

Administrowanie systemami sieciowymi - Linux

Laboratorium 2.4 - Konfiguracja i monitorowanie sieci; zdalny dostęp

Zadania do wykonania

1. Zainstalować i uruchomić serwer (demon) ssh.
2. Określić adres sprzętowy interfejsu sieciowego (karty sieciowej) i bazując na tej informacji ustalić jego producenta.
3. Zapoznać się z konfiguracją interfejsu sieciowego (karty sieciowej). Dodać i skonfigurować nowy pseudointerfejs (wraz z adresem, żeby odpowiadał na 'pingi').
4. Dla trzech wybranych węzłów w sieci Internet (Polska, Europa, Świat):
 - określić średni czas potrzebny na osiągnięcie węzła przez pakiet
 - zbadać trasę jaką są przesyłane pakiety do podanego węzła
 - określić maksymalny rozmiar pakietu, dla którego węzeł docelowy "odpowiada"

Wyniki i podsumowania zamieścić (i przeanalizować) w sprawozdaniu.

5. Zarejestrować i zapisać do pliku (za pomocą tcpdump) wszystkie pakiety związane z:
 - testowaniem za pomocą polecenia ping nieistniejącego hosta (np. niematakiegohosta.pl)
 - testowaniem za pomocą polecenia ping dowolnego istniejącego hosta
 - rejestrowaniem trasy do dowolnego istniejącego hosta (nie odwiedzanego wcześniej) za pomocą traceroute.

Analizę wybranych pakietów zamieścić w sprawozdaniu.

6. Za pomocą tcpdump ustalić, czy korzystanie z e-Portalu jest bezpieczne, tzn.:
 - czy nazwa użytkownika i hasło są przesyłane w postaci zaszyfrowanej
 - czy treści (nazwy kursów, opisy, itd.) są przesyłane w postaci zaszyfrowanej

Odpowiednie pakiety wraz z analizą zamieścić w sprawozdaniu.

7. Wyświetlić bieżącą tablicę tras, usunąć ścieżkę domyślną dla pakietów (sprawdzić czy jest dostęp do Internetu), a następnie dodać ją ponownie.

8. Korzystając z polecenia netstat wyświetlić listę połączeń opartych na protokole TCP. Następnie nawiązać sesję z dowolnym serwerem WWW. Ponownie wyświetlić listę połączeń - dwa razy: raz z nazwami hostów i portów, a drugi raz numerami IP hostów i portów. Przeanalizować wyniki odpowiadające nawiązanym sesjom, wyjaśnić znaczenie pól.
9. Korzystając z polecenia nmap:
 - ustalić jakie komputery w sieci laboratorium (lub domowej) są dostępne (wykorzystać pakiety ICMP, wyniki zapisać do pliku XML).
 - przeskanować porty jednego z komputerów (można uruchomić wirtualną maszynę z Windows lub Linux). Przeanalizować wyniki dla jednego z otwartych portów.
10. Za pomocą scp:
 - skopiować plik na zdalny komputer
 - skopiować plik ze zdalnego komputera
 - skopiować poddrzewo katalogów ze zdalnego komputera(Ćwiczenie należy wykonać w parach lub uruchomić drugi system Linux).
11. Wyświetlić tablicę arp, przeanalizować wybrany wpis.