



Bezpieczeństwo systemów rozproszonych

SPRAWOZDANIE Z ĆWICZENIA: Kontrola dostępu do usług

Imię Nazwisko: nr albumu:

data ćwiczenia: godzina:



Aby wykonać poniższe ćwiczenia uruchom system operacyjny Linux czysty

Zapisz nazwę swojego komputera, jego adres IP i maskę podsieci:



Pobierz przykładową konfigurację do ćwiczeń zgodnie z instrukcjami pod adresem:

https://www.cs.put.poznan.pl/mszychowiak/security/tools/lab_tcpd/

1. Demon internetowy xinetd

1. W którym pliku i jaką modyfikację należy wykonać, aby wymusić pośredniczenie narzędzia TCP Wrapper w nadzorowaniu połączeń dla usługi rlogin?

plik:

modyfikacja:

2. TCP Wrapper

2. Zapewnij zasadę domyślnej odmowy dostępu. Podaj zawartość odpowiedniego pliku.

nazwa pliku:

zawartość:

3. Skonfiguruj politykę dostępu tak, aby umożliwić dostęp do usługi rlogin jedynie z sąsiedniego komputera. Wypisz jakie zostały wykonane zmiany i w których plikach:

4. Skonfiguruj tcpd tak, aby umożliwiał dostęp do usługi rlogin z bieżącej sieci lokalnej z wyjątkiem sąsiedniego komputera. Zapisz regułę konfiguracyjną:

W przypadku próby dostępu z sąsiedniego komputera, klient powinien otrzymać przygotowany przez ciebie komunikat o zablokowanym dostępie. Zapisz regułę konfiguracyjną:

5. Przed czym i w jaki sposób chroni użycie w polityce predykatu PARANOID?

2.2 Wykorzystanie polityk dostępu przez sshd bez użycia tcpd

6. Skonfiguruj politykę tak, aby umożliwić dostęp do usługi ssh jedynie z sąsiedniego komputera (bez użycia xinetd i tcpd). Wypisz jakie zostały wykonane zmiany i w których plikach:

nazwa pliku:

zawartość:

Koniecznie przetestuj konfigurację!

2.3 Kontrola dostępu wbudowana w xinetd

7. Skonfiguruj xinetd bez użycia tcpd tak, aby umożliwiał dostęp do usługi rlogin jedynie z sąsiedniego komputera. Wypisz jakie zostały wykonane zmiany i w których plikach:

nazwa pliku:

zawartość:

8. Jak ograniczyć w konfiguracji xinetd dozwolone godziny wykorzystania usługi rlogin?