WYŻSZA SZKOŁA HANDLOWA W RADOMIU

RADOM ACADEMY OF ECONOMICS

Wyższa Szkoła Handlowa w Radomiu

Podstawy kryptografii
Laboratorium 2

Radom 2020/2021

1. Cel zadania

Zadanie polegać będzie na przetestowaniu działania tuneli sieciowych z wykorzystaniem technologii VPN

2. Potrzebne narzędzia.

- Wireshark
- Virtualbox z systemem Linux lub Windows
- dostęp do sieci
- opcjonalnie system Linux Kali lub blackarch (https://blackarch.org, https://www.kali.org)

3. Informacje wstępne

Coraz powszechniejszą praktyką jest praca zdalna. Wielu pracowników musi wykonywać pracę poza biurem (np. kontrole w terenie), mają pile wyjazdy służbowe bądź zostali zmuszeni do pracy w domu (np. obecna sytuacja epidemiologiczna). Administratorzy IT chcąc zapewnić wspomnianym użytkownikom dostęp do zasobów firmowych i/lub usług dostępnych wyłącznie na łączu służbowym (jak dostęp do danych wrażliwych, rozliczeń firmowych, części monitoringu itp.) tworzą w sieci firmowej serwery połączeń zdalnych do wirtualnej sieci prywatnej (VPN).

Praca z taką siecią musi mieć zapewnione bezpieczeństwo przesyłu danych. W przypadku jakichkolwiek lub w zabezpieczeniach atakujący mógłby się bowiem dostać do sieci wewnętrznej firmy, a to początek do włamania i potężnych szkód od strony atakującego.

Dlatego też każde z połączeń musi zostać odpowiednio zabezpieczone przy wykorzystaniu wszelkich dostępnych w danej technologii środków. Przebieg ćwiczenia ma na celu uświadomienie, które z połączeń jest najbezpieczniejsze i która technologia daje najlepszą ochronę przy jednoczesnej prostocie konfiguracji.

4. Przebieg.

Praca powinna być wykonywana w parach. Na jednym z komputerów powinien być uruchomiony program Wireshark. Należy śledzić nim działania komputera atakowanego (drugiej osoby).

Początkowo należy ustawić tunel bez zabezpieczeń. Połączeniem tego typu jest tunel PPTP. Następnie na drugim komputerze trzeba wykonać operację logowania do sieci. Jednocześnie w tym samym momencie należy sprawdzić logi Wiresharka – w nich powinny pojawić się pakiety z loginem i hasłem użytkownika. Oznacza to, że protokół ten nie jest bezpieczny.

Następnie należy zainstalować i skonfigurować protokół OpenVPN. W jego ustawieniach należy wybrać maksymalną ochronę, tj. każdy z użytkowników powinien posiadać własne klucze autoryzacyjne (z certyfikatem), zaś transmisja powinna być chroniona kierunkowym kluczem TLS. Należy ponownie sprawdzić programem Wireshark jak będzie wyglądać proces logowania się do sieci poprzez OpenVPN

Ćwiczenie można powtórzyć (opcjonalnie) dla innych protokołów (np. L2TP, SSTP).

5. Zakończenie

Z przebiegu laboratorium należy sporządzić sprawozdanie. Należy porównać sprawdzone technologie połączeniowe oraz sporządzić notatkę o zabezpieczeniach OpenVPN (generowanych kluczach, podpisać oraz szyfrowaniu połączenia). Ponadto należy porównać poziom skomplikowania konfiguracji OpenVPN z innymi systemami tunelowania (można posłużyć się danymi z portali traktujących o bezpieczeństwie VPN).