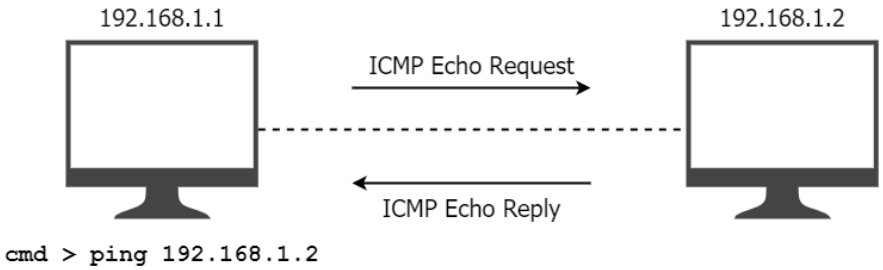
Temat: Zarządzanie usługami i logami w systemach Linux

1. Zakres laboratorium:

Celem laboratorium jest zapoznanie studenta z podstawowymi mechanizmami bezpieczeństwa systemach rodziny Linux. W ramach ćwiczenia student ma za zadanie skonfigurować firewall, tak aby blokował przychodzące pakiety ICMP. Kolejnym etapem jest zmiana domyślnego portu usługi SSH.

Umiejętności nabyte przez studenta należą do zestawu elementarnych umiejętności, które powinni posiadać zarówno administratorzy IT (ang. DevOps), ale również programiści pracujący w środowisku Linux.

2. Schemat działania polecenia ping

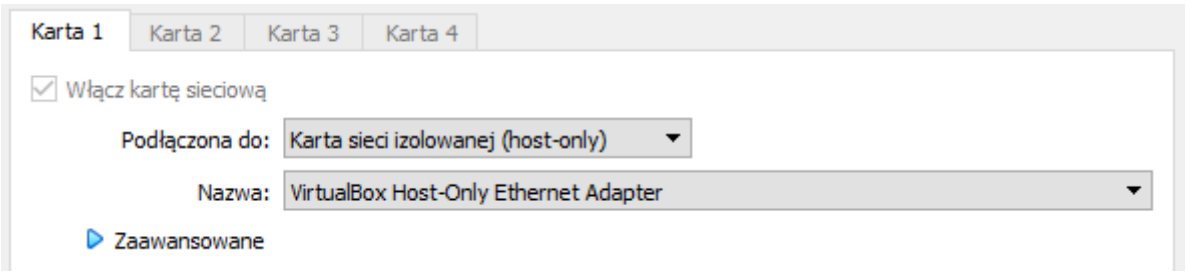


3. Wymagane oprogramowanie:

- program VirtualBox
- maszyna wirtualna z systemem CentOS 8 w wersji Minimal
- program Putty
- program Wireshark

4. Konfiguracja VirtualBox

Na potrzeby tego zadania należy zmienić tryb pracy karty sieciowej na: „Karta sieci izolowanej”



Uwaga! W tym trybie powstaje osoba podsieć między systemem hosta a maszyną wirtualną. Domyślnie adres tej podsieci to 192.168.56.0/24. Niestety w tym trybie Twoja maszyna wirtualna nie ma dostępu do sieci zewnętrznej.

Aby mieć dostęp do sieci zewnętrznej należy dodać drugą kartę sieciową i ustawić jej tryb pracy na „NAT”.

5. Instalacja dodatkowego oprogramowania

Domyślnie systemy operacyjne nie mają zainstalowanego żadnego edytora tekstu, więc w celu instalacji swojego ulubionego edytora należy wykorzystać menadżer pakietów yum:

- VIM: `yum install vim`
- NANO: `yum install nano`

Dodatkowo w tym zadaniu

UWAGA! Instalacja dodatkowego oprogramowania jest możliwa dopiero po uzyskaniu dostępu do sieci internetowej, np. poprzez uruchomienie klienta DHCP.

6. Przebieg laboratorium:

1. Uruchom maszynę wirtualną przy pomocy programu VirtualBox
2. Zaloguj się jako root (pass: root)
3. Stwórz konto użytkownika wykorzystując swoje imię i nazwisko (np. pierwsza litera imienia i nazwisko), jako komentarz podaj swoje pełne imię i nazwisko
4. Na potrzeby tego ćwiczenia możesz przypisać użytkownikowi proste, słownikowe hasło
5. Dodaj użytkownika do grupy wheel, dzięki czemu będzie mógł korzystać z sudo:

   ```
   usermod -G wheel nazwa_uzytkownika
   ```

6. Wyświetl zawartość pliku `/etc/passwd` (zrzut ekranu dodaj do notatek)
7. Uruchom klienta DHCP dla interfejsu ethernet (enp…):

   ```
   dhclient nazwa_interfejsu
   ```

8. Wyświetl stan interfejsów. Wykonaj zrzut ekranu i dodaj go do notatek. Podaj jaki adres IP został przydzielony do maszyny wirtualnej.
9. Zaloguj się przy pomocy Putty na maszyne wirtualną wykorzystując wcześniej przygotowane konto użytkownika. Od tej pory wszystkie polecenia wykonuj przy użyciu Putty. Dodaj do notatek zrzut ekranu przedstawiający pomyślne zalogowanie przez Putty.
10. Wykonaj ping z systemu hosta (np. z terminala w systemie Windows) do maszyny wirtualnej (zrób zrzut przedstawiający wynik polecenia)
11. W kolejnych krokach będziesz wykorzystywał polecenie `firewall-cmd`, aby wyświetlić instrukcję tego polecenia wpisz `man firewall-cmd`.
12. Znajdź opcję polecenia firewall-cmd, która wyświetla stan usługi firewalld, a następnie wywołaj ją (zapisz w notatkach użyte polecenie oraz zrzut ekranu przedstawiający wynik polecenia).
13. Pierwszym zadaniem będzie zablokowanie pakietów ICMP Echo Request wysyłanych przez polecenie ping do maszyny wirtualnej.
14. Sprawdź, które wersje protokołu IP są obsługiwane przez typ ICMP Echo Request.

    ```
    firewall-cmd --info-icmptype=echo-request
    ```

15. Sprawdź, czy pakiety ICMP Echo Request są blokowane przez firewall:

    ```
    firewall-cmd --query-icmp-block=echo-request
    ```

16. Jeśli ten typ pakietów nie jest blokowany, należy go zablokować:

    ```
    firewall-cmd --add-icmp-block=echo-request
    ```

17. Wyświetl stan strefy domyślnej (zapisz zrzut ekranu przedstawiający wynik polecenia):

    ```
    firewall-cmd --list-all
    ```

18. Uruchom Wireshark, wybierz interfejs VirtualBox Host-Only Network, a następnie z systemu hosta wykonaj ping do wirtualnej maszyny (wykonaj zrzut ekranu przedstawiający wynik polecenia ping). Nie wyłączaj Wiresharka do końca ćwiczenia!
19. Wykonaj zrzut ekranu programu Wireshak przedstawiający wysłane i odebrane pakiety ICMP.
20. Wyłącz wcześniej ustaloną blokadę:

    ```
    firewall-cmd --remove-icmp-block=echo-request
    ```

21. Zmień tryb pracy firewalla:

    ```
    firewall-cmd --permanent --set-target=DROP
    ```

22. Ustal blokadę wszystkich typów wiadomości ICMP:

    ```
    firewall-cmd --add-icmp-block-inversion
    ```

23. Przeładuj reguły firewalla:

    ```
    firewall-cmd --reload
    ```

24. Wyświetl stan strefy domyślnej (zapisz zrzut ekranu przedstawiający wynik polecenia):

    ```
    firewall-cmd --list-all
    ```

25. Ponownie wykonaj ping do wirtualnej maszyny (wykonaj zrzut ekranu przedstawiający wynik polecenia ping)
26. Wykonaj zrzut ekranu programu Wireshark przedstawiający pakiety ICMP powiązane z wykonaniem polecenia ping w poprzednim punkcie.
27. Kolejny etapem jest zmiana domyślnego portu usługi SSH. W tym celu należy zainstalować program `semanage:`

    ```
    yum install -y policycoreutils-python-utils
    ```

28. Otwórz w dowolny edytorze plik /etc/ssh/sshd_config a następnie odkomentuj linijkę zawierającą Port 22. Zamiast 22 wpisz dowolny numer portu. Uwaga! Nie może to być „dobrze znany” port, dlatego najlepiej wybrać liczbę większą od 1024.
29. Wykonaj zrzut ekranu przedstawiający wykonaną zmianę a następnie zapisz plik.
30. Przy pomocy menadżera SELinux, należy zezwolić na pracę usługi ssh na innym porcie:

    ```
    semanage port -a -t ssh_port_t -p tcp nowy_port
    ```

31. Sprawdź, czy zmiany zostały wprowadzone (zapisz zrzut ekranu):

    ```
    semanage port -l | grep ssh
    ```

32. Dodaj nowy port usługi ssh do reguł, a następnie przeładuj firewalla:

```
firewall-cmd --add-port=nowy_port/tcp --permanent
firewall-cmd --reload
```

33. Sprawdź reguły usług w firewall, jeśli ssh jest dodane do reguł usuną ją (zapisz zrzut ekranu):

```
firewall-cmd --list-services
firewall-cmd --remove-service=ssh --permanent
firewall-cmd --reload
```

34. Zrestartuj usługę ssh, następnie sprawdź status (zapisz zrzut ekranu):

```
systemctl restart sshd
systemctl status sshd
```

35. Przy pomocy putty spróbuj zalogować się na wirtualną maszynę. Za pierwszym razem wykorzystaj domyślny port 22. Za drugim razem wykorzystaj do połączenia nowo ustalony port. Zapisz zrzuty ekranu obydwóch prób.
36. Odpowiedz na pytania:
    - Na podstawie informacji z Wiresharka napisz, jaka jest różnica między pierwszą a drugą metodą blokowania pakietów ICMP Echo Request?
    - Która z tych metod jest lepsza pod kątem bezpieczeństwa i dlaczego?
    - Jaki jest cel zmiany domyślnych portów usług?

7. Notatki z ćwiczenia:

Data	*Grupa*
Imię i nazwisko	

1. Nazwa użytkownika: …
2. Adres IP wykorzystywanej maszyny wirtualnej:
3. Wykonane zrzuty ekranu wraz z opisem:

4. Odpowiedz na pytania z punktu 35.
    a. odpowiedź
    b. odpowiedź
    c. odpowiedź