Autentykacja użytkownika przy pomocy klucza w protokole SSH

Paweł Topa

18 marca 2025

Protokół SSH (Secured Shell) jest jednym z najważniejszych narzędzi pracy administratora umożliwiających zdalne połączenia się z odległym systemem i wykonywanie na nim pracy. Protokół SSH jest podstawą wielu narzędzie umożliwiających wymianę danych np. kopiowanie plików (SCP, SSH), realizacja protokołu X11 umożliwiającego uruchamianie programów graficznych.

W systemach typ Unix oraz MacOS klient i serwer SSH jest standardem. W systemach typu Windows również jest możliwe korzystanie z tego protokołu.

Logowanie się do zdalnego systemu przy pomocy hasła może być kłopotliwe zwłaszcza obecnie. Powszechną praktyką jest kradzież haseł z różnych serwisów, które następnie wykorzystywane do prób zalogowanie się do innych systemów. Ponadto sposób użytkowania hasła osłabia jego bezpieczeństwo: hasło możliwe do zapamiętania nie jest losowym ciągiem znaków. W przypadku SSH możliwe jest skonfigurowanie autentykacji za pomocą kluczy.

Instrukcja

Autentykacja z użyciem kryptografii asymetrycznej

☐1 W trakcie ćwiczenia skonfigurujesz klienta i serwer SSH: często tę funkcję pełni jeden i drugi komputer. Dla ustalenia uwagi jeden z komputerów zespoły będzie pełnił rolę zdalnego serwera, a drugi klienta, z którego konfigurujemy dostęp.

☐2 Pliki konfiguracyjne SSH w systemie Linux zlokalizowane są w katalogu `/etc/ssh/`. Obejrzyj ich zawartość. Sprawdź lokalizację kluczy publicznych i prywatnych komputera.

☐3 Pracując jak zwykły użytkownik, upewnij się, że jesteś w katalogu domowym. Wygeneruj klucze publiczny i prywatny używając polecenia `ssh-keygen`. Wybierz klucz innyego typu niż RSA! Zanotuj hasło jeśli ustawiłeś:..... (na wszelki wypadek) Zwróć gdzie umieszczone są wygenerowane klucze.

☐4 Gdy para kluczy jest już wygenerowana nadszedł czas na umieszczenie klucza publicznego na komputerze, z którym chcemy się łączyć przy użyciu klucza SSH. W tym celu należy użyć polecenia `ssh-copy-id`. Po raz ostatni należy w tym przypadku podać stare hasło, którym logowaliśmy się dotychczas.

☐5 Sprawdź poprawność działania logowania.

☐6 Wykonaj na zdalnym komputerze komendę nie logując się tam.

☐7 Wykorzystując program `wireshark` podsłuchaj nawiązywanie komunikacji między klientem, a serwerem. Przeanalizuj proces nawiązywania połączenia i korzystając z internetu, krótko opisz funkcje zaobserwowanych pakietów.

Lp.	Nazwa komunikatu	Opis funkcji/zawartości komunikatu
1		
2		
3		
4		
5		
6		
7		

Logowanie się z użyciem SSH i klucza sprzętowego Ybikey

- ☐a Skonfiguruj użycie kluczy sprzętowych Yubikey do logowanie się za pośrednictwem protokołu SSH
- ☐b Tutorial dla różnych wariantów dostępne jest tutaj: `https://developers.yubico.com/SSH/`
- ☐c Zademonstruj działanie tego sposobu autentykacji.
- ☐d Wezwij prowadzącego celem weryfikacji poprawności zadania.....

Tunel SSH

Tunelowanie SSH jest przesyłaniem nieszyfrowanego ruchu TCP (np. POP3 czy HTTP) poprzez bezpieczny protokół SSH.

- ☐a Na jednym z komputerów stwórz prostą stronę internetową (wystarczy edycja pliku `/var/www/html/index.html`). Uruchom serwer www. Sprawdź widoczność strony.
- ☐b Stwórz tunel SSH pomiędzy komputerami (liczne opisy w internecie), który przekieruje port 80 zdalnej maszyny na port 8888 maszyny lokalnej.
- ☐c Otwórz stronę *http://localhost:8888* na komputerze na którym otwarto tunel.
- ☐d Używając wiresharka sprawdź ruch w trakcie odświeżania powyższej strony.
- ☐e Zamknij tunel i ponownie sprawdź stronę *http://localhost:8888*.
- ☐f Wezwij prowadzącego celem weryfikacji poprawności zadania.....

Zaliczenie ćwiczenia

Zapisz do pliku kluczowe komendy zastosowane w celu wykonania ćwiczenia. Zapisz do pliku utworzone certyfikaty. Zapisz ostateczne wersje plików konfiguracyjnych serwera. Wszystko razem dołącz do odpowiedzi na zadanie w Teams.