|  |
| --- |
| Politechnika Wrocławska, Informatyka Stosowana |
| ATAKI NA KOMUNIKACJĘ |
| Cyberbezpieczeństwo, Laboratorium nr.8 - raport |

|  |
| --- |
| Autor: Aleksander Stepaniuk  Nr. Indeksu: 272644 |

**4. Problemy i pytania**

**Pytanie 1.1;**

Ataki aktywne typu MitM polegają na przechwytywaniu oraz modyfikacji ruchu w czasie rzeczywistym, np. zatruwanie ARP czy modyfikacja pakietów. Pasywne ataki MitM ograniczają się do podsłuchiwania i analizy ruchu bez jego zmiany (np. przechwytywanie wiadomości / pliku wysłanego emailem). Ataki pasywne są znacznie trudniejsze do wykrycia od aktywnych, ponieważ osoba trzecia pozostaje niewidoczna dla obydwu stron komunikacji.

**Pytanie 1.2;**

Można stosować statyczne tablice ARP lub filtrowanie ARP w routerze, co uniemożliwia modyfikację tablic ARP przez atakującego. Alternatywnie, użycie protokołu „DHCP Snooping” oraz dynamicznego ARP Inspection (DAI) w przełącznikach sieciowych znacznie ogranicza ryzyko takich ataków. Warto również dbać o aktualne oprogramowanie antywirusowe oraz zaporę sieciową (firewall), które również mogą wykrywać i blokować niepożądany ruch w sieci.

**Pytanie 1.3;**

DNSSEC zapewnia integralność danych DNS poprzez cyfrowe podpisy i szyfrowanie asymetryczne, co uniemożliwia fałszowanie odpowiedzi DNS. Chroni to użytkowników przed przekierowaniem na fałszywe strony, zmniejszając ryzyko kradzieży danych czy innych ataków (sam DNS nie zawiera żadnych mechanizmów zabezpieczających i każdy użytkownik może uruchomić w sieci własny serwer DNS i przekierować na niego ruch sieciowy.

**Pytanie 1.4;**

Tryb monitorowania pozwala karcie sieciowej przechwytywać wszystkie pakiety w zasięgu danej sieci, niezależnie od tego, czy są one przeznaczone dla danego urządzenia. Używa się go do analizy ruchu, diagnozowania problemów w sieci, wykrywania ataków, a także do przeprowadzania audytów bezpieczeństwa. W połączeniu z narzędziami takimi jak Wireshark, pozwala dokładnie analizować dane przesyłane w sieci, przechwytywać dane uwierzytelniające lub identyfikować podatności. W sieciach bezprzewodowych może służyć do wykrywania nieautoryzowanych urządzeń lub prób przejęcia sesji.

**5. Zadania**

Adresy IP:

* Ubuntu: 192.168.188.34/24
* Kali: 192.168.188.35/24
* Meta: 192.168.188.36/24
* Domyślna brama: 192.168.188.1/24

**Obraz zawierający tekst, zrzut ekranu, oprogramowanie, wyświetlacz

Opis wygenerowany automatycznie**

**Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Czcionka

Opis wygenerowany automatycznie**

**Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie**

**Obraz zawierający tekst, bezkręgowiec, zrzut ekranu, owad

Opis wygenerowany automatycznie**

**Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Oprogramowanie multimedialne

Opis wygenerowany automatycznie**

Obraz zawierający tekst, elektronika, zrzut ekranu, oprogramowanie

Opis wygenerowany automatycznie

Widać, że połączenie jest niezabezpieczone (protokół HTTP zamiast HTTPS) i atak jest skuteczny, bo przeniosło nas na domyślną stronę apache.

**Obraz zawierający tekst, zrzut ekranu, Czcionka, logo

Opis wygenerowany automatycznie**

**Obraz zawierający tekst, zrzut ekranu, Czcionka, oprogramowanie

Opis wygenerowany automatycznie**

**Obraz zawierający tekst, Czcionka, zrzut ekranu

Opis wygenerowany automatycznie**

**Obraz zawierający tekst, zrzut ekranu, oprogramowanie, wyświetlacz

Opis wygenerowany automatycznie**