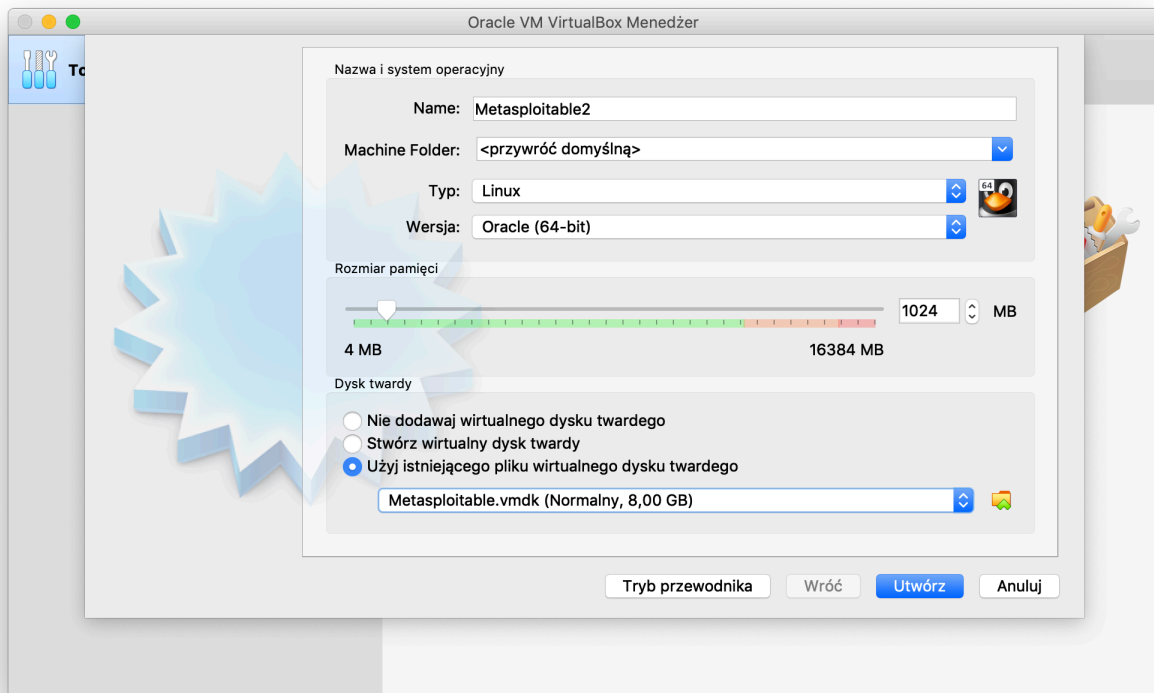


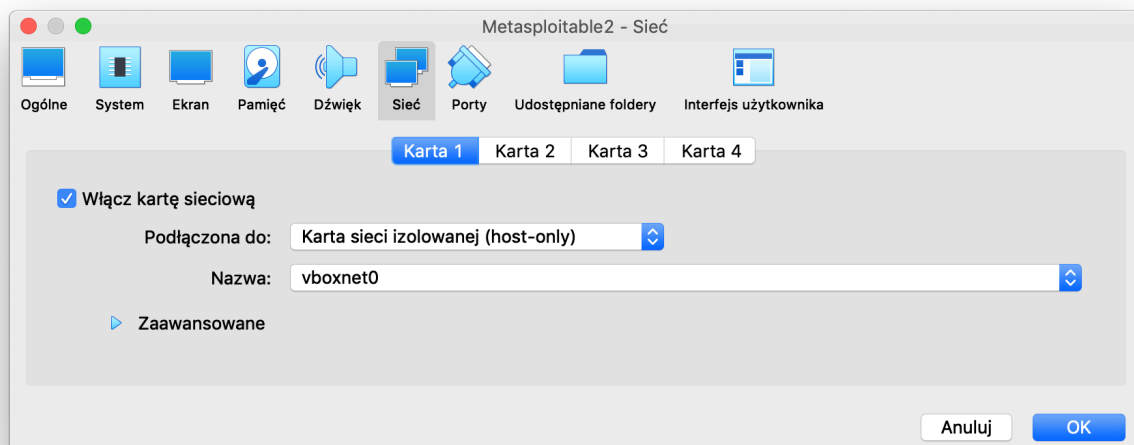
3. Zanim utworzymy maszynę wirtualną, należy wykonać polecenie, które pozwoli na podłączenie dysku w trybie „tylko do odczytu”:

VBoxManage modifymedium /home/ee1/prac/chaberb/share/metasploitable2.vmdk --type immutable

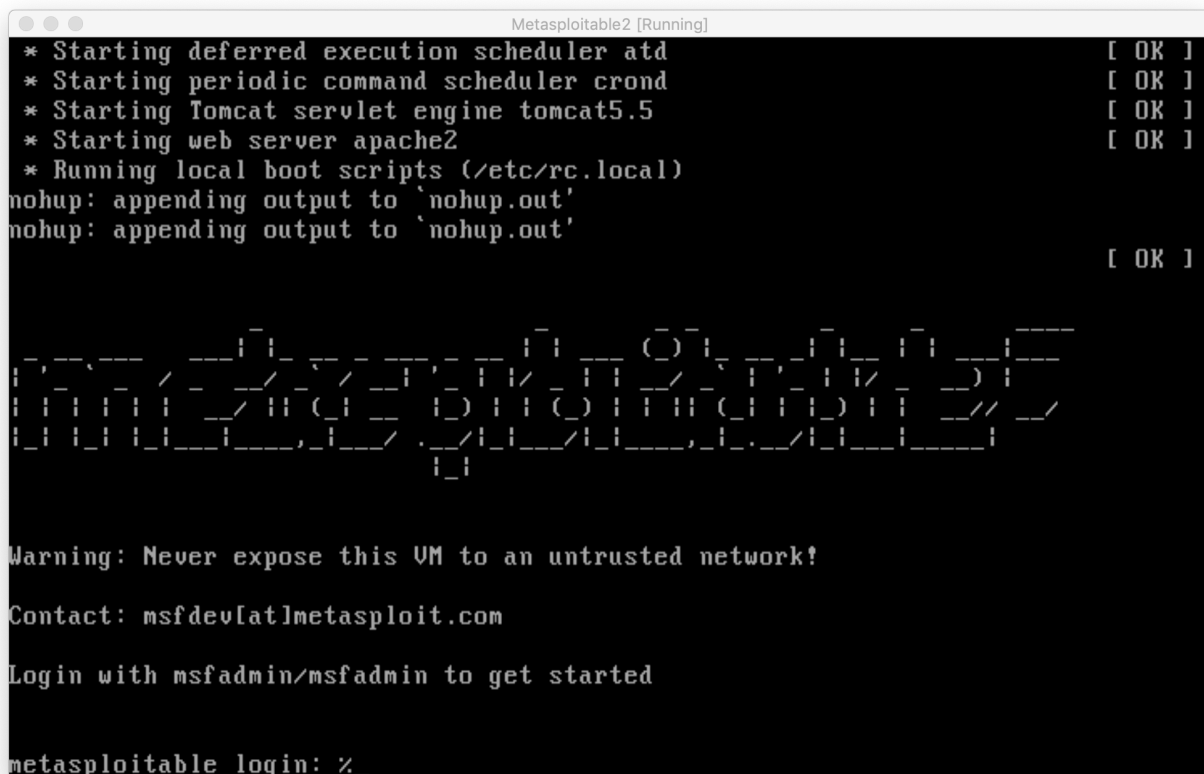
4. Utwórz nową maszynę wirtualną używając istniejącego pliku wirtualnego dysku twardego. Plik **metasploitable2.vmdk** znajduje się pod ścieżką **/home/ee1/prac/chaberb/share**



5. Przydziel maszynie co najmniej 1GB pamięci, jako „Wersja” podaj **Ubuntu (64-bit)**
6. Edytuj „Ustawienia” utworzonej maszyny, przejdź do zakładki „Sieć” i zmień „Podłączona do:” z **NAT** na **Karta sieci izolowanej (host-only)**. Pole „Nazwa” powinno automatycznie uzupełnić się wartością sieci dodanej w 2. (tj. **vboxnet0**). Zatwierdzamy zmiany przyciskiem „OK”



7. Maszyna jest gotowa do uruchomienia wybierając przycisk „Start”.
8. Po uruchomieniu możemy zalogować się do systemu (login: **msfadmin**, hasło: **msfadmin**), a następnie sprawdzić przydzielony adres IP poleceniem **ip a**; zwykle



```
Metasploitable2 [Running]
* Starting deferred execution scheduler atd [ OK ]
* Starting periodic command scheduler crond [ OK ]
* Starting Tomcat servlet engine tomcat5.5 [ OK ]
* Starting web server apache2 [ OK ]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to 'nohup.out'
nohup: appending output to 'nohup.out' [ OK ]

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login: %_
```

będzie to **192.168.56.101**.

9. Teraz można zalogować się na maszynę z konsoli systemu gospodarza: **ssh msfadmin@192.168.56.101** lub uzyskać dostęp do działających aplikacji internetowych poprzez przeglądarkę (adres URL: **http://192.168.56.101**).

