Bezpieczeństwo systemów informatycznych

SPRAWOZDANIE Z ĆWICZENIA: SSH

Imię Nazwisko: Dariusz Max Adamski nr albumu: 136674

data ćwiczenia: 22.12.2020 godzina: 15:10

Aby wykonać poniższe ćwiczenia uruchom swój lokalny lub wirtualny system operacyjny Linux.

Zapisz swój publiczny adres IP widoczny na zewnątrz (→ http://showip.net):

185.225.102.117

1. Secure Shell i protokół SSH

1.1 Protokół SSH

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

RSA, (EC)DSA, Diffie-Hellman

1.2 Program ssh

2. Zaloguj się przy pomocy programu ssh na swoje konto studenckie w zdalnym systemie unixlab.cs.put.poznan.pl. Po pomyślnym logowaniu wróć każdorazowo do lokalnego systemu (wyloguj się). Obejrzyj klucze publiczne zdalnych systemów pozyskane w czasie nawiązywania komunikacji SSH. Gdzie te klucze się znajdują?

~/.ssh/known_hosts

Na które prawa dostępu do tego pliku należy zwrócić uwagę by zapewnić poprawne (bezpieczne) uwierzytelniania zdalnych systemów?

Tylko wlasciciel pliku powinien miec prawo zapisu. Ogolnie uprawnienia powinny byc 644.

3. Wykonaj w zdalnym systemie polecenie wyświetlające plik `/etc/HOSTNAME`. Jakie polecenie należy w tym celu wydać lokalnie:

ssh inf136674@unixlab.cs.put.poznan.pl cat /etc/hostname

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

```
scp inf136674@unixlab.cs.put.poznan.pl:/etc/hostname unixlab-hostname
```

5. 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):

```
publickey - uwierzytelnianie asymetryczna kryptografia RSA/(EC)DSA
password - uwierzytelninianie przez haslo systemowe (szyfrowana transmisja)
keyboard-interactive - interfejs do metod uwierzytelniania korzystajacych z klawiatury
```

1.3 Zarządzanie kluczami kryptograficznymi

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

7. Skonfiguruj dostęp do swojego konta w zdalnym systemie, tak aby uwierzytelnianie odbywało się kryptograficznie.
   – jakie polecenie wykonałeś(-aś) aby osiągnąć efekt?

```
scp ~/.ssh/id_ecdsa.pub inf136674@unixlab.cs.put.poznan.pl:~/.ssh/authorized_keys
```

   – sprawdź czy efekt jest osiągnięty również dla polecenia scp.

8. Skopiuj klucz prywatny do pliku `~/.ssh/gate_key`. Dla oryginalnego pliku z kluczem prywatnym ustaw hasło ochrony (*passphrase*). Następnie w pliku `~/.ssh/config` ustaw własne parametry konfiguracyjne dla połączenia z serwerem unixlab, zmieniając nazwę pliku z kluczem na `~/.ssh/gate_key`.

   Sprawdź efekt w połączeniu SSH z serwerem.

1.4 Tunele wirtualne warstwy aplikacji (TCP port forwarding)

9. Przygotuj się do ustawienia tunelu kryptograficznego do propagowania lokalnych połączeń wg poniższych parametrów:

lokalny port	8080
zdalna brama	unixlab.cs.put.poznan.pl
docelowy serwer	www
docelowy port	80

   – jakim poleceniem należy uaktywnić tunelowanie?

```
ssh -L 8080:www.example.com:80 inf136674@unixlab.cs.put.poznan.pl
```

   – jak zweryfikować czy tunelowanie działa jak powinno?

```
Np. wykonac komende: curl -H "Host: www.example.com" -L localhost:8080
Powinien byc zwrocony kod html tej strony
```

10. Ustaw tunelowanie typu `DynamicForward` i zweryfikuj jego działania na stronie http://showip.net. Jaki adres IP klienta podaje w/w strona:

150.254.30.38

11. Stwórz plik konfiguracyjny, w którym zapiszesz profile dla obu powyższych ćwiczeń. Przedstaw zawartość tych profili:

```
Host example_put
  HostName unixlab.cs.put.poznan.pl
  User inf136674
  IdentityFile ~/.ssh/id_ecdsa.pub
  LocalForward 8080 www.example.com:80

Host proxy_put
  HostName unixlab.cs.put.poznan.pl
  User inf136674
  IdentityFile ~/.ssh/id_ecdsa.pub
  DynamicForward 8080
```