Podstawy analizy ruchu sieciowego, protokoły DNS, HTTP i numery portów

Eksploatacja Lokalnych Sieci Komputerowych

Cele zajęć

1. Zaznajomienie się z narzędziem Wireshark oraz podstawowymi funkcjami.
2. Analiza ruchu sieciowego związanego z zapytaniami DNS oraz HTTP.
3. Rozpoznawanie i interpretowanie numerów portów w ruchu sieciowym.
4. Tworzenie raportu z analizy ruchu sieciowego

Analiza zapytań DNS

DNS (Domain Name System) to kluczowy element internetu, który zamienia nazwy domen (np. www.example.com) na odpowiadające im adresy IP. Pozwala to użytkownikom na korzystanie z łatwych do zapamiętania nazw stron internetowych. Zadanie polega na prześledzeniu procesu wysłania zapytania DNS, wykonywanego w momencie gdy użytkownik próbuje odwiedzić stronę internetową, a także odpowiedzi serwera DNS.

1. Uruchom Wireshark i rozpocznij przechwytywanie ruchu.
2. Otwórz przeglądarkę internetową i wpisz adres dowolnej strony (np. www.google.com).
3. Zatrzymaj przechwytywanie ruchu po załadowaniu strony
4. Ustaw filtra na „DNS" w Wiresharku i znajdź zapytanie do serwera DNS oraz jego odpowiedź.
5. Wyświetl szczegóły zapytania DNS, zwróć uwagę na numer portu (53), typ zapytania (np. A – adres IPv4).
6. Wykonaj zrzut ekranu zapytania oraz odpowiedzi DNS, zaznacz numer portu oraz typ zapytania, a także zwrócony adres IP.

Analiza protokołu HTTP

HTTP (Hypertext Transfer Protocol) jest protokołem komunikacyjnym, który umożliwia przeglądarkom internetowym pobieranie stron WWW z serwerów. To fundament działania stron internetowych. W ramach tego zadania przeanalizowany zostanie ruch HTTP, który odbywa się między przeglądarką a serwerem.

1. Uruchom Wireshark i rozpocznij przechwytywanie ruchu.
2. Otwórz przeglądarkę internetową i wejdź na stronę, która używa HTTP (np. http://neverssl.com – strona celowo nie korzystająca z HTTPS).
3. Zatrzymaj przechwytywanie ruchu po załadowaniu strony
4. Użyj filtra HTTP w Wiresharku i znajdź pakiety związane z wysyłaniem i odbieraniem danych HTTP.
5. Zidentyfikuj różne typy zapytań HTTP (np. GET, POST).
6. Pokaż szczegóły zapytania GET, w tym nagłówki (User-Agent, Host, itd.,) i udokumentuj je zrzutem ekranu.
7. Wyjaśnij, dlaczego HTTPS jest bezpieczniejsze od HTTP (SSL/TLS)

* Spróbuj przechwycić zawartość pakietu przesłanego do serwera

Numery portów i ich znaczenie

Porty sieciowe to logiczne kanały komunikacyjne używane do identyfikacji specyficznych procesów lub usług działających na urządzeniach w sieci. Kiedy dane są przesyłane między urządzeniami, porty pomagają określić, która aplikacja lub usługa ma uzyskać otrzymane dane.

Porty dzielą się na **dobrze znane** (0-1023) – wykorzystywane przez popularne protokoły, takie jak HTTP (port 80) czy HTTPS (port 443), **zarejestrowane** (1024-49151) – dla konkretnych aplikacji, oraz **dynamiczne i prywatne** (49152-65535) – używane tymczasowo przez systemy.

1. Przyjrzyj się wcześniejszym przechwyconym pakietom i zidentyfikuj numery portów (filtr tcp.port == 80 lub udp.port == 53)
2. Podaj 5 przykładów portów oraz ich użycia.
3. Wyjaśnij różnicę między portami TCP a UDP.
4. Zrób zrzut ekranu pakietu TCP oraz UDP, wraz z informacją o numerze portu (powtórz przechwytywanie w razie potrzeby).

Przygotuj krótki raport z przeprowadzonych działań. Umieść w nim wykonane zrzuty ekranu wraz z niezbędnymi informacjami dotyczącymi każdego z nich (np. co pokazują, jakie informacje można z nich odczytać, itp.). Pracę zapisz jako plik .pdf i prześlij na adres szkola@davidkasperek.com