Bezpieczeństwo systemów informatycznych

SPRAWOZDANIE Z ĆWICZENIA: SSH

Imię Nazwisko: ..... nr albumu: .....

data ćwiczenia: ..... godzina: .....

Aby wykonać poniższe ćwiczenia uruchom system operacyjny VM Linux

Zapisz nazwę domenową swojego komputera i jego adres IP:

1. Secure Shell i protokół SSH

1.1 Protokół SSH

1. Wymień algorytmy kryptograficzne stosowane w protokole SSH do uwierzytelniania stron komunikacji:

1.2 Program ssh

2. Zaloguj się przy pomocy programu ssh na swoje konto w systemie sąsiedniego komputera. Po pomyślnym logowaniu wróć każdorazowo do lokalnego systemu (wyloguj się).

3. Obejrzyj klucze publiczne zdalnych systemów pozyskane w czasie nawiązywania komunikacji SSH. Gdzie te klucze się znajdują?

Na które prawa dostępu do tego pliku należy zwrócić uwagę?

Dlaczego?

4. Wykonaj zdalne polecenie wyświetlające plik `/etc/HOSTNAME` z sąsiedniego systemu. Jaką postać ma komenda ssh wydana w tym celu lokalnie:

5. Skopiuj w/w plik do swojego katalogu zmieniając nazwę pliku. Zapisz polecenie:

6. Zweryfikuj wymianę komunikatów w protokole SSH widoczną przy nawiązywaniu połączenia, uruchamiając klienta ssh w trybie *verbose* (opcja -v). Wymień, jakie są dopuszczalne metody uwierzytelniania użytkownika dla zaobserwowane sesji (podaj co te metody oznaczają):

1.3 Zarządzanie kluczami kryptograficznymi

7. Wygeneruj swoją parę kluczy asymetrycznych do uwierzytelniania metodą ECDSA. Przyjmij domyślne lokalizacje plików z kluczami. Wyjątkowo na potrzeby ćwiczeń nie skorzystaj z ochrony pliku z kluczem prywatnym na hasło (*passphrase*).

8. Skonfiguruj dostęp do swojego konta w sąsiednim systemie, tak aby uwierzytelnianie odbywało się kryptograficznie.
   – jakie polecenie wykonałeś(-aś) aby osiągnąć efekt?
   – sprawdź czy efekt jest osiągnięty również dla polecenia scp.

9. Skopiuj klucz prywatny do pliku `~/.ssh/gate_key`. Dla oryginalnego pliku z kluczem prywatnym ustaw hasło ochrony (*passphrase*). Sprawdź efekt w połączeniu SSH z sąsiednim komputerem.

10. W pliku `~/.ssh/config` ustaw własne parametry konfiguracyjne dla połączenia z sąsiednim komputerem, zmieniając nazwę pliku z kluczem na `~/.ssh/gate_key`. Sprawdź efekt.

1.4 Tunele wirtualne warstwy aplikacji (TCP port forwarding)

11. Przygotuj się do ustawienia tunelu kryptograficznego do propagowania lokalnych połączeń wg parametrów podanych przez prowadzącego:

lokalny port	
zdalna brama	
docelowy serwer	
docelowy port	

   – jakim poleceniem należy uaktywnić tunelowanie?

– jak zweryfikować czy tunelowanie działa jak powinno?

12. Zezwól na tunelowanie dowolnego połączenia ze swojej sieci lokalnej na twój lokalny port 8080 do wskazanego serwera www. Zapisz polecenie utworzenia tunelu:

13. Ustaw tunelowanie typu `DynamicForward` i zweryfikuj jego działanie na stronie http://showip.net. Zapisz jaki adres IP klienta podaje w/w strona:

14. Stwórz plik konfiguracyjny, w którym zapiszesz profile dla ćwiczeń 12 i 13. Przedstaw zawartość stworzonego profilu:

15. Stwórz profil (lub profile) w pliku konfiguracyjnym, który umożliwi połączenie się z sąsiednim komputerem poprzez 2 inne (twój → komp1 → komp2 → sąsiedni) jednym poleceniem ssh. Przedstaw konfigurację: