemu przechwytywania.

Filtrowanie: Aby poprawić wydajność, ważne jest filtrowanie przechwytywanych pakietów, tak aby uwzględniały tylko te, które są potrzebne do analizy. Można to zrobić za pomocą filtrów, takich jak Berkeley Packet Filter (BPF), lub za pomocą specjalistycznego oprogramowania z wbudowanymi funkcjami filtrowania.

Na przykład, możesz użyć wbudowanych funkcji filtrowania Wiresharka, aby filtrować pakiety na podstawie określonych kryteriów, takich jak źródłowy lub docelowy adres IP, numer portu lub protokół. Możesz również użyć opcji „Przechwytywanie | Opcje" w Wireshark, aby ustawić filtr przechwytywania, aby ograniczyć liczbę pakietów do przechwycenia i analizy.

BPF, filtr pakietów Berkeley: BPF to zaawansowany mechanizm filtrowania, który umożliwia filtrowanie pakietów na podstawie określonych kryteriów, takich jak źródłowy lub docelowy adres IP, numer portu lub protokół. Może to pomóc zmniejszyć liczbę pakietów, które należy przechwycić i przetworzyć, poprawiając wydajność. Na przykład, możesz użyć wbudowanych funkcji filtrowania Wiresharka, aby filtrować pakiety na podstawie określonych kryteriów, takich jak źródłowy lub docelowy adres IP, numer portu lub protokół. Możesz również użyć opcji „Przechwytywanie | Opcje" w Wireshark, aby ustawić filtr przechwytywania, aby ograniczyć liczbę pakietów do przechwycenia i analizy.

Przechwytywanie częściowych pakietów danych: Przechwytując tylko nagłówki pakietów lub tylko dane, można zmniejszyć ilość danych, które trzeba przechowywać i przetwarzać. Można to zrobić za pomocą specjalistycznego oprogramowania, które pozwala przechwycić tylko potrzebne fragmenty pakietu, lub stosując filtry wykluczające zbędne dane. Na przykład, można użyć wbudowanych funkcji filtrowania Wiresharka, aby wykluczyć pakiety zawierające zbędne dane, takie jak ruch DNS. Można również użyć opcji „Przechwytywanie | Opcje" w Wireshark, aby ustawić filtr przechwytywania, ograniczając liczbę pakietów do przechwycenia i analizy.

Wyłącz rozpoznawanie nazw DNS: Jednym ze sposobów zmniejszenia obciążenia systemu przechwytywania jest wyłączenie rozpoznawania nazw hostów na adresy IP. Można to zrobić za pomocą specjalistycznego oprogramowania, które umożliwia wyłączenie tej funkcji, lub stosując filtry wykluczające ruch DNS. Na przykład, możesz użyć opcji „Edycja | Preferencje | Rozpoznawanie nazw" w programie Wireshark, aby wyłączyć rozpoznawanie nazw hostów na adresy IP. Możesz również użyć opcji „Przechwytywanie | Opcje" w programie Wireshark, aby ustawić filtr przechwytywania, ograniczając liczbę pakietów do przechwycenia i analizy.

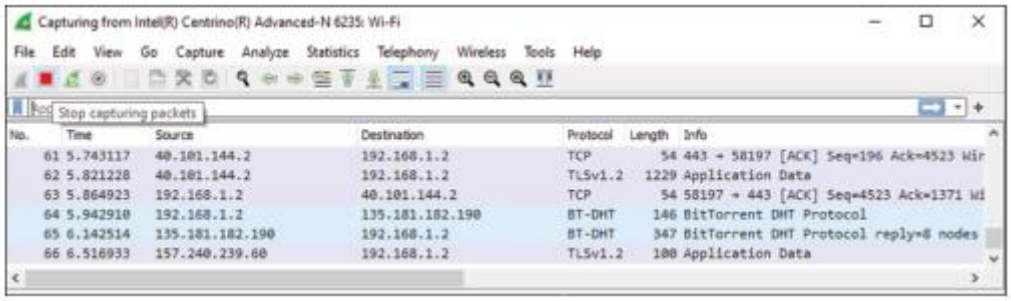
Wdrażając te techniki, można zmniejszyć obciążenie systemu przechwytywania i poprawić wydajność programu Wireshark podczas przechwytywania pakietów. Należy pamiętać, że konkretna implementacja będzie zależeć od wzorców ruchu sieciowego, natężenia ruchu i używanego narzędzia do przechwytywania.

Zatrzymaj przechwytywanie, zapisywanie i eksportowanie pakietów

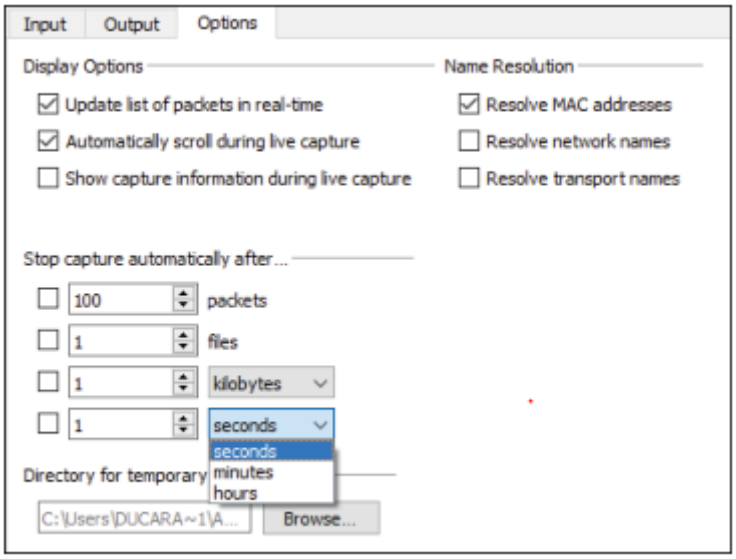
W programie Wireshark można zatrzymać przechwytywanie, zapisywanie i eksportowanie pakietów, korzystając z następujących metod:

Zatrzymaj przechwytywanie

Po rozpoczęciu przechwytywania w programie Wireshark pakiety są przechwytywane i wyświetlane w czasie rzeczywistym. Aby zatrzymać przechwytywanie pakietów, można kliknąć menu „Przechwytywanie” u góry ekranu i wybrać opcję „Zatrzymaj” lub nacisnąć przycisk „Zatrzymaj” na pasku narzędzi programu Wireshark, jak pokazano na rysunku 23.



Spowoduje to zatrzymanie procesu przechwytywania i dalsze przechwytywanie pakietów nie będzie możliwe. Pakiety, które zostały już przechwycone, pozostaną widoczne w programie Wireshark, umożliwiając dalszą analizę. W Wireshark można również ustawić zatrzymanie przechwytywania po określonej liczbie pakietów lub po upływie określonego czasu. Aby to zrobić, przejdź do menu „Przechwytywanie” i wybierz „Opcje”. W oknie dialogowym „Opcje przechwytywania” opcję „Zatrzymaj przechwytywanie” można ustawić na „Po N pakietach” lub „Po N minutach”. Można wprowadzić liczbę pakietów lub minut, przez które przechwytywanie ma się odbywać, jak pokazano na rysunku 24:



Po zatrzymaniu przechwytywania Wireshark wyświetli monit o zapisanie pliku przechwytywania do późniejszego obejrzenia. Następnie możesz wybrać lokalizację zapisu pliku i kliknąć Zapisz, aby zapisać przechwytywanie.

Pamiętaj, że ustawienie warunku zatrzymania przechwytywania to dobry sposób na uniknięcie przechwytywania zbyt dużej ilości danych, co może być przydatne, jeśli interesuje Cię tylko określona część ruchu. Alternatywnie, możesz również użyć skrótu klawiaturowego Ctrl+E, aby zatrzymać proces przechwytywania.

Zapisywanie przechwyconych pakietów danych

Po przechwyceniu pakietów możesz je zapisać do pliku. Przejdź do menu Plik i wybierz opcję Zapisz jako, aby zapisać pakiety w różnych formatach, takich jak PCAP, CSV lub tekstowy. Możesz również automatycznie zapisywać pakiety, zaznaczając opcję „Automatyczne przewijanie podczas przechwytywania na żywo" w oknie dialogowym Opcje przechwytywania. Spowoduje to automatyczne zapisanie pakietów w pliku tymczasowym. Zostanie on zapisany w domyślnej lokalizacji ustawionej w preferencjach Wiresharka.

Należy pamiętać, że zapisanie pakietów w pliku spowoduje zapisanie wszystkich pakietów przechwyconych do tego momentu. Upewnij się również, że plik przechwytywania został zapisany pod odpowiednią nazwą i w odpowiedniej lokalizacji, aby można go było łatwo później znaleźć. Ogólnie rzecz biorąc, zapisywanie pakietów w programie Wireshark pozwala zachować przechwycone pakiety do dalszej analizy lub udostępnienia innym osobom.

Eksportowanie pakietów

Eksportowanie pakietów w programie Wireshark umożliwia zapisanie podzbioru przechwyconych pakietów w innym formacie pliku w celu dalszej analizy lub udostępnienia innym.

1. Po przechwyceniu pakietów możesz wybrać pakiety, które chcesz wyeksportować, klikając je w oknie programu Wireshark. Możesz zaznaczyć wiele pakietów, przytrzymując klawisz Ctrl podczas klikania. Przejdź do menu Plik i wybierz opcję Eksportuj określone pakiety. Spowoduje to otwarcie okna dialogowego Eksportuj określone pakiety, w którym możesz wybrać format pliku, do którego chcesz wyeksportować pakiety (np. PCAP, CSV lub tekstowy), oraz lokalizację zapisu pliku.

2. Po wybraniu formatu pliku i lokalizacji kliknij przycisk Zapisz, aby wyeksportować wybrane pakiety. Wyeksportowane pakiety zostaną zapisane w określonym formacie i lokalizacji. Dodatkowo, możesz również skorzystać z opcji „Plik | Eksportuj podziały pakietów", aby wyeksportować pakiety w różnych formatach, takich jak zwykły tekst, PSML, PS, PDF i CSV. Ta opcja umożliwia eksportowanie analiz pakietów w bardziej ustrukturyzowanym formacie, co może być przydatne do udostępniania szczegółów pakietów innym osobom. Eksportowanie pakietów w Wireshark to przydatna funkcja, ponieważ pozwala zapisać podzbiór przechwyconych pakietów w innym formacie pliku, co może być przydatne do dalszej analizy lub udostępniania innym osobom. Dodatkowo, pozwala zachować oryginalny plik przechwycony w stanie nienaruszonym i udostępniać wyeksportowane pakiety innym osobom bez konieczności udostępniania całego pliku przechwyconego.

Wyzwania/ograniczenia przechwytywania pakietów

Przechwytywanie pakietów to cenna technika analizy, monitorowania i rozwiązywania problemów sieciowych, ale wiąże się z nią szereg wyzwań i ograniczeń. Oto niektóre z kluczowych wyzwań i ograniczeń przechwytywania pakietów:

Obawy o prywatność: Przechwytywanie i analiza pakietów może potencjalnie ujawnić poufne lub prywatne informacje, co budzi obawy o prywatność. Prawidłowe przetwarzanie danych i środki bezpieczeństwa są niezbędne, aby złagodzić te problemy.

Kwestie prawne i etyczne: Przechwytywanie pakietów sieciowych bez odpowiedniego upoważnienia może być nielegalne i nieetyczne. Kluczowe jest uzyskanie zgody lub działanie w ramach prawnych, takich jak odpowiednie przepisy o ochronie danych.

Duża ilość danych: Sieci generują ogromne ilości danych, a przechwytywanie i przechowywanie wszystkich pakietów może być przytłaczające. Obsługa dużych ilości danych wymaga znacznych zasobów pamięci masowej i przetwarzania.

Wymagania dotyczące pamięci masowej: Przechwytywanie pakietów szybko zużywa miejsce na dysku. Może to być kosztowne i wymaga efektywnych strategii przechowywania i archiwizacji danych.

Wpływ na wydajność: Ciągłe przechwytywanie pakietów może wpływać na wydajność sieci, szczególnie w sieciach o dużym natężeniu ruchu. Niewłaściwe zarządzanie może prowadzić do utraty pakietów lub opóźnień.

Filtrowanie pakietów: Filtrowanie pakietów w celu skupienia się na konkretnym ruchu, który nas interesuje, jest niezbędne. Jednak skonfigurowanie dokładnych filtrów może być trudne, a nieprawidłowe filtrowanie może skutkować utratą kluczowych danych.

Wrażliwość na czas: Analiza ruchu w czasie rzeczywistym wymaga specjalistycznych narzędzi i metod. Opóźniona analiza może spowodować pominięcie ważnych zdarzeń.

Ruch szyfrowany: Szyfrowanie, takie jak TLS/SSL, może uniemożliwić przechwytywanie i analizę zawartości pakietów. Chociaż można przechwytywać zaszyfrowane pakiety, odszyfrowanie ich zawartości może być trudne.

Utrata pakietów: W sieciach o dużym natężeniu ruchu lub w okresach dużego ruchu pakiety mogą zostać utracone lub nie zostać przechwycone w całości. Może to wpłynąć na kompletność przechwytywania pakietów.

Złożoność dekodowania: Interpretacja surowych danych pakietowych często wymaga wiedzy z zakresu protokołów sieciowych i narzędzi do analizy pakietów, co może stanowić barierę dla niektórych użytkowników.

Obciążenie i wykorzystanie zasobów: Narzędzia do przechwytywania pakietów wymagają zasobów systemowych, takich jak procesor i pamięć, co może wpływać na wydajność urządzenia przechwytującego.

Segmentacja sieci: W sieciach segmentowanych przechwytywanie całego ruchu we wszystkich segmentach może być trudne. Do przechwytywania ruchu z różnych segmentów sieci mogą być wymagane specjalne konfiguracje.

Aby sprostać tym wyzwaniom i ograniczeniom, często konieczne jest połączenie technologii, najlepszych praktyk i wiedzy specjalistycznej w celu zapewnienia skutecznego i etycznego przechwytywania i analizy pakietów.

Podsumowanie

Podsumowując, skuteczne podsłuchiwanie pakietów sieciowych wymaga jasnego zrozumienia, co chcemy przechwycić, a także odpowiednich narzędzi i technik. Wybierając konkretny interfejs sieciowy

lub wiele interfejsów, można skupić się na interesującym ruchu i odfiltrować niepotrzebne pakiety. Przeprowadzanie podsłuchiwania pakietów, zarówno w sieci lokalnej, jak i zdalnej, pozwala na przechwytywanie i analizowanie pakietów w czasie rzeczywistym, a korzystanie z filtrów wyświetlania i przechwytywania pozwala skupić się na konkretnych interesujących pakietach. Maksymalizacja wydajności przechwytywania pakietów poprzez zastosowanie wydajnych kart sieciowych, filtrów i wydajnych systemów pamięci masowej ma kluczowe znaczenie dla skutecznej analizy i rozwiązywania problemów. Wiedza o tym, jak zatrzymać podsłuchiwanie, zapisywanie i eksportowanie pakietów w programie Wireshark, jest również ważna dla efektywnego zarządzania przechwyconymi pakietami i przechowywania ich do dalszej analizy lub udostępniania innym. Ogólnie rzecz biorąc, dzięki zrozumieniu i wdrożeniu tych technik można skutecznie podsłuchiwać pakiety sieciowe i analizować je w celu rozwiązywania problemów sieciowych.

Pytania

1. Jaki jest cel filtrów przechwytywania w podsłuchiwaniu pakietów?

a) Aby wybrać konkretny interfejs sieciowy lub wiele interfejsów

b) Aby przechwytywać określone typy pakietów

c) Aby zmaksymalizować wydajność przechwytywania pakietów

d) Aby zatrzymać podsłuchiwanie, zapisywanie i eksportowanie pakietów

2. Co należy wiedzieć przed rozpoczęciem sesji podsłuchiwania pakietów?

a) Jaki interfejs sieciowy należy użyć

b) Jaki typ pakietów przechwytywać

c) Jaka jest lokalizacja urządzenia docelowego

d) Wszystkie powyższe

3. Jaki jest cel stosowania filtrów wyświetlania w podsłuchiwaniu pakietów?

a) Aby ograniczyć liczbę/rodzaj wyświetlanych pakietów

b) Aby zwiększyć liczbę/rodzaj przechwytywanych pakietów

c) Aby zaszyfrować pakiety

d) Aby zmienić format pakietów

4. Jak można poprawić wydajność sesji podsłuchiwania pakietów? a) Użyj szybkiego interfejsu sieciowego

b) Przechwyć tylko niezbędne pakiety

c) Użyj filtra wyświetlania

d) Wszystkie powyższe

5. Czy możesz podsłuchiwać pakiety sieciowe ze zdalnych lokalizacji?

a) Tak, jeśli masz dostęp do routera lub bramy sieciowej.

b) Tak, jeśli używasz narzędzia takiego jak Wireshark lub tcpdump.

c) Nie, możesz podsłuchiwać pakiety tylko z własnego interfejsu sieciowego.

d) Nie, potrzebujesz fizycznego dostępu do kabla sieciowego lub urządzenia.

6. Jaka jest główna funkcja opcji „-i” w interfejsie wiersza poleceń Wiresharka?

a) Aby wybrać konkretny interfejs sieciowy lub wiele interfejsów do przechwytywania pakietów

b) Aby określić filtr przechwytywania pakietów

c) Aby określić filtr wyświetlania do analizy pakietów

d) Aby zapisać przechwycone pakiety do określonego pliku

7. Dlaczego ważne jest, aby wiedzieć, co chcesz podsłuchiwać przed rozpoczęciem sesji podsłuchiwania pakietów? a) Aby ograniczyć ilość przechwytywanego ruchu sieciowego

b) Aby zapewnić przechwytywanie właściwych pakietów

c) Aby poprawić wydajność sesji podsłuchu pakietów

d) Wszystkie powyższe

8. Jaka jest główna funkcja opcji „-w” w interfejsie wiersza poleceń programu Wireshark?

a) Aby wybrać konkretny interfejs sieciowy lub wiele interfejsów do przechwytywania pakietów

b) Aby określić filtr przechwytywania pakietów

c) Aby określić filtr wyświetlania do analizy pakietów

d) Aby zapisać przechwycone pakiety do określonego pliku

9. Jaka jest główna funkcja opcji „-R” w interfejsie wiersza poleceń programu Wireshark?

a) Aby wybrać konkretny interfejs sieciowy lub wiele interfejsów do przechwytywania pakietów

b) Aby określić filtr przechwytywania pakietów

c) Aby określić filtr wyświetlania do analizy pakietów

d) Aby zapisać przechwycone pakiety do określonego pliku

10. Jaka jest główna funkcja opcji „-f” w interfejsie wiersza poleceń programu Wireshark? a) Aby wybrać konkretny interfejs sieciowy lub wiele interfejsów do przechwytywania pakietów

b) Aby określić filtr przechwytywania pakietów

c) Aby określić filtr wyświetlania do analizy pakietów

d) Aby zapisać przechwycone pakiety do określonego pliku

Odpowiedzi

1. b

2. d

3. a

4. d

5. a

6. a

7. d

8. d

9. c

10. b