T: Zabezpieczenie dostępu do komputera.

Cel ogólny lekcji jest nauczenie uczniów zabezpieczania dostępu do komputera poprzez ustawienie statycznego adresu IP, instalację serwera SSH i DenyHosts, oraz zastosowanie różnych metod zabezpieczania dostępu poprzez blokowanie i odblokowywanie dostępu dla wybranych komputerów lub podsieci.

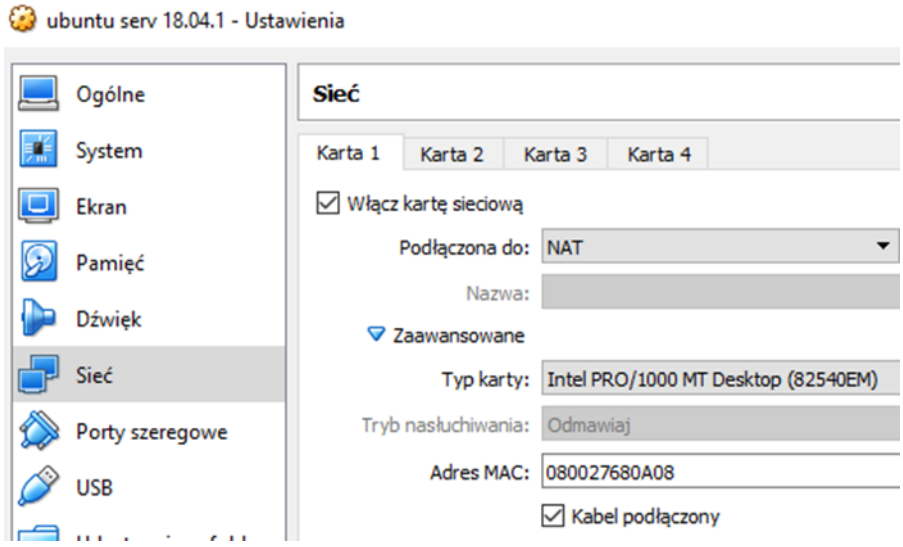
Cele szczegółowe lekcji:

1. Zapoznanie uczniów z poleceniami służącymi do zabezpieczania dostępu do komputera, takimi jak instalacja serwera SSH i DenyHosts.
2. Uczyć, jak używać statycznego adresu IP, aby zabezpieczyć komputer przed nieautoryzowanym dostępem.
3. Nauczyć, jak blokować i odblokowywać dostęp do serwera dla wybranych komputerów lub podsieci poprzez edycję plików hosts.deny i hosts.allow.
4. Uczyć, jak korzystać z usługi telnet do testowania połączenia z serwerem.

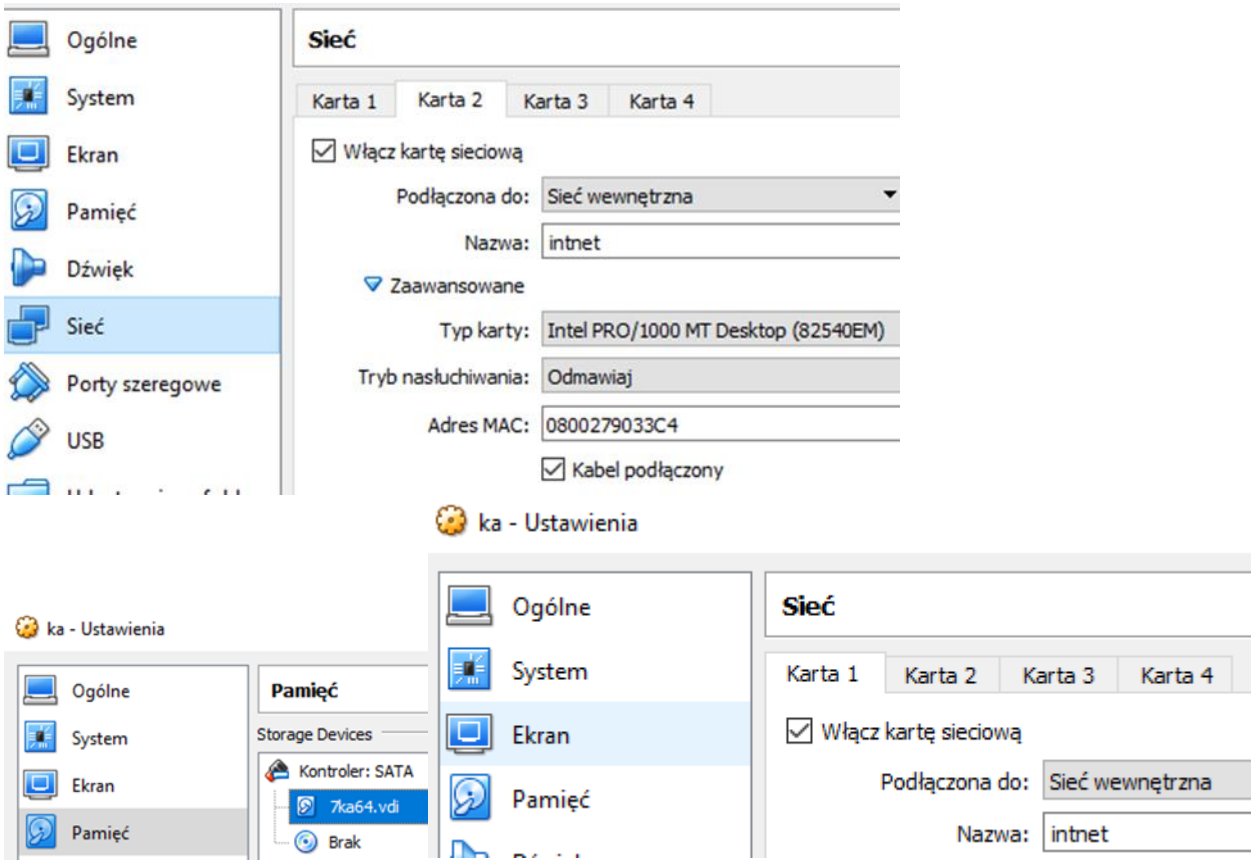
Podczas wykonywania poniższych zadań w zeszycie w sprawozdaniu podaj i wyjaśnij
1. polecenia, które użyjesz, aby zabezpieczyć dostęp do komputera.
2. odpowiedzi na pytania zadane w treści zadań.

Przed przystąpieniem do ćwiczenia sprawdź czy ustawienie maszyny wirtualnej pozwala na dostęp do Internetu, jeżeli ustawienia są niezgodne wykonaj konfigurację pierwszej i drugiej karty sieciowej według instrukcji, a następnie uruchom Ubuntu.

Adapter 1



Adapter 2



Do ćwiczenia potrzebna jest nowa (czysta):

- instalacja Ubuntu serwera. Przygotuj Ubuntu - przywróć migawkę 1 wykonaną na pierwszej lekcji.

- instalacja Windows (7 lub 10) – przekopiuj z folderu z wzorcowymi plikami dysków do swojego folderu.

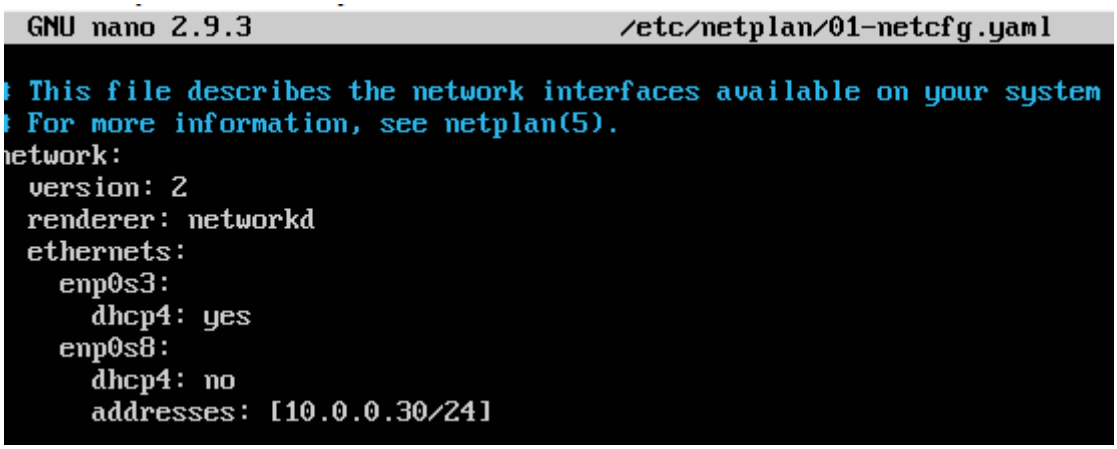
Po uruchomieniu Ubuntu podaj **login**: ubuntu **Password**: 1234

Wpisz sudo -s **Password**: 1234

```
ubuntu@dlp:~$ sudo -s
[sudo] password for ubuntu:
```

Przygotowanie do ćwiczenia. Ustawienie statycznego adresu IP.

1. Pozostaw adres IP dla Ubuntu na Adapter 2 na statyczny.
Otwórz plik, który opisuje interfejsy sieciowe nano /etc/netplan/01-netcfg.yaml
Pozostaw zalecane wpisy w tym pliku



2. Jeżeli dokonałeś zmian zastosuj ustawienia
root@dlp:~# netplan apply

```
root@dlp:/# netplan apply
```

3. Zaktualizuj pamięć podręczną repozytorium pakietów, używając następującej komendy:
apt-get update
4. Zainstaluj serwer SSH, uruchom następujące polecenie
apt install openssh-server -y
5. Zainstaluj DenyHosts dla Ubuntu
apt-get install denyhosts

Zadanie 1

Zabezpieczanie dostępu do komputera.

Zapisz w zeszycie kolejne czynności wykonane w celu zabezpieczania dostępu do komputera.

Aby umożliwić dostęp do serwera tylko wybranego komputera w sieci, lub grupie wybranych komputerów w sieci:

1. Pozostań zalogowanym do konta użytkownika root. Zablokuj dostęp do wszystkich usług serwera.

   Przygotuj pliki zabezpieczanego komputera (serwera).

   a) Wykonaj kopie pliku hosts.deny

   ```
   root@dlp:~# cp /etc/hosts.deny /etc/kopiahosts.deny
   ```

   b) Edytuj pliku hosts.deny

   ```
   root@debian:~# nano /etc/hosts.deny
   ```

   c) W pliku /etc/hosts.deny na końcu dopisz ALL: ALL.

   ```
   ALL: ALL
   ```

2. Odblokuj dostęp tylko dla wybranego komputera.

   a) Wykonaj kopie pliku hosts.alllow

   ```
   root@dlp:~# cp /etc/hosts.allow /etc/kopiahosts.allow
   ```

   b) Edytuj pliku hosts.alllow

```
root@dlp:~# nano /etc/hosts.allow
```

c) W pliku /etc/hosts.allow dopisz adres komputera uprawnionego do korzystania z serwera np. ALL: 10.0.0.41 `ALL: 10.0.0.41`

3. Odblokuj dostęp tylko dla podsieci komputerów.

d) W pliku /etc/hosts.alIow dopisz adres podsieci z komputerami uprawnionymi do korzystania z serwera, np. ALL: 10.0.0.0/255.255.255.0 `All: 192.167.0.0/255.255.255.0`

4. Odblokuj dostęp tylko dla podsieci, z wyjątkiem jednego z komputerów.

a) W pliku /etc/hosts.allow dopisz adres podsieci z komputerami uprawnionymi do korzystania z serwera i podaj adres zablokowanego komputera, np. ALL: 10.0.0.0/255.255.255.0 EXCEPT 10.0.0.224

```
All: 192.167.0.0/255.255.255.0 EXCEPT 192.167.0.224
```

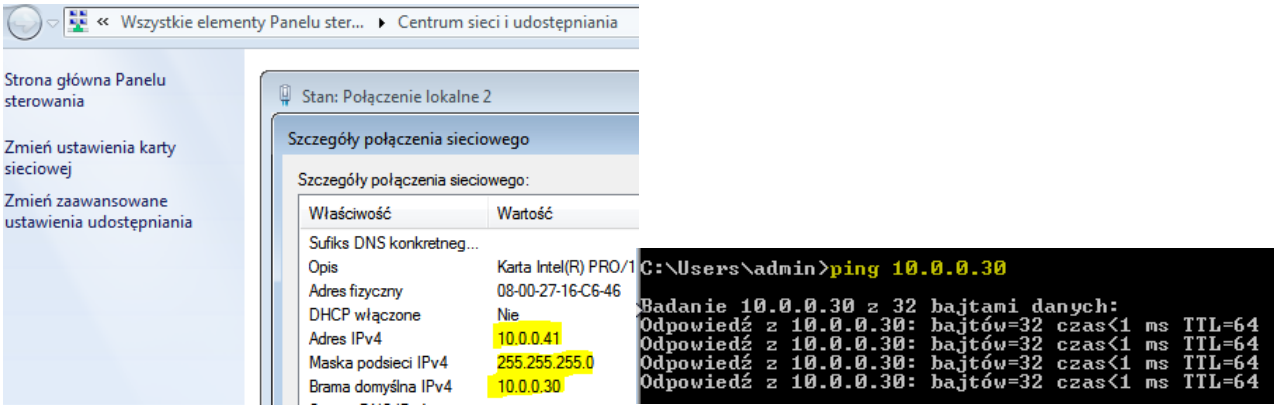
5. Przetestuj możliwość nawiązywania połączenia z serwerem.

a) Zainstaluj usługę telnet. `root@dlp:~# apt install telnetd`

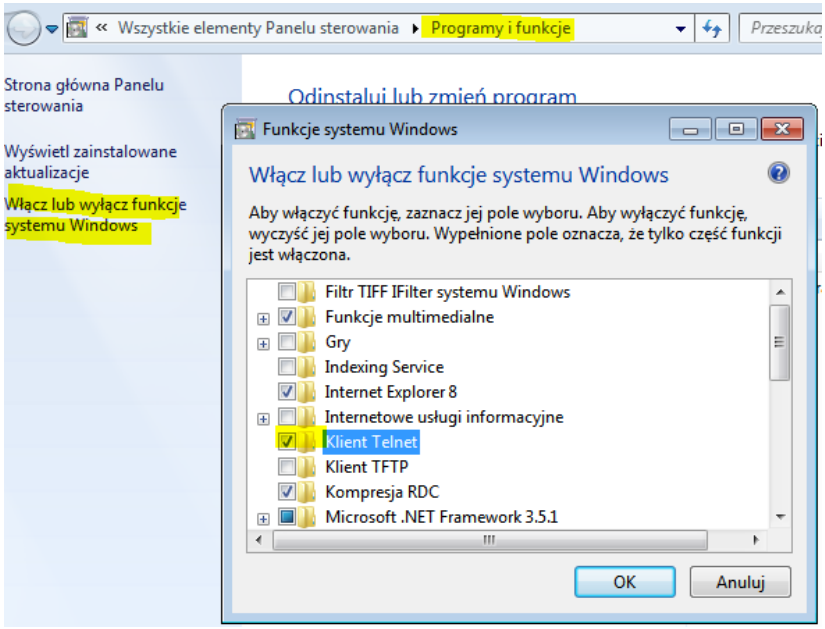
b) Wykonaj restart demona telnetu.

```
root@dlp:~# /etc/init.d/openbsd-inetd restart
[ ok ] Restarting openbsd-inetd (via systemctl): openbsd-inetd.service.
```

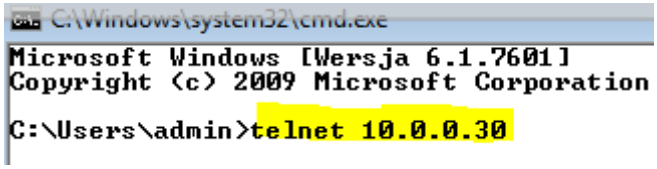
c) Ustaw na kliencie (7-ce) adres ip.



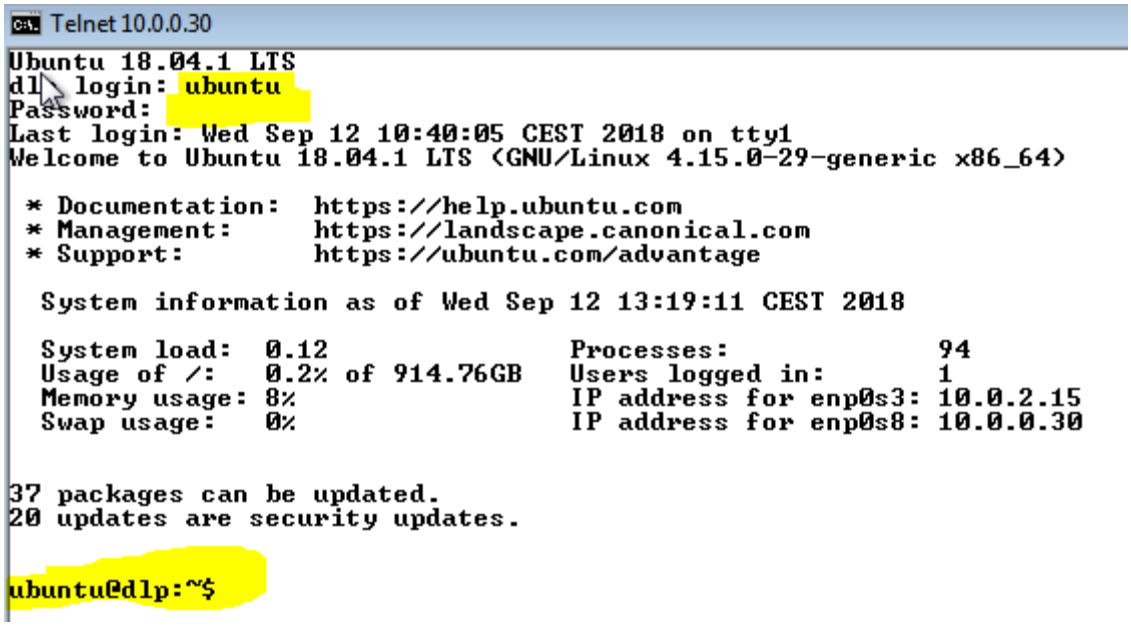
d) Ustaw na kliencie (7-ce) funkcje Klient Telnet.



e) Uruchom telnet na 10.0.0.30



f) Podaj login ubuntu i hasło 1234 (uwaga hasło nie wyświetla się)



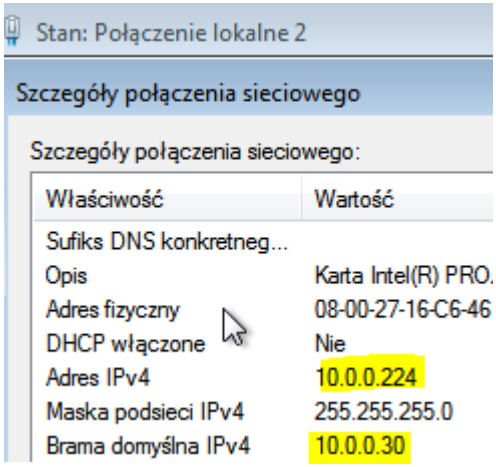
g) Sprawdź nawiązane połączenia i otwarte porty protokołu TCP/IP na porcie 23.

```
C:\Users\admin>netstat -an |find /i "23"
  TCP        10.0.0.41:49164        10.0.0.30:23           USTANOWIONO
  TCP        10.0.2.15:49167        157.56.96.123:443      USTANOWIONO
  UDP        10.0.2.15:63723        *:*
```

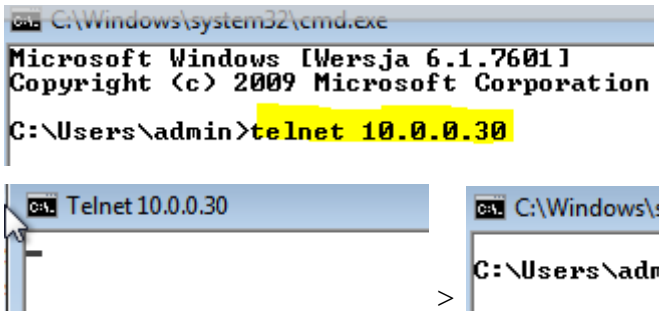
h) Czy jest ustawione połączenia na porcie 23?

(zgłoszenie) 1

i) Zmień adres ip na 10.0.0.224.



j) Sprawdź możliwość korzystania z usługi telnetu.



k) Sprawdź nawiązane połączenia i otwarte porty protokołu TCP/IP na porcie 23.

```
C:\Users\admin>netstat -an |find /i "23"
C:\Users\admin>_
```

l) Czy jest ustawione połączenia na porcie 23?

m) Dlaczego nie jest ustawione połączenia na porcie 23?

(zgłoszenie) 2

Zadanie 2

Konfigurowanie DenyHosts

Plik konfiguracyjny DenyHosts w Ubuntu to /etc/denyhosts.conf

Aby edytować plik konfiguracyjny DenyHosts, uruchom następujące polecenie:

nano /etc/denyhosts.conf

Przyjrzyjmy się teraz niektórym właściwościom w pliku konfiguracyjnym DenyHosts i ich działaniu.

DENY_THRESHOLD_INVALID

Ta opcja jest odpowiedzialna za blokowanie logowania SSH dla kont użytkowników, które nie istnieją w systemie. Domyślna wartość to 5. Oznacza to, powiedzmy, że ktoś próbuje zalogować się do serwera

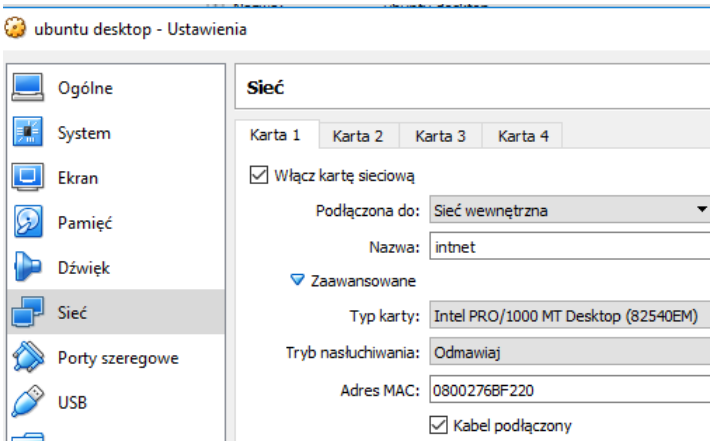
SSH jako różne nazwy użytkowników. Jeśli próba jest w sumie większa niż 5 razy, wówczas adres IP komputera próbującego nawiązać połączenie zostanie dołączony do pliku /etc/hosts.deny, w ten sposób komputer nie będzie mógł połączyć się z serwerem SSH dopóki nie zostanie usunięty z pliku /etc/hosts.deny.

```
#
DENY_THRESHOLD_VALID = 10
#
```

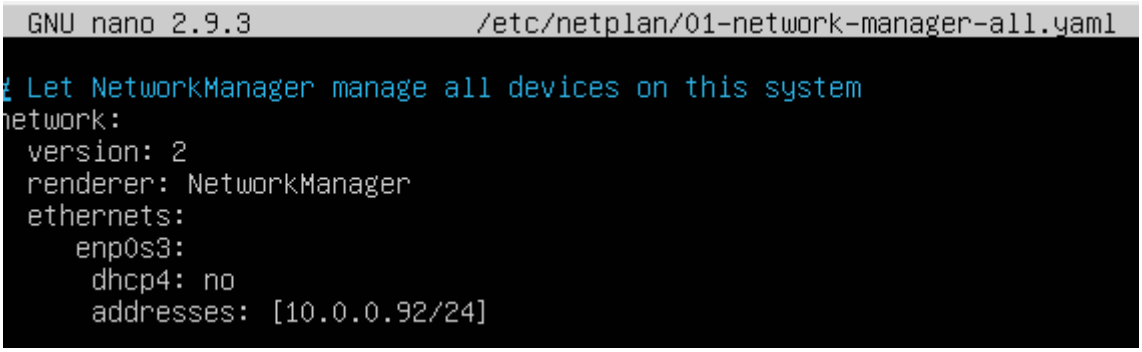
Na poniższym zrzucie ekranu widać, że adres IP mojego serwera denyhosts to 10.0.0.30

```
root@dlp:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
0
    link/ether 08:00:27:ef:99:cd brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic e
       valid_lft 81957sec preferred_lft 81957sec
    inet6 fe80::a00:27ff:feef:99cd/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
0
    link/ether 08:00:27:13:dd:98 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.30/24 brd 10.0.0.255 scope global enp0s8
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe13:dd98/64 scope link
       valid_lft forever preferred_lft forever
```

1. Ustaw maszynę wirtualną drugiego komputera (ubuntu desktop),



2. Ustaw adres IP drugiego komputera (ubuntu desktop), który spróbuję połączyć się z serwerem denyhosts, to 10.0.0.92




```
root@bolek-VirtualBox:~# netplan apply
```

3. Spróbuj połączyć się z serwerem jako baduser. Zauważ, że użytkownik baduser nie istnieje w serwerze denyhosts. Podaj przypadkowe hasło.

ssh baduser@10.0.0.30

Jak widać, próbowałem zalogować się kilka razy i każda próba nie powiodła się.

```
root@bolek-VirtualBox:~# ping 10.0.0.30
PING 10.0.0.30 (10.0.0.30) 56(84) bytes of data.
64 bytes from 10.0.0.30: icmp_seq=1 ttl=64 time=0.622 ms
64 bytes from 10.0.0.30: icmp_seq=2 ttl=64 time=0.497 ms
64 bytes from 10.0.0.30: icmp_seq=3 ttl=64 time=0.500 ms
^C
--- 10.0.0.30 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2030ms
rtt min/avg/max/mdev = 0.497/0.539/0.622/0.064 ms
root@bolek-VirtualBox:~# ssh baduser@10.0.0.30
The authenticity of host '10.0.0.30 (10.0.0.30)' can't be established.
ECDSA key fingerprint is SHA256:ujdruTloGRTzpNXQzE9KojeR26kOUlOqAU9ON8p1aOg.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.0.30' (ECDSA) to the list of known hosts.
baduser@10.0.0.30's password:
Permission denied, please try again.
baduser@10.0.0.30's password:
Permission denied, please try again.
baduser@10.0.0.30's password:
baduser@10.0.0.30: Permission denied (publickey,password).
root@bolek-VirtualBox:~#
```

4. Spróbuj jeszcze kilka razy, otrzymasz komunikat "Połączenie zamknięte przez zdalny host". Oznacza to, że mój adres IP został zablokowany przez DenyHosts.
5. Przeczytaj zawartość pliku /etc/hosts.deny za pomocą polecenia:

cat /etc/hosts.deny

Powinieneś zobaczyć adres IP komputera, który próbowałeś zalogować jako nieistniejący użytkownik baduser. Więc DenyHosts działa idealnie (patrz poniżej).

```
root@dlp:~# cat /etc/hosts.deny
# /etc/hosts.deny: list of hosts that are _not_ allowed to access the system.
#                  See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:    ALL: some.host.name, .some.domain
#             ALL EXCEPT in.fingerd: other.host.name, .other.domain
#
# If you're going to protect the portmapper use the name "rpcbind" for the
# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.
#
# The PARANOID wildcard matches any host whose name does not match its
# address.
#
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID
ALL: ALL
sshd: 10.0.0.92
root@dlp:~#
```

6. Opisz w zeszycie poniższe opcje:

DENY_THRESHOLD_VALID

Ta opcja jest taka sama jak DENY_THRESHOLD_INVALID

Jedyna różnica polega na tym, że DENY_THRESHOLD_VALID dotyczy istniejących użytkowników na maszynie denyhosts-server.

Oznacza to, że jeśli próby logowania dla istniejących użytkowników zakończą się niepowodzeniem 10 razy (wartość domyślna), adres IP komputera próbującego nawiązać połączenie zostanie dołączony do pliku /etc/hosts.deny.

Maszyna próbująca się połączyć nie będzie już mogła łączyć się z serwerem.

```
#
# DENY_THRESHOLD_VALID: block each host after the number of failed
# login attempts has exceeded this value.  This value applies to valid
# user login attempts (eg. user accounts that exist in /etc/passwd) except
# for the "root" user
#
DENY_THRESHOLD_VALID = 10
#
```

DENY_THRESHOLD_ROOT

To samo, co pozostałe dwie opcje. Tak samo jak pozostałe dwie opcje. Wartość to 1. Oznacza to, że jeśli ktoś spróbuje połączyć się z serwerem denyhosts jako root i raz się nie powiedzie, jego / jej adres IP zostanie dołączony do pliku /etc/hosts.deny. Nie będzie on już mógł się połączyć z serwerem.

HOSTNAME_LOOKUP

Domyślnie w systemie Ubuntu DenyHosts nie rozpoznaje nazw hostów. Oznacza to, że adresy IP nie zostaną przekształcone na nazwy hostów. Ale jeśli potrzebujesz rozwiązać nazwy hostów na adres IP i tak dalej, ustaw HOSTNAME_LOOKUP na YES i zapisz plik.

```
# HOSTNAME_LOOKUP
#
# HOSTNAME_LOOKUP=YES|NO
# If set to YES, for each IP address that is reported by Denyhosts,
# the corresponding hostname will be looked up and reported as well
# (if available).
#
HOSTNAME_LOOKUP=NO
#
```

AGE_RESET_VALID

AGE_RESET_VALID informuje DenyHosts po upływie czasu, przez który nieudane próby logowania dla istniejącego użytkownika zostaną zresetowane do wartości 0. Domyślna wartość to 5 dni. Oznacza to, że jeśli ktoś spróbuje zalogować się w dniu 1, a następnie czekać przez 5 dni i spróbować ponownie zalogować się, DenyHosts nie umieszcza ich w pliku /etc/hosts.deny.

```
#
# AGE_RESET_VALID: Specifies the period of time between failed login
# attempts that, when exceeded will result in the failed count for
# this host to be reset to 0.  This value applies to login attempts
# to all valid users (those within /etc/passwd) with the
# exception of root.  If not defined, this count will never
# be reset.
#
# See the comments in the PURGE_DENY section (above)
# for details on specifying this value or for complete details
# refer to:  http://denyhost.sourceforge.net/faq.html#timespec
#
AGE_RESET_VALID=5d
#
```

AGE_RESET_ROOT

To samo co AGE_RESET_VALID, ale dotyczy tylko nieprawidłowych loginów root.

Domyślna wartość to 25 dni.

```
#
# AGE_RESET_VALID: Specifies the period of time between failed login
# attempts that, when exceeded will result in the failed count for
# this host to be reset to 0.  This value applies to login attempts
# to all valid users (those within /etc/passwd) with the
# exception of root.  If not defined, this count will never
# be reset.
#
# See the comments in the PURGE_DENY section (above)
# for details on specifying this value or for complete details
# refer to:  http://denyhost.sourceforge.net/faq.html#timespec
#
AGE_RESET_VALID=5d
#
```

AGE_RESET_INVALID

To samo, co AGE_RESET_VALID, ale dotyczy tylko nieudanych prób zalogowania się nieistniejących użytkowników maszyny denyhosts-server.

```
# AGE_RESET_INVALID: Specifies the period of time between failed login
# attempts that, when exceeded will result in the failed count for
# this host to be reset to 0.  This value applies to login attempts
# made to any invalid username (those that do not appear
# in /etc/passwd).  If not defined, count will never be reset.
#
# See the comments in the PURGE_DENY section (above)
# for details on specifying this value or for complete details
# refer to:  http://denyhost.sourceforge.net/faq.html#timespec
#
AGE_RESET_INVALID=10d
```

Jest więcej opcji. Ale są one poza zakresem tego ćwiczenia. Proszę zajrzeć na oficjalną stronę DenyHosts pod adresem http://denyhosts.sourceforge.net, aby uzyskać więcej informacji.

(zgłoszenie) 3

Przywróć pierwszą migawkę.

Podsumowanie:

Po wykonaniu wszystkich czynności z powyższej instrukcji przeczytaj ponownie z zrozumieniem cel ogólny i cele szczegółowe, które znajdują się na pierwszej stronie instrukcji. Jeżeli one zostały niezrealizowane to powtarzaj wykonie tej instrukcji w szkole lub/i w domu do momentu zrealizowania.