Sprawozdanie

Bezpieczeństwo sieci komputerowych laboratorium 2.10.2025

*Maciej Myśków 272794*

*Bartosz Gancarek*

# Zadanie 2

Z komputera K nawiązano połączenie z serwerem WWW działającym na komputerze S, wpisując w przeglądarce adres http://192.168.1.1. Następnie z komputera S uruchomiono klienta Telnet, aby połączyć się z routerem o adresie 192.168.0.100. W celu weryfikacji aktywności sieciowej na komputerze S wykonano polecenie **netstat -ano**.

Wynik polecenia netstat pokazał listę portów nasłuchujących oraz aktywnych połączeń. Wśród portów w stanie LISTENING zidentyfikowano kluczowe usługi: serwer FTP na porcie 21, serwer DNS na porcie 53 oraz serwer WWW na porcie 80. W sekcji aktywnych połączeń widoczne były dwie sesje w stanie ESTABLISHED: połączenie z komputera K na serwer WWW S oraz połączenie Telnet z komputera S do routera.

Zaobserwowane stany połączeń TCP potwierdzają poprawną komunikację. Stan **LISTENING** oznacza, że usługa oczekuje na przychodzące połączenia. Stan **ESTABLISHED** wskazuje na aktywne, trwające sesje wymiany danych. Stan **TIME\_WAIT** jest normalnym stanem przejściowym po zamknięciu połączenia, gwarantującym poprawne odebranie wszystkich pakietów.

Obraz zawierający zrzut ekranu, czarne

Zawartość wygenerowana przez AI może być niepoprawna.Obraz zawierający zrzut ekranu, tekst, miejsce parkingowe/przestrzeń

Zawartość wygenerowana przez AI może być niepoprawna.

Obraz zawierający tekst, zrzut ekranu, design

Zawartość wygenerowana przez AI może być niepoprawna.

# Zadanie 4

**Charakterystyka pakietów skanujących**

Wykonano skanowanie portów 0-1000 na serwerze (192.168.1.1) i routerze (192.168.1.100) za pomocą Nmap, wykorzystując metody SYN i Connect. Ruch sieciowy przechwycono w Wireshark.

Pakiety skanujące SYN charakteryzują się wysyłaniem żądań z ustawioną flagą TCP SYN, bez nawiązywania pełnego połączenia. W skanowaniu Connect po odebraniu SYN-ACK wysyłane jest ACK, finalizując handshake, a następnie RST do zerwania połączenia.

**Łatwość rozpoznania pakietów**

Skanowanie jest stosunkowo łatwe do wykrycia. W Wireshark widać serie pakietów SYN z jednego źródła do różnych portów docelowego hosta w krótkim czasie. Po odebraniu SYN-ACK brakuje normalnej wymiany danych, a połączenie jest natychmiast zrywane - ta nietypowa sekwencja zdarzeń jest charakterystyczna dla skanera.

## Server 192.168.1.1

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, wyświetlacz

Zawartość wygenerowana przez AI może być niepoprawna.

## Router 192.168.1.100

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Ikona komputerowa

Zawartość wygenerowana przez AI może być niepoprawna.

## Wireshark

Obraz zawierający tekst, zrzut ekranu, menu, Czcionka

Zawartość wygenerowana przez AI może być niepoprawna.

# Zadanie 5

Na maszynie wirtualnej Windows 7 uruchomiono program Cain i aktywowano funkcję ARP Poison Routing. W tabeli ARP widoczne są prawidłowe adresy MAC hosta 192.168.1.1 (serwer) i 192.168.1.100 (router) przed atakiem.

Po uruchomieniu ataku ARP Poison Routing, tablica ARP została zatruta - program Cain wysyłał sfałszowane pakiety ARP, które przekierowywały ruch sieciowy przez komputer atakującego.

W programie Cain w zakładce/kolumnie "Packets -> " Widać ilość zatrutych pakietów podczas transmisji danych za pomocą nieszyfrowanego protokołu telnet. Potwierdza to skuteczność oprogramowania Cain do zatruwania wpisów ARP w tablicy MAC przełącznika.

**Pakiety wykorzystywane w ataku**

Program Cain generował okresowo wysyłane, sfałszowane pakiety ARP Reply. Każdy taki pakiet zawierał adres IP routera (192.168.1.100) w polu nadawcy, połączony z adresem MAC komputera atakującego.

Sfałszowane pakiety powodowały, że przełącznik aktualizował swoją tablicę ARP, tworząc błędne powiązanie. W efekcie adres IP routera był trwale powiązany z adresem MAC komputera atakującego, a nie prawdziwego routera.

Wszystkie pakiety przeznaczone dla routera, w tym wrażliwe dane z sesji Telnet, były przekierowywane przez komputer atakującego. Umożliwiło to pełny podsłuch komunikacji i przechwycenie loginów oraz haseł.

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, wyświetlacz

Zawartość wygenerowana przez AI może być niepoprawna.

Obraz zawierający tekst, zrzut ekranu, Czcionka, numer

Zawartość wygenerowana przez AI może być niepoprawna.

# Zadanie 6

## Utworzenie kont użytkowników z hasłami

Obraz zawierający tekst, komputer, zrzut ekranu, oprogramowanie

Zawartość wygenerowana przez AI może być niepoprawna.

## Utworzone konta

Obraz zawierający tekst, Czcionka, zrzut ekranu

Zawartość wygenerowana przez AI może być niepoprawna.

## Przygotowanie środowiska wraz z NTML do pracy/łamania haseł

Obraz zawierający tekst, zrzut ekranu, wyświetlacz, oprogramowanie

Zawartość wygenerowana przez AI może być niepoprawna.

Łamanie hasła 3-znakowego

Czas: natychmiast

Obraz zawierający tekst, zrzut ekranu, wyświetlacz, oprogramowanie

Zawartość wygenerowana przez AI może być niepoprawna.

Łamanie hasła 4-znakowego

Czas: natychmiast

Obraz zawierający tekst, elektronika, zrzut ekranu, wyświetlacz

Zawartość wygenerowana przez AI może być niepoprawna.

Łamanie hasła 5-znakowego

Czas: natychmiast

Obraz zawierający tekst, elektronika, wyświetlacz, zrzut ekranu

Zawartość wygenerowana przez AI może być niepoprawna.

Łamanie hasła 6-znakowego

Czas: natychmiast

Obraz zawierający tekst, elektronika, zrzut ekranu, oprogramowanie

Zawartość wygenerowana przez AI może być niepoprawna.

Łamanie hasła 7-znakowego

Czas: 6,5 min

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, wyświetlacz

Zawartość wygenerowana przez AI może być niepoprawna.

Podsumowanie

|  |  |
| --- | --- |
| Długość hasła [znaki] | Czas |
| 3 | >1s - natychmiast |
| 4 | >1s - natychmiast |
| 5 | >1s - natychmiast |
| 6 | >1s - natychmiast |
| 7 | 6,5 min |