AKADEMIA HANDLOWA NAUK STOSOWANYCH W RADOMIU

RADOM ACADEMY OF ECONOMICS

INSTRUKCJA LABORATORYJNA NUMER 1	
Przedmiot: Zagrożenia bezpieczeństwa systemów	Tok: 2024/2025
Cel praktyczny zajęć: Rozpoznawanie systemów operacyjnych na podstawie ruchu sieciowego.	

1. Scenariusz ćwiczenia

Celem ćwiczenia jest zapoznanie ze sposobem rozpoznawania systemów na podstawie ruchu sieciowego.

Zainstaluj środowisko Wireshark, możesz go pobrać ze strony:
https://www.wireshark.org/download.html

Uruchom nasłuch pakietów wysyłanych do internetu lub sieci lokalnej, znajdź i wybierz trzy pakiety do analizy (np.: TCP i UDP oraz jeden dowolny). Zapoznaj się z przeznaczeniem wybranych pakietów oraz z tym z czego się składają.

- Opisz pakiety na wybranych przykładach, przeanalizuj nagłówek, zdekoduj wszystkie informacje w nim zawarte.
- Wypisz informacje o sieci, które uda Ci się odczytać.
- Odczytaj informacje zapisane w formacie hex.
- Czy udało się znaleźć informacje o typie źródłowego lub docelowego systemu operacyjnego?

UDP

1. Z wykorzystaniem, jakich numerów portów przebiega komunikacja, (jaki jest numer odbiorcy a jaki nadawcy)?

2. Jaki jest rozmiar datagramu?

3. Jaki jest rozmiar pola danych przez datagram?

4. Czy została policzona suma kontrolna, jeśli tak, jaka ma wartość i czy jest ona prawidłowa?

5. Czy jesteśmy w stanie zweryfikować, jaką wiadomość przesyła datagram?

6. Czy TTL oraz wielkość ramki pokrywa się z założeniami dla Twojego systemu?

TCP

1. Z wykorzystaniem, jakich numerów portów przebiega komunikacja, (jaki jest numer odbiorcy a jaki nadawcy)?

2. Jakiego typu jest to wiadomość, czy jest to wiadomość typu potwierdzenie, czy przenosi dane, czy informacje na temat przebiegu transmisji?

3. Jaki jest rozmiar segmentu?

4. Jaki jest rozmiar pola danych przez segment?

5. Czy została policzona suma kontrolna, jeśli tak, jaka ma wartość i czy jest ona prawidłowa?

6. Jaka jest maksymalna wartość przesyłanego segmentu bez potwierdzenia ACK ze strony odbiorcy?

7. Czy wiadomość została wysłana z większym priorytetem?

8. Na podstawie odebranego segmentu wskazać stan, w jakim jest transmisja?

9. Czy TTL oraz wielkość ramki pokrywa się z założeniami dla Twojego systemu?

Po zakończonej pracy nie zapomnij przesłać wybranych pakietów oraz odpowiedzi!