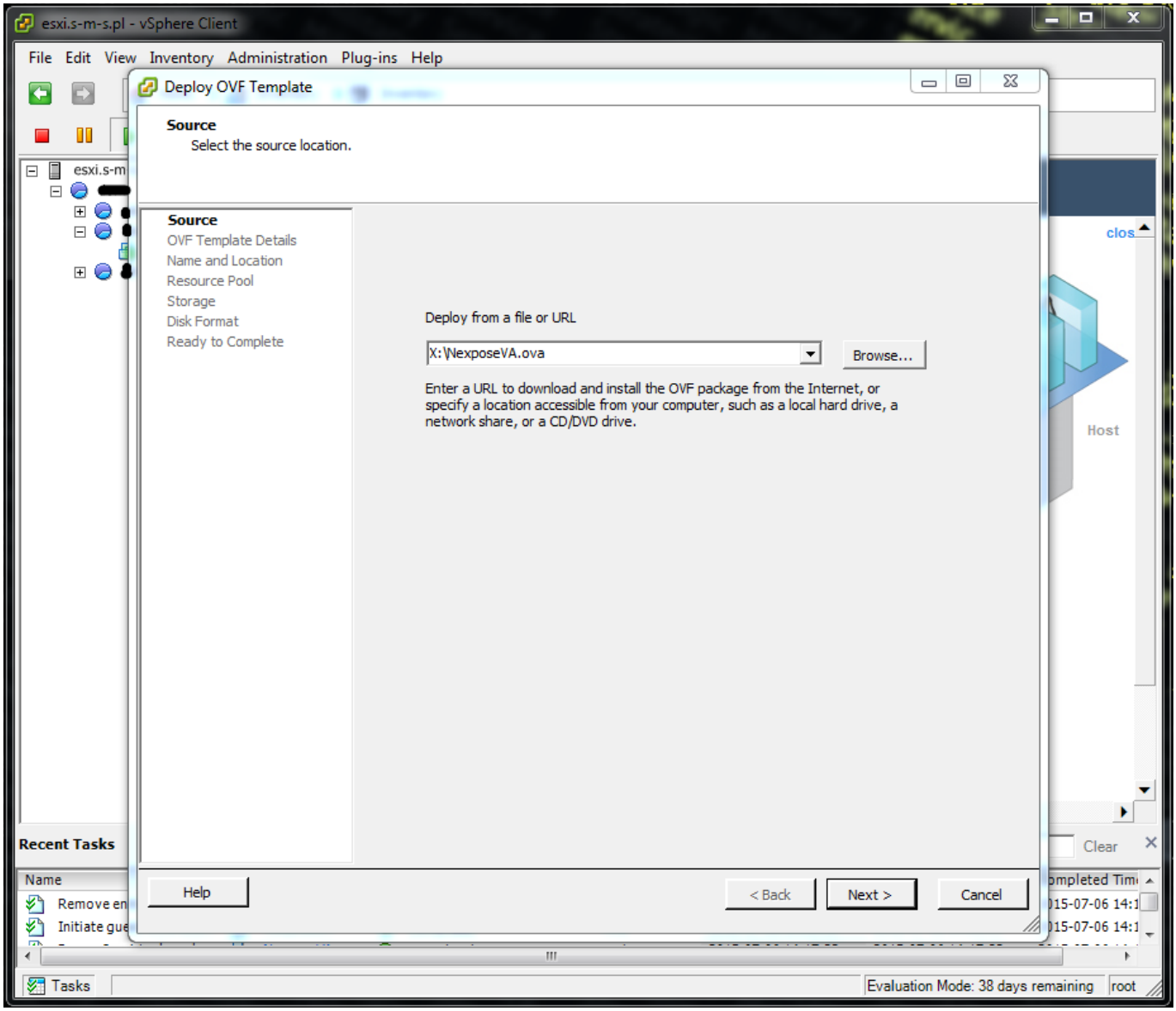
Po krótkiej przerwie powracamy do pisania postów i z tej okazji postanowiłem wypuścić kolejny – drugi – odcinek serii o zarządzaniu podatnościami. Dziś postaram się przekazać Wam jak poprawnie skonfigurować skaner podatności Nexpose.

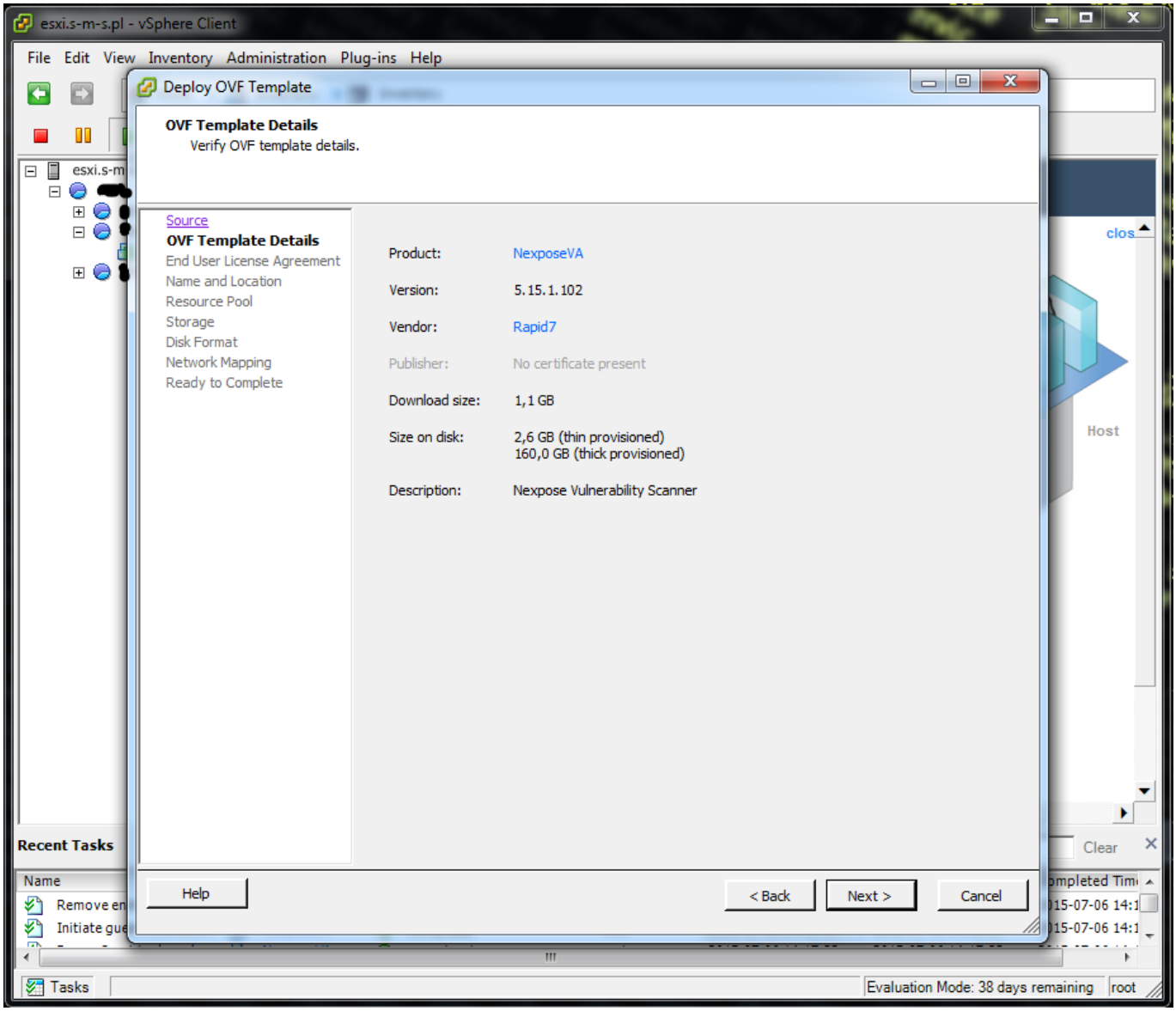
Przedstawię dzisiaj instalację i konfigurację za pomocą pliku .ovf, czyli wirtualnej maszyny przygotowanej do instalacji na serwerze wirtualizacji, oraz manualnej instalacji Nexpose na wcześniej przygotowanym systemie operacyjnym. Artykuł zawiera dużą ilość screenów, które maja charakter poglądowy i w większości nie wymagają komentarza.

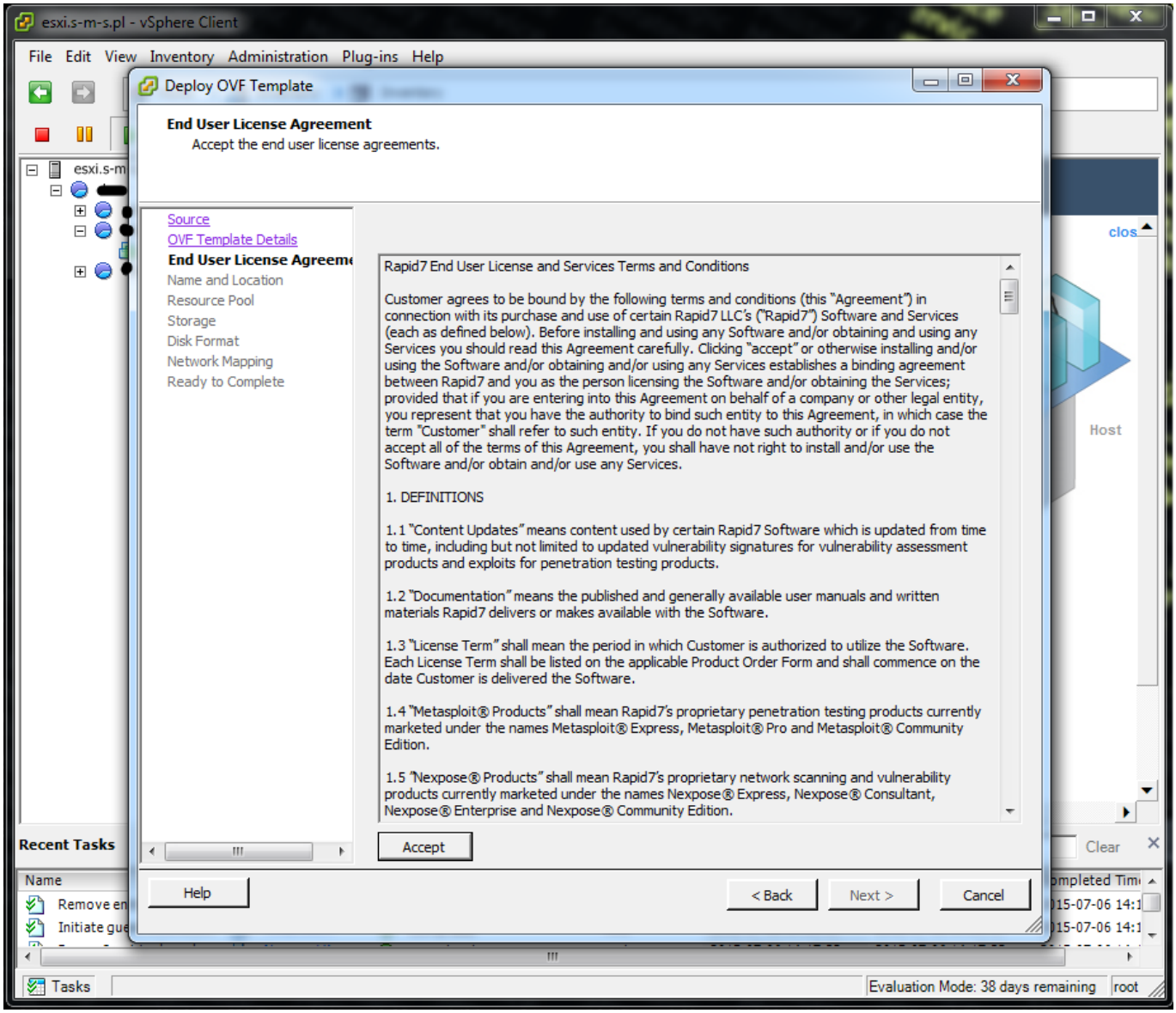
Instalacja z gotowego obrazu .ova.

Do wirtualizacji użyję serwera ESXi w wersji 5.5.

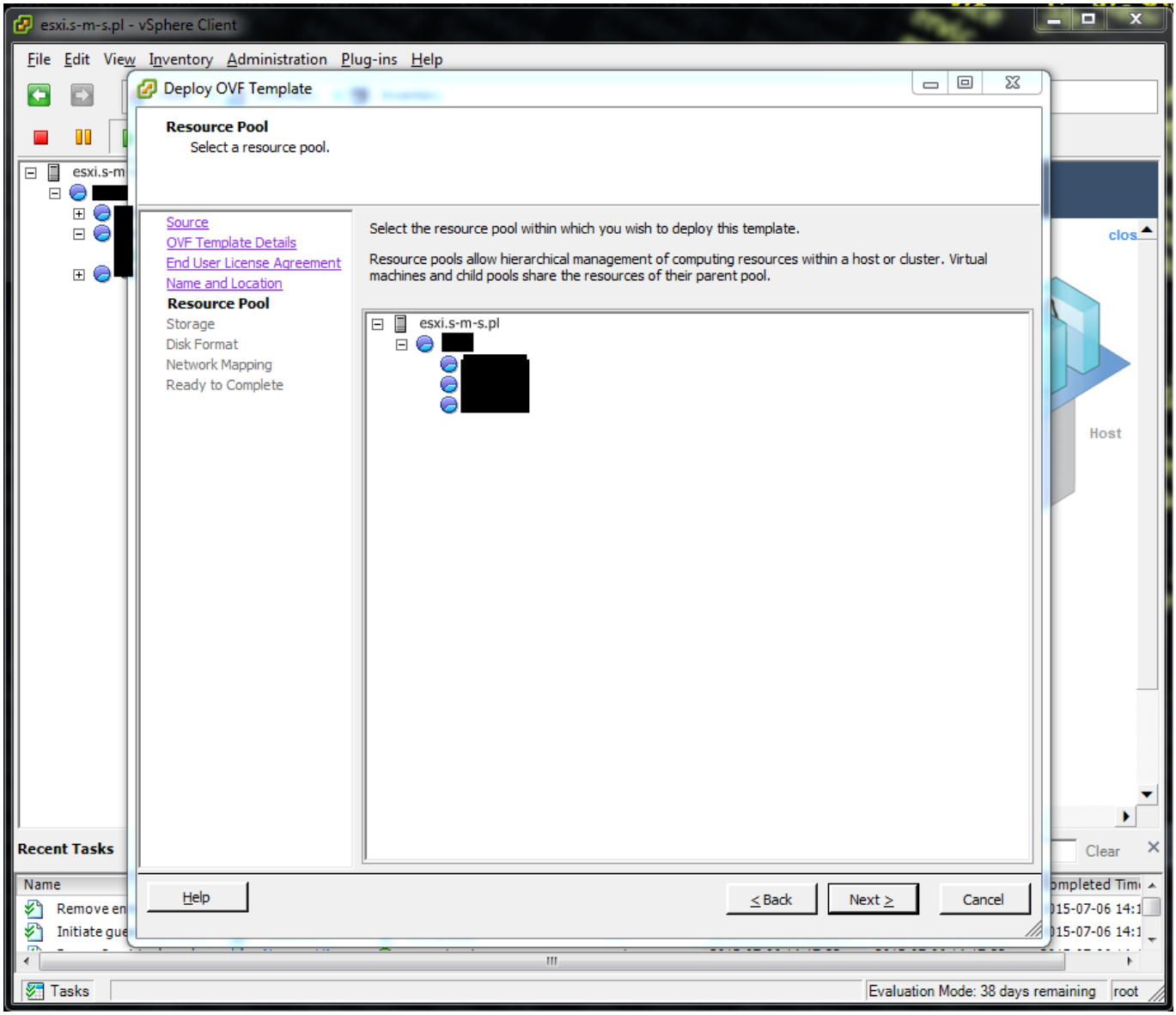


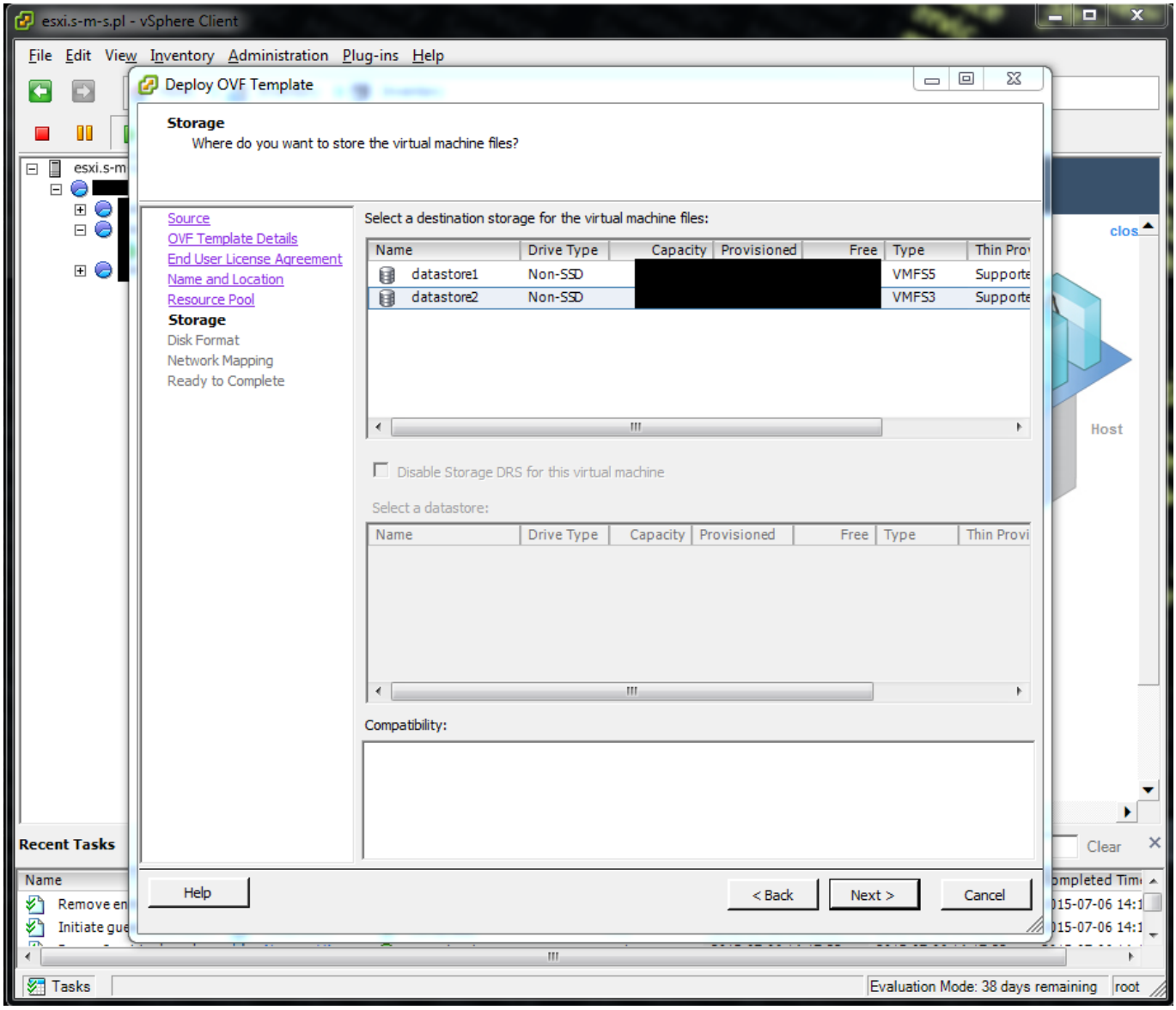
Pierwszym co musimy zrobić to wczytać obraz maszyny wirtualnej pobranej ze strony Rapid7.

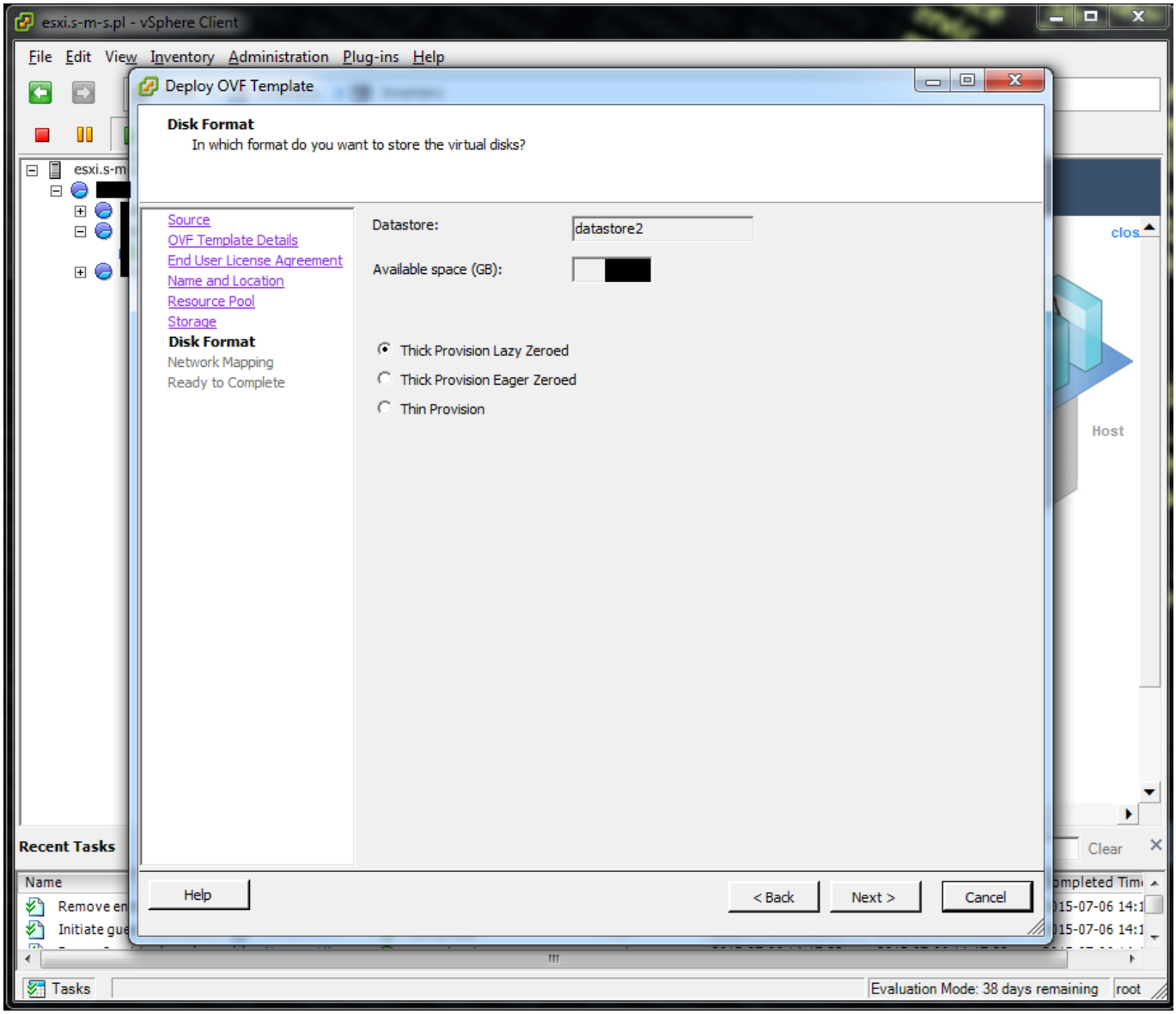

esxi.s-m-s.pl - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Deploy OVF Template
OVF Template Details
Verify OVF template details.
Source
OVF Template Details
End User License Agreement
Name and Location
Resource Pool
Storage
Disk Format
Network Mapping
Ready to Complete
Product: NexposeVA
Version: 5.15.1.102
Vendor: Rapid7
Publisher: No certificate present
Download size: 1,1 GB
Size on disk: 2,6 GB (thin provisioned)
160,0 GB (thick provisioned)
Description: Nexpose Vulnerability Scanner
Help
< Back
Next >
Cancel
Recent Tasks
Name
Tasks
Evaluation Mode: 38 days remaining
root

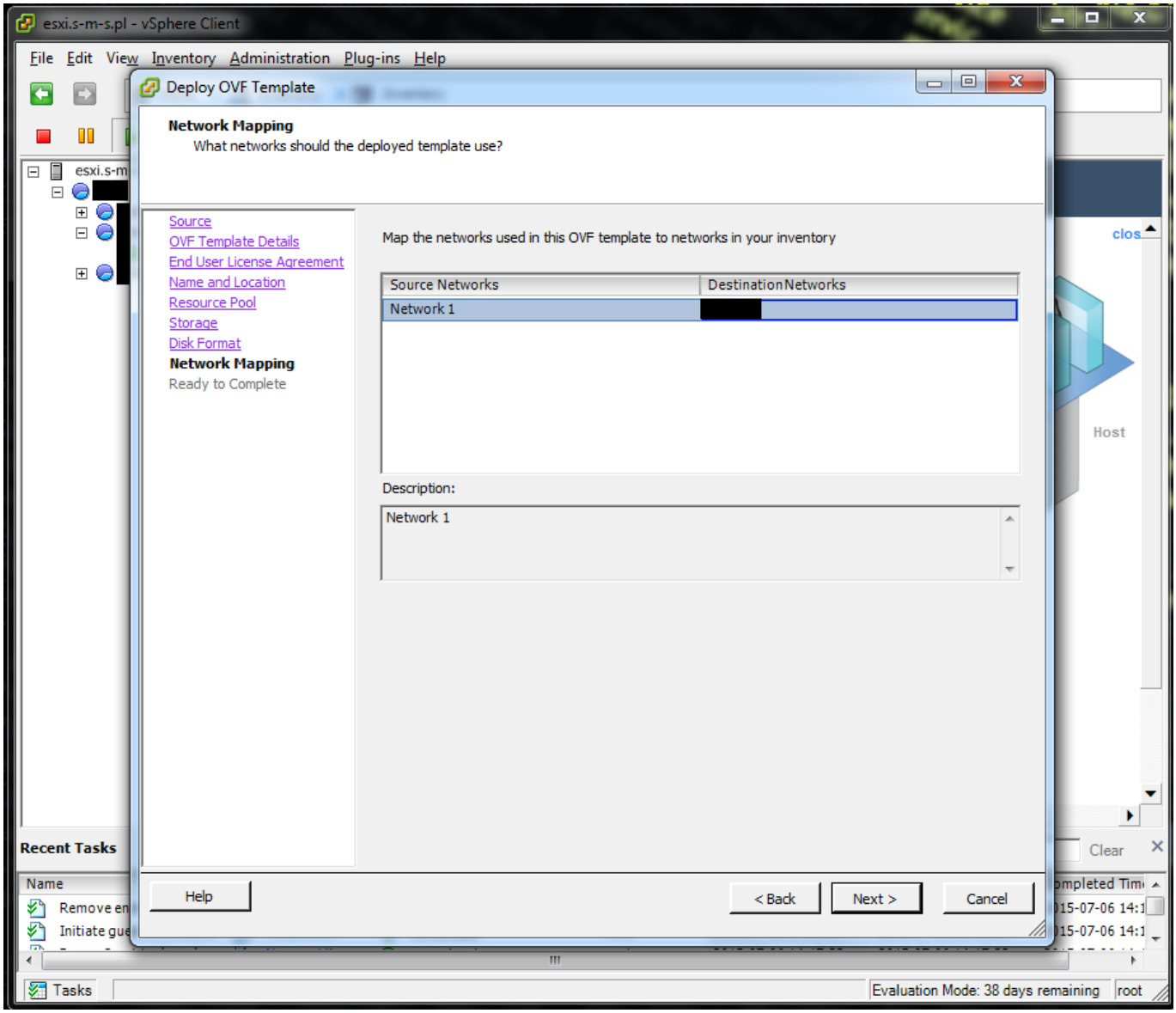


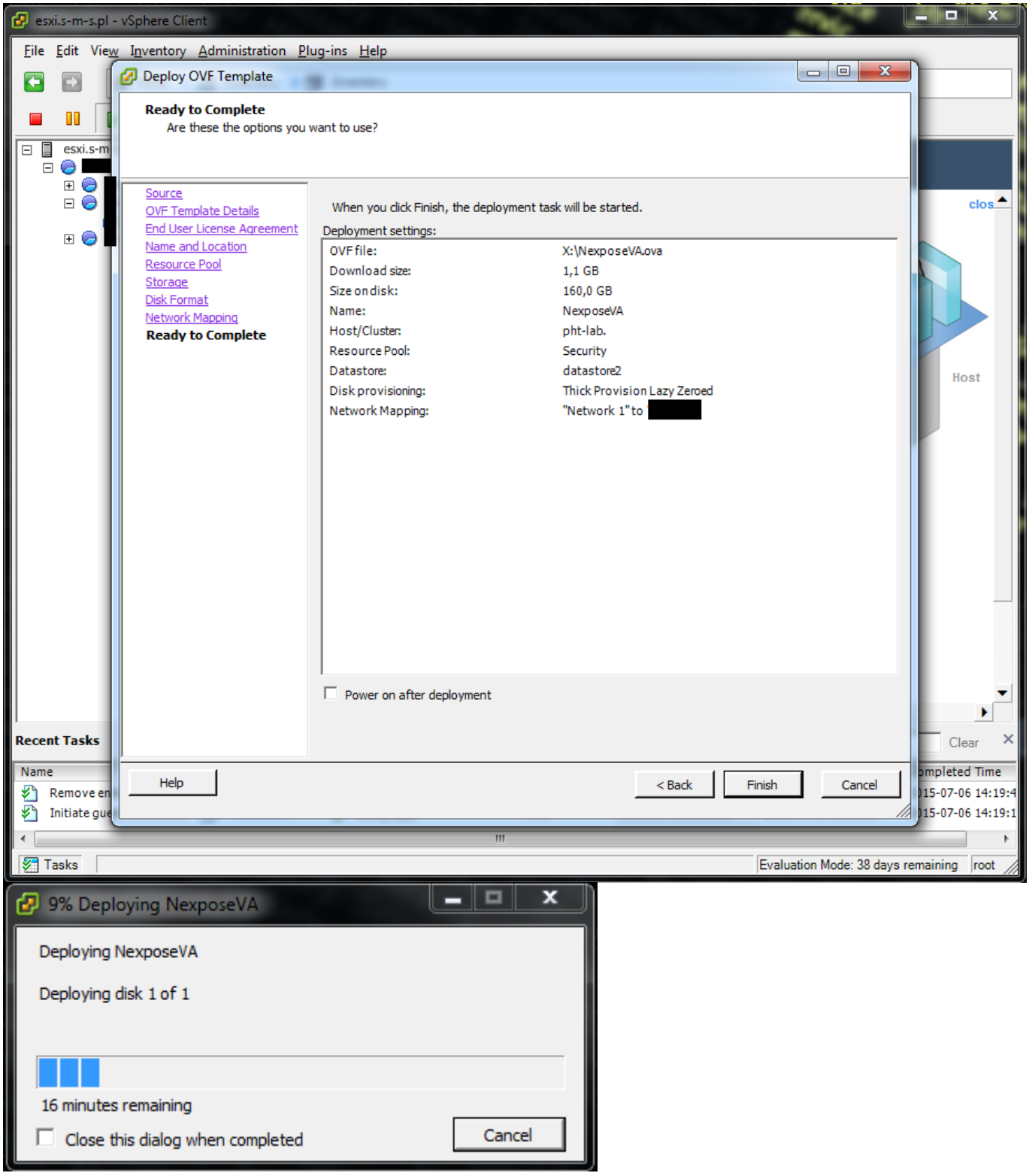
Zapoznajemy się z EULA i akceptujemy postanowienia licencji.

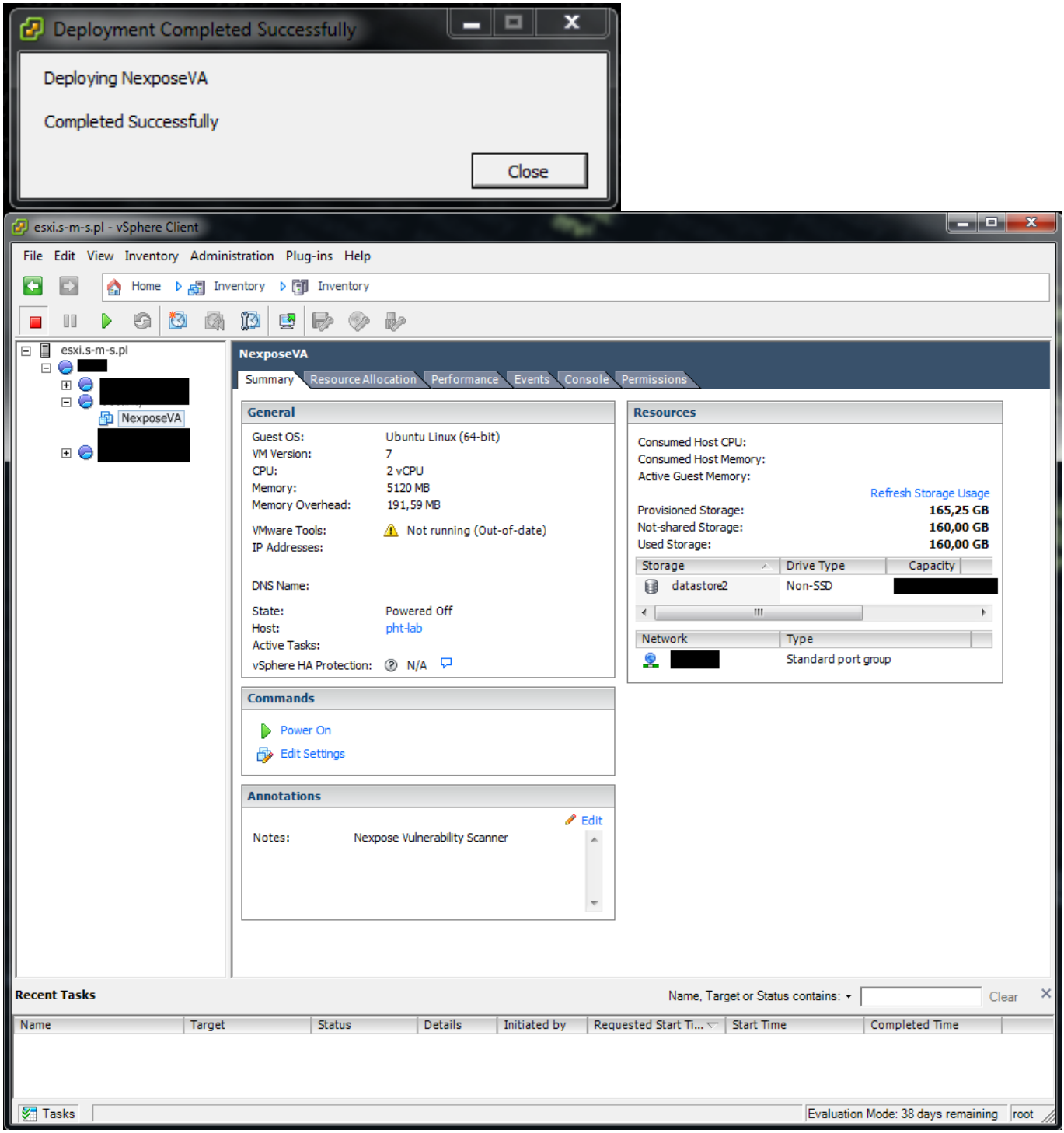

esxi.s-m-s.pl - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Deploy OVF Template
Resource Pool
Select a resource pool.
Source
OVF Template Details
End User License Agreement
Name and Location
Resource Pool
Storage
Disk Format
Network Mapping
Ready to Complete
Select the resource pool within which you wish to deploy this template.
Resource pools allow hierarchical management of computing resources within a host or cluster. Virtual machines and child pools share the resources of their parent pool.
esxi.s-m-s.pl
Help
< Back
Next >
Cancel
Recent Tasks
Name
Clear
Tasks
Evaluation Mode: 38 days remaining
root


esxi.s-m-s.pl - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Deploy OVF Template
Storage
Where do you want to store the virtual machine files?
Source
OVF Template Details
End User License Agreement
Name and Location
Resource Pool
Storage
Disk Format
Network Mapping
Ready to Complete
Select a destination storage for the virtual machine files:
Name
Drive Type
Capacity
Provisioned
Free
Type
Thin Prov
datastore1
Non-SSD
VMFS5
Supporte
datastore2
Non-SSD
VMFS3
Supporte
Disable Storage DRS for this virtual machine
Select a datastore:
Compatibility:
Help
< Back
Next >
Cancel
Recent Tasks
Name
Clear
Host
Tasks
Evaluation Mode: 38 days remaining
root


esxi.s-m-s.pl - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Deploy OVF Template
Disk Format
In which format do you want to store the virtual disks?
Source
OVF Template Details
End User License Agreement
Name and Location
Resource Pool
Storage
Disk Format
Network Mapping
Ready to Complete
Datastore:
datastore2
Available space (GB):
Thick Provision Lazy Zeroed
Thick Provision Eager Zeroed
Thin Provision
Help
< Back
Next >
Cancel
Recent Tasks
Name
Tasks
Evaluation Mode: 38 days remaining
root


esxi.s-m-s.pl - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Deploy OVF Template
Network Mapping
What networks should the deployed template use?
Source
OVF Template Details
End User License Agreement
Name and Location
Resource Pool
Storage
Disk Format
Network Mapping
Ready to Complete
Map the networks used in this OVF template to networks in your inventory
Source Networks
Destination Networks
Network 1
Description:
Network 1
Help
< Back
Next >
Cancel
Recent Tasks
Name
Tasks
Evaluation Mode: 38 days remaining
root

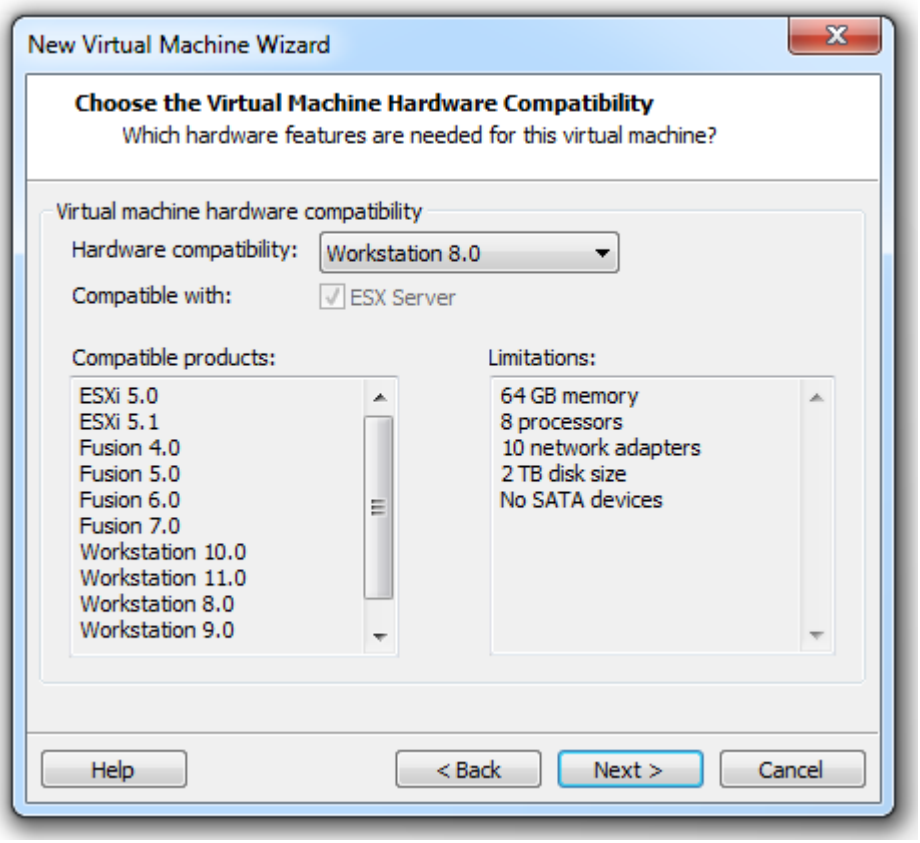

esxi.s-m-s.pl - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Deploy OVF Template
Ready to Complete
Are these the options you want to use?
Source
OVF Template Details
End User License Agreement
Name and Location
Resource Pool
Storage
Disk Format
Network Mapping
Ready to Complete
When you click Finish, the deployment task will be started.
Deployment settings:
OVF file: X:\NexposeVA.ova
Download size: 1,1 GB
Size on disk: 160,0 GB
Name: NexposeVA
Host/Cluster: pht-lab.
Resource Pool: Security
Datastore: datastore2
Disk provisioning: Thick Provision Lazy Zeroed
Network Mapping: "Network 1" to [redacted]
Power on after deployment
Help
< Back
Finish
Cancel
Recent Tasks
Name
Tasks
Evaluation Mode: 38 days remaining
root
9% Deploying NexposeVA
Deploying NexposeVA
Deploying disk 1 of 1
16 minutes remaining
Close this dialog when completed
Cancel


Deployment Completed Successfully
Deploying NexposeVA
Completed Successfully
Close
esxi.s-m-s.pl - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Inventory
esxi.s-m-s.pl
NexposeVA
NexposeVA
Summary Resource Allocation Performance Events Console Permissions
General
Guest OS: Ubuntu Linux (64-bit)
VM Version: 7
CPU: 2 vCPU
Memory: 5120 MB
Memory Overhead: 191,59 MB
VMware Tools: Not running (Out-of-date)
IP Addresses:
DNS Name:
State: Powered Off
Host: pht-lab
Active Tasks:
vSphere HA Protection: N/A
Resources
Consumed Host CPU:
Consumed Host Memory:
Active Guest Memory:
Refresh Storage Usage
Provisioned Storage: 165,25 GB
Not-shared Storage: 160,00 GB
Used Storage: 160,00 GB
Storage Drive Type Capacity
datastore2 Non-SSD
Network Type
Standard port group
Commands
Power On
Edit Settings
Annotations
Edit
Notes: Nexpose Vulnerability Scanner
Recent Tasks
Name, Target or Status contains:
Clear
Name Target Status Details Initiated by Requested Start Ti... Start Time Completed Time
Tasks
Evaluation Mode: 38 days remaining
root

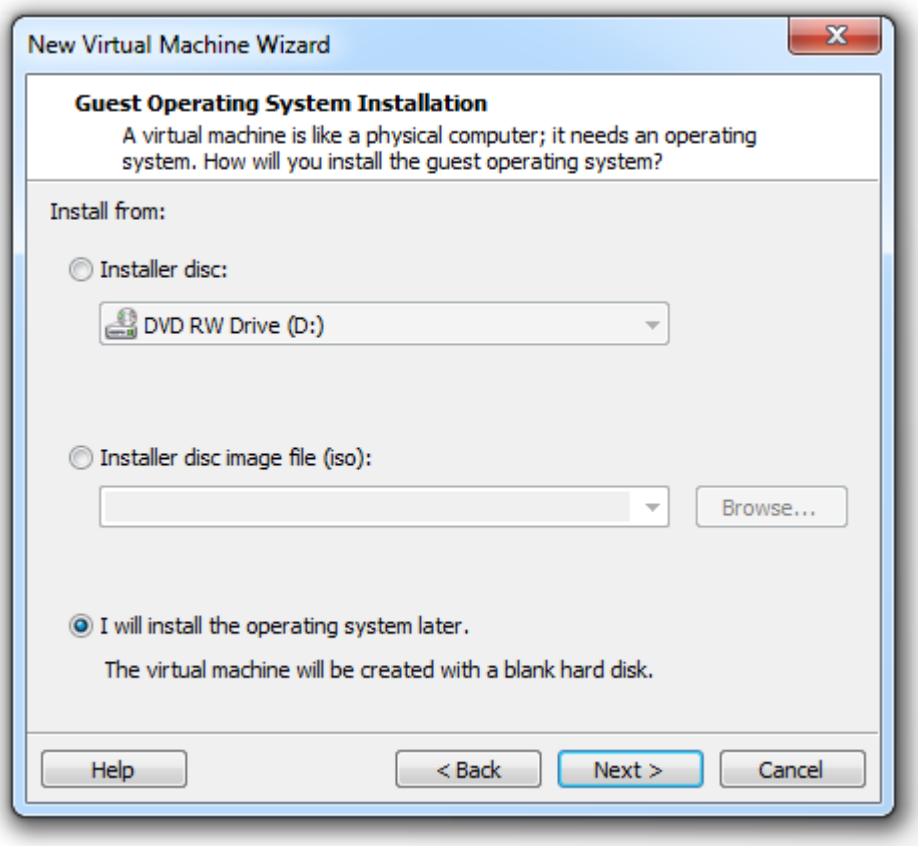
Instalacja manualna z pliku binarnego.

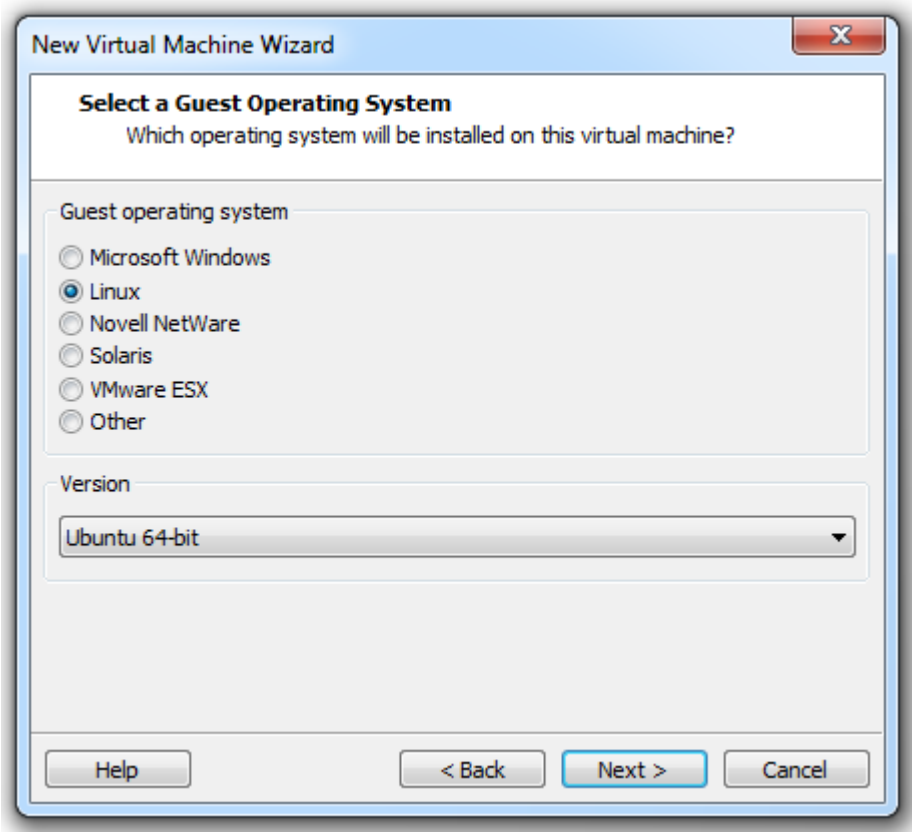
Przygotowanie wirtualnej maszyny.

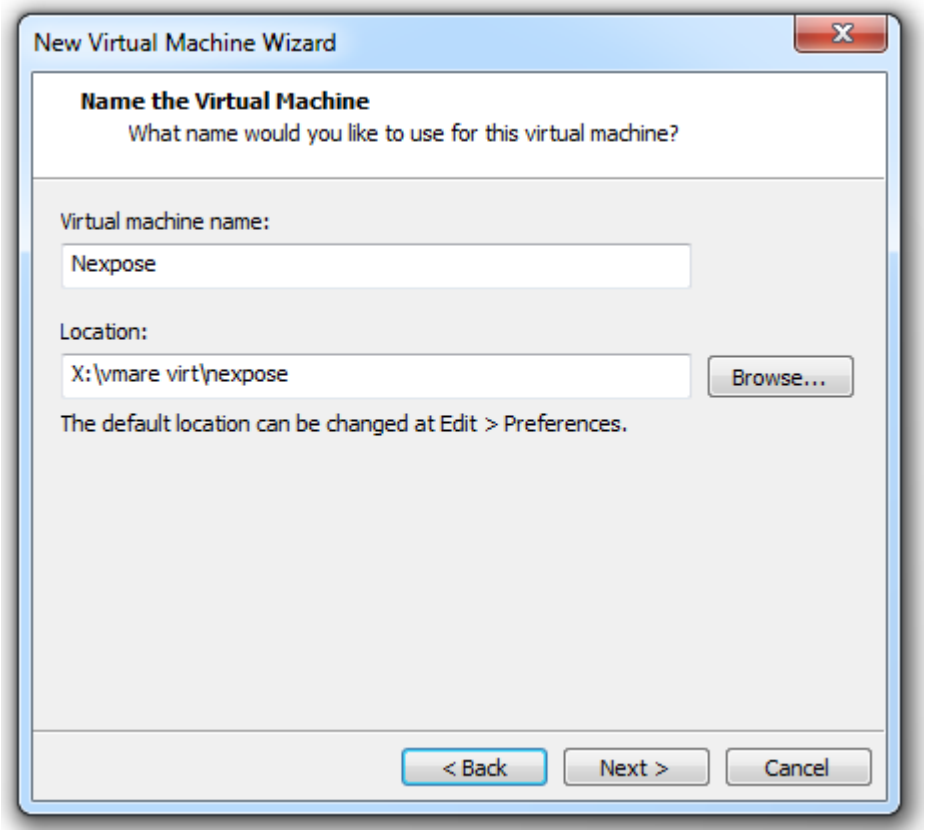
Alternatywą dla tego sposobu jest ręczna instalacja. Pierwszym co musimy zrobić to utworzenie nowej maszyny, lub wykorzystanie fizycznej maszyny i instalacja jednego z wspieranych systemów operacyjnych. Listę systemów wymieniliśmy tutaj. Wybraliśmy Ubuntu w wersji 14.04. Poniżej procedura przygotowania maszyny w VMware Workstation. Zalecamy przy tworzeniu maszyny wybranie opcji „Custom”.

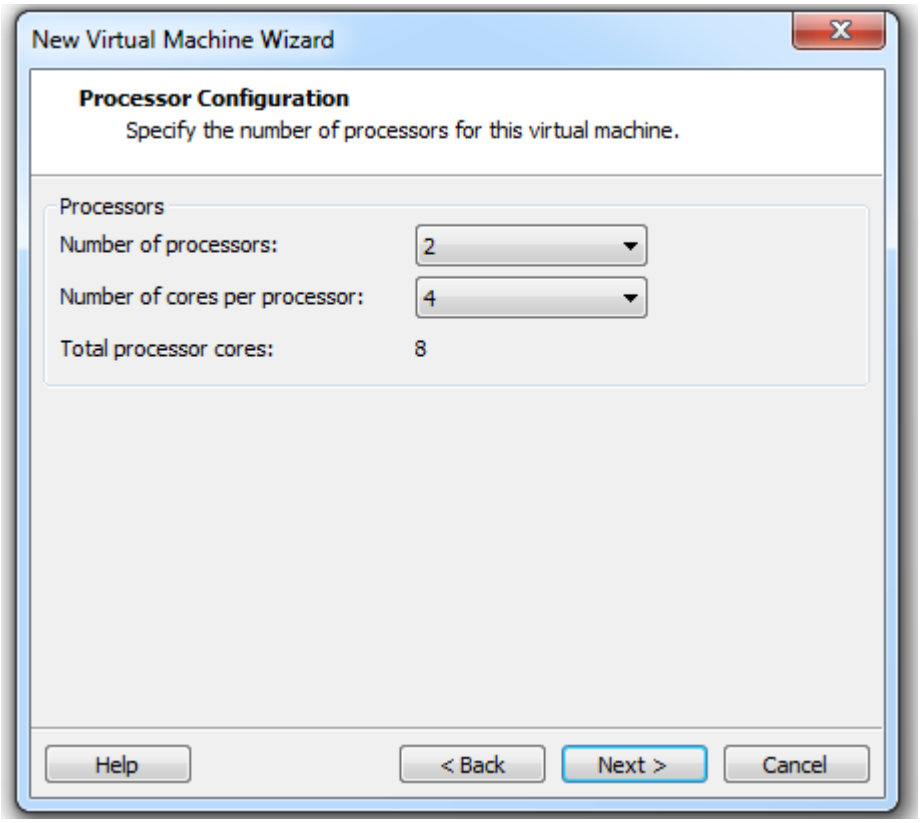


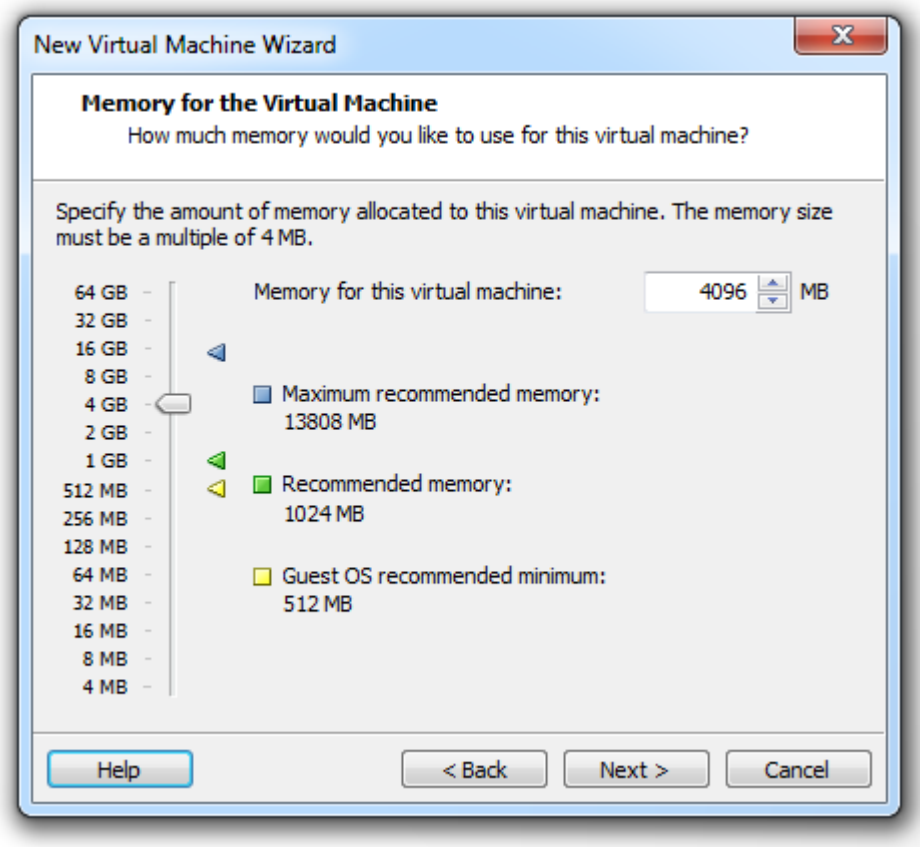
Wybieramy wersje Workstation 8.0, tak by przygotowany przez nas obraz mógł być wczytany do serwera wirtualizacji ESXi.


New Virtual Machine Wizard
Guest Operating System Installation
A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?
Install from:
Installer disc:
DVD RW Drive (D:)
Installer disc image file (iso):
Browse...
I will install the operating system later.
The virtual machine will be created with a blank hard disk.
Help
< Back
Next >
Cancel

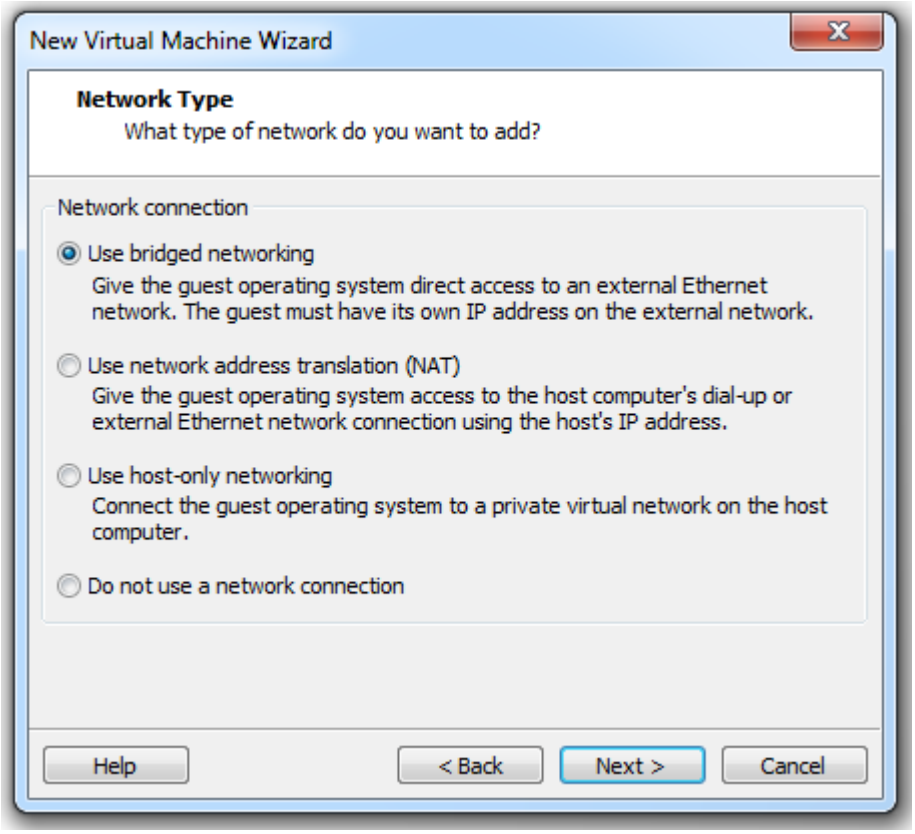

New Virtual Machine Wizard
Select a Guest Operating System
Which operating system will be installed on this virtual machine?
Guest operating system
Microsoft Windows
Linux
Novell NetWare
Solaris
VMware ESX
Other
Version
Ubuntu 64-bit
Help
< Back
Next >
Cancel

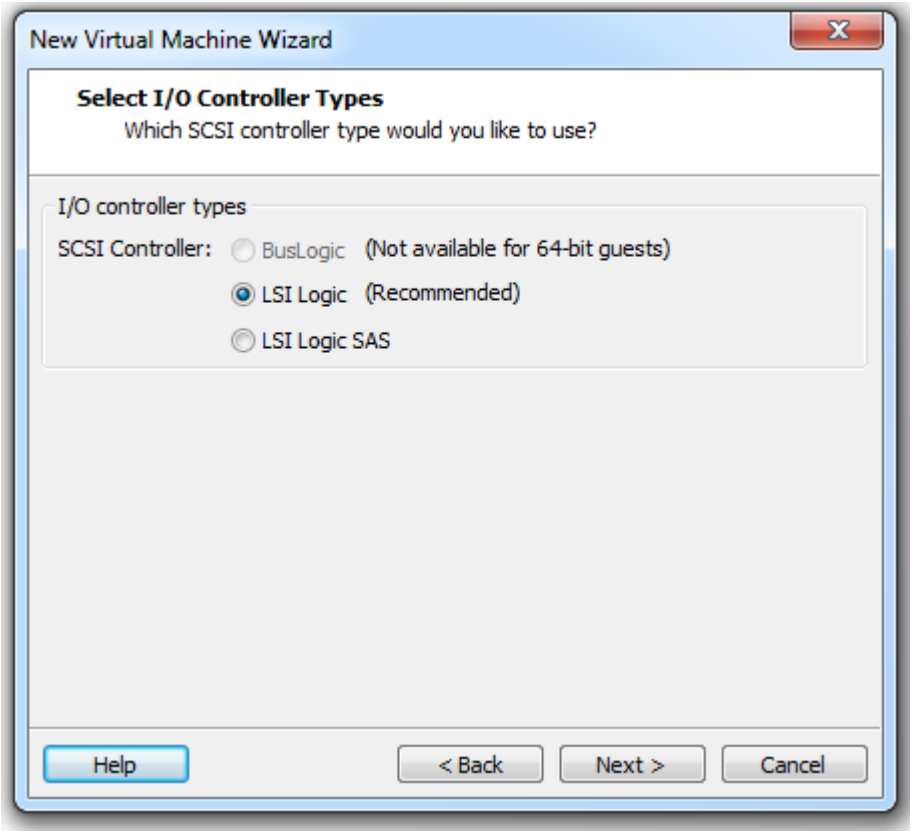

New Virtual Machine Wizard
Name the Virtual Machine
What name would you like to use for this virtual machine?
Virtual machine name:
Nexpose
Location:
X:\vmare virt\nexpose
Browse...
The default location can be changed at Edit > Preferences.
< Back
Next >
Cancel

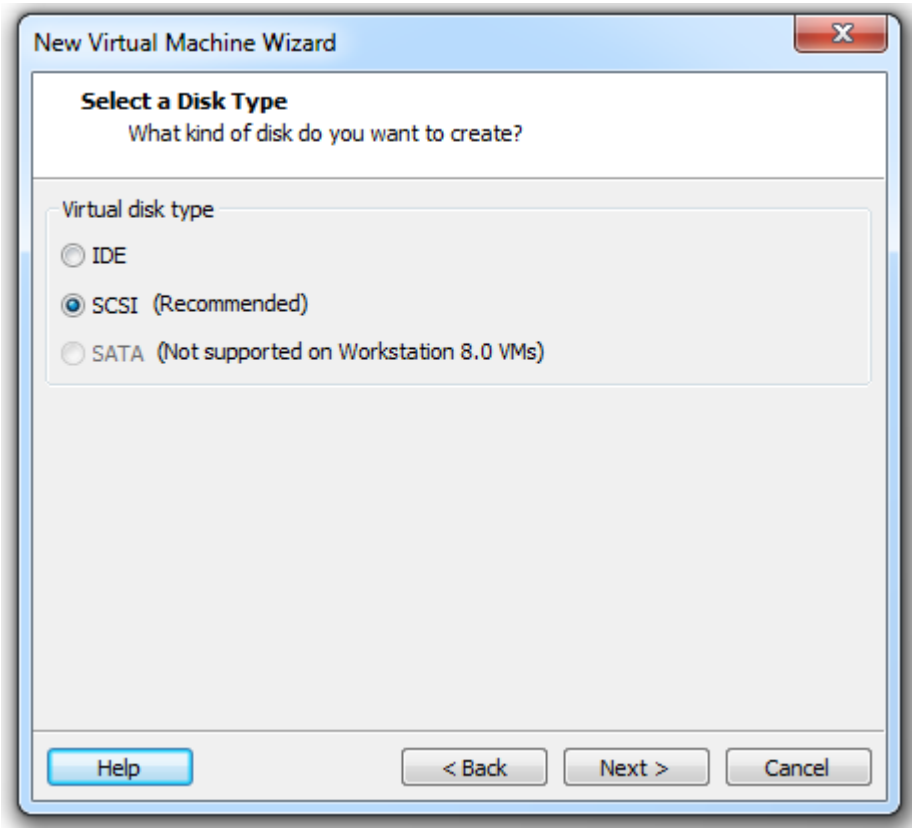

New Virtual Machine Wizard
Processor Configuration
Specify the number of processors for this virtual machine.
Processors
Number of processors:
2
Number of cores per processor:
4
Total processor cores:
8
Help
< Back
Next >
Cancel

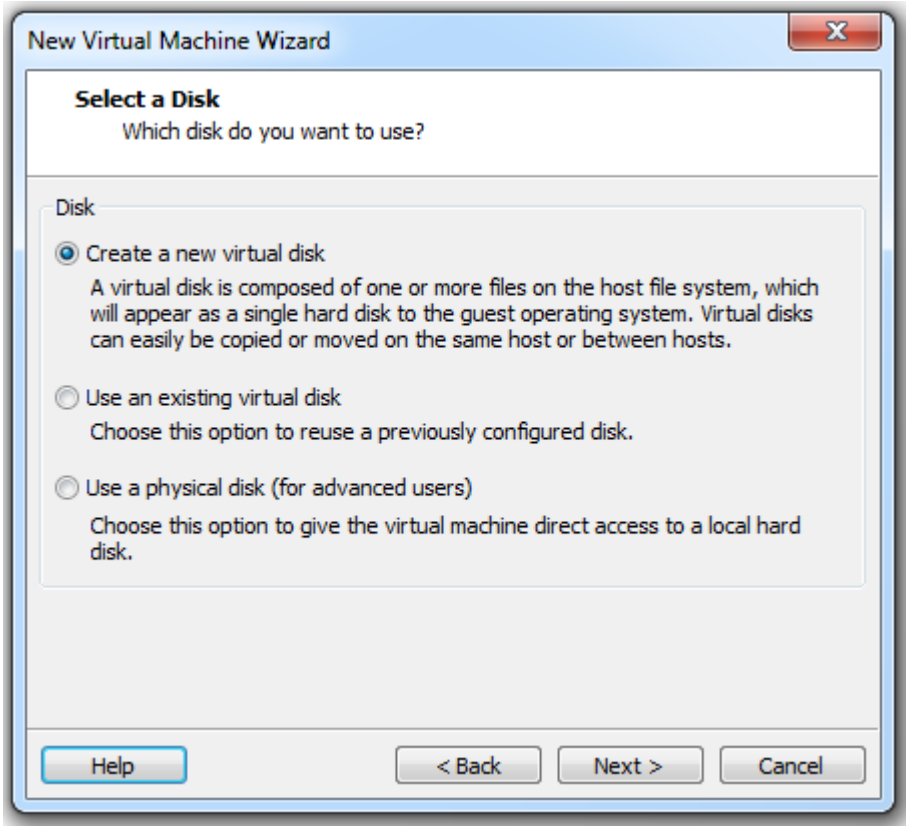


Zalecanym przez Rapid7 jest ustawienie 16 GB ramu dla nexpose, minimalnie zaś 8 GB. Spokojnie można ustawić 4 GB, skany bedą się odbywać wolniej, ale do labu w zupełności wystarczy.

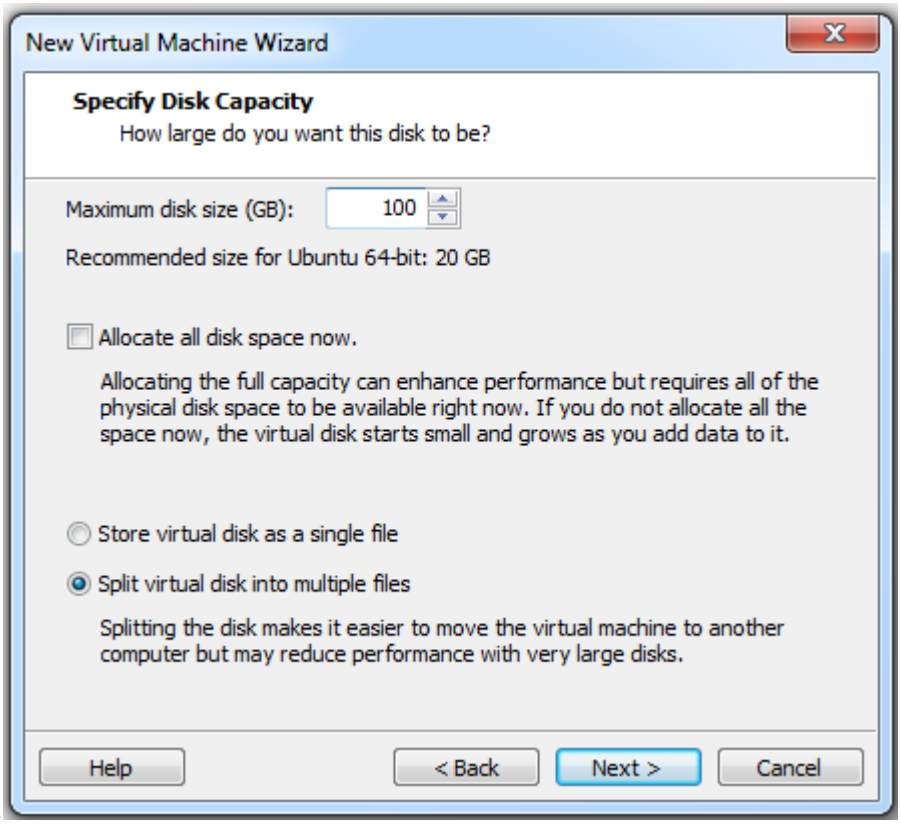

New Virtual Machine Wizard
Network Type
What type of network do you want to add?
Network connection
Use bridged networking
Give the guest operating system direct access to an external Ethernet network. The guest must have its own IP address on the external network.
Use network address translation (NAT)
Give the guest operating system access to the host computer's dial-up or external Ethernet network connection using the host's IP address.
Use host-only networking
Connect the guest operating system to a private virtual network on the host computer.
Do not use a network connection
Help
< Back
Next >
Cancel


New Virtual Machine Wizard
Select I/O Controller Types
Which SCSI controller type would you like to use?
I/O controller types
SCSI Controller:
BusLogic (Not available for 64-bit guests)
LSI Logic (Recommended)
LSI Logic SAS
Help
< Back
Next >
Cancel

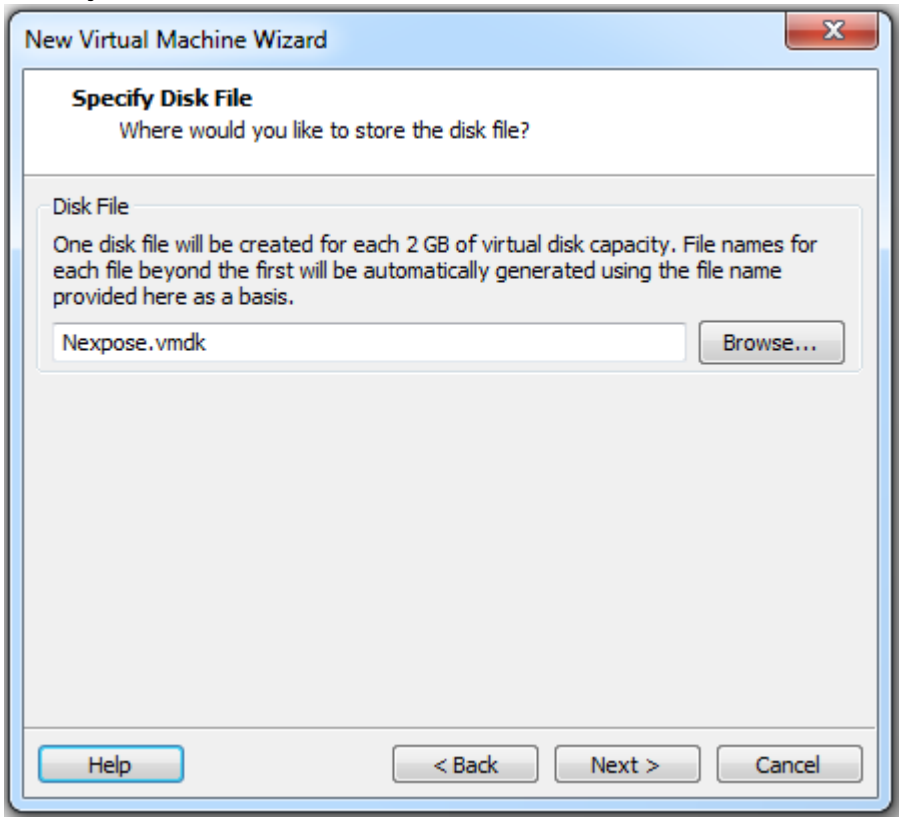

New Virtual Machine Wizard
Select a Disk Type
What kind of disk do you want to create?
Virtual disk type
IDE
SCSI (Recommended)
SATA (Not supported on Workstation 8.0 VMs)
Help
< Back
Next >
Cancel

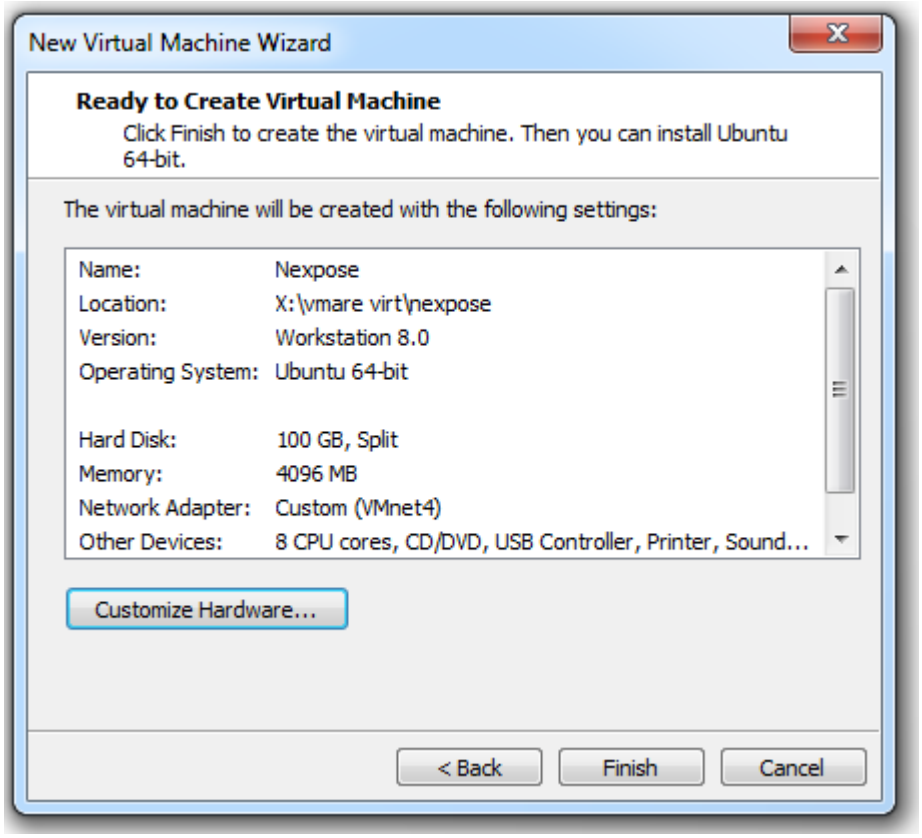


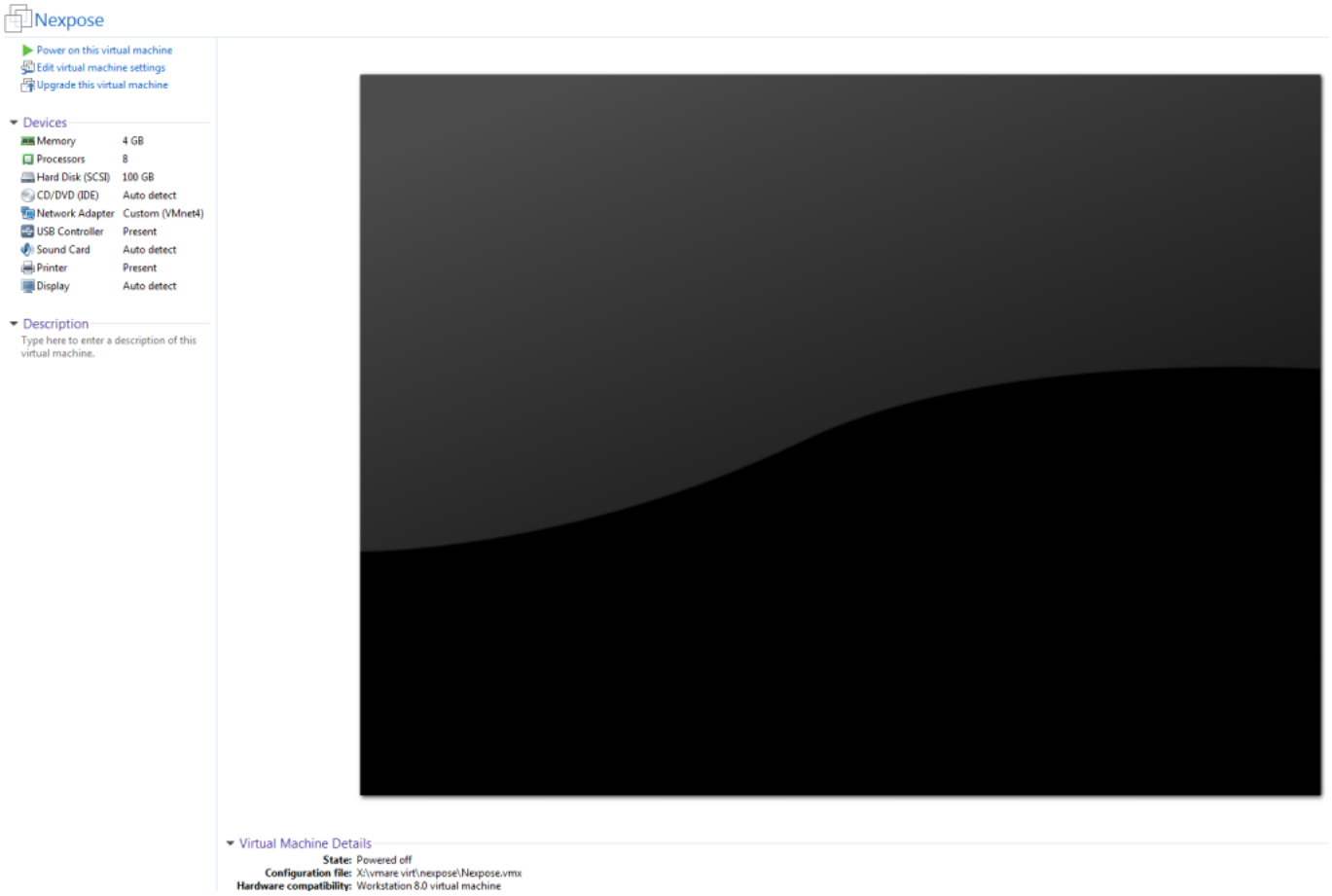
Jeżeli chodzi o przestrzeń dyskową, zalecanym jest 80+ GB, my polecamy trzymanie się



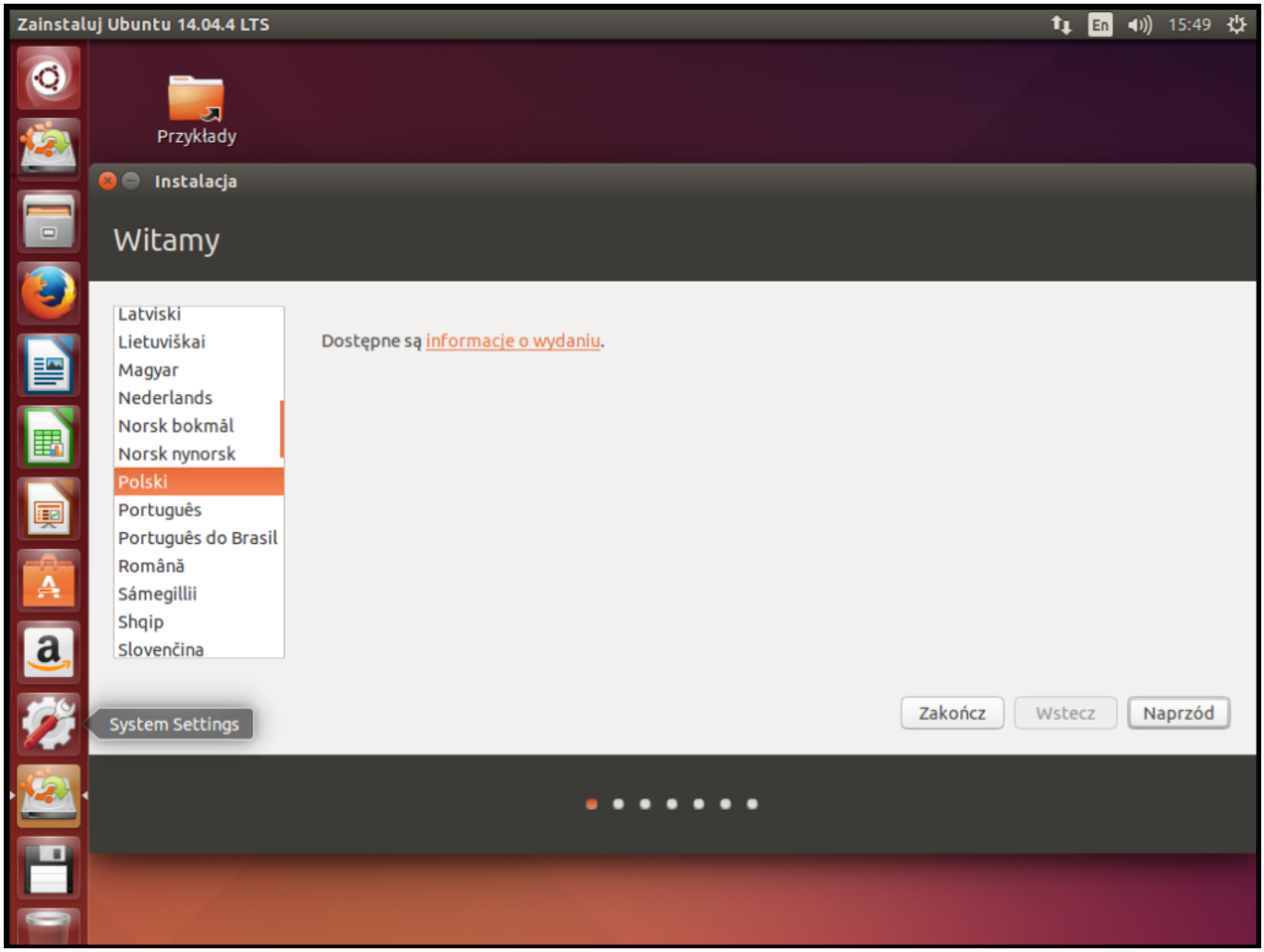
zasady 100+ GB.



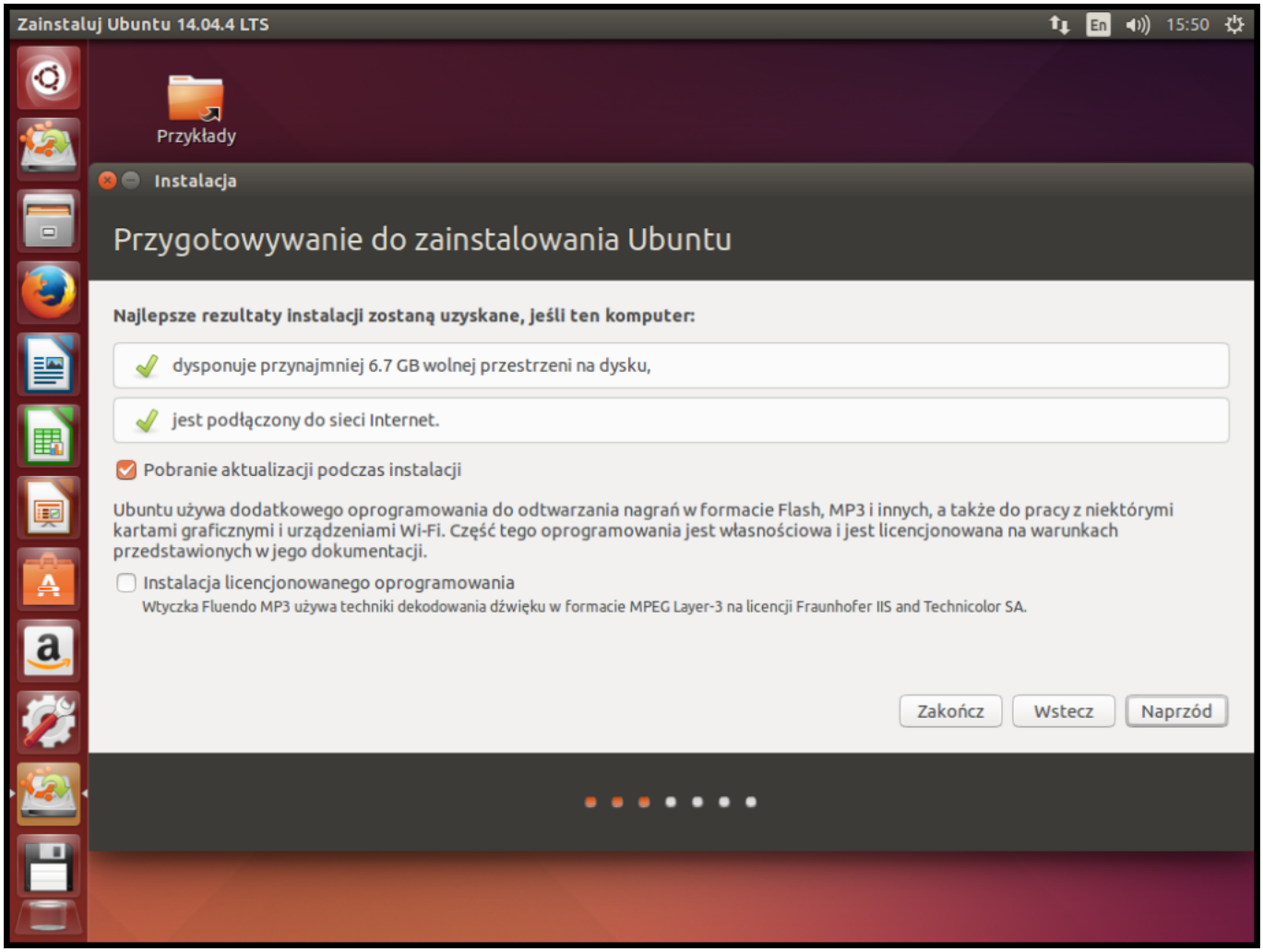

New Virtual Machine Wizard
Ready to Create Virtual Machine
Click Finish to create the virtual machine. Then you can install Ubuntu 64-bit.
The virtual machine will be created with the following settings:
Name: Nexpose
Location: X:\vmare virt\nexpose
Version: Workstation 8.0
Operating System: Ubuntu 64-bit
Hard Disk: 100 GB, Split
Memory: 4096 MB
Network Adapter: Custom (VMnet4)
Other Devices: 8 CPU cores, CD/DVD, USB Controller, Printer, Sound...
Customize Hardware...
< Back
Finish
Cancel



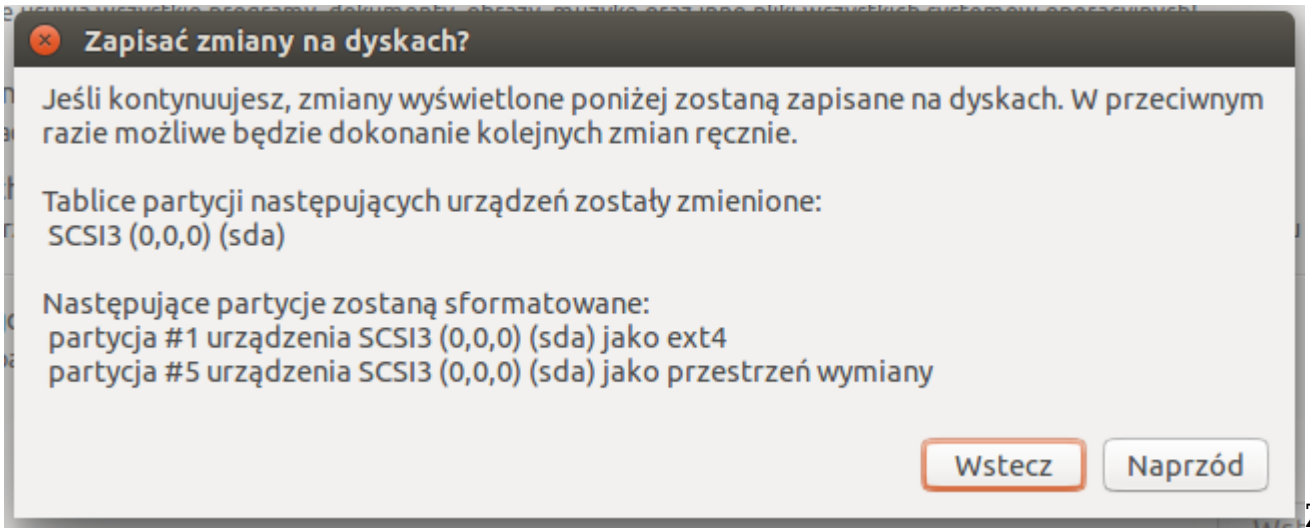
Instalacja systemu na wirtualnej maszynie.



Po przygotowaniu wirtualnej maszyny montujemy w naszym napędzie plik iso z systemem, który będziemy instalować i instalujemy.

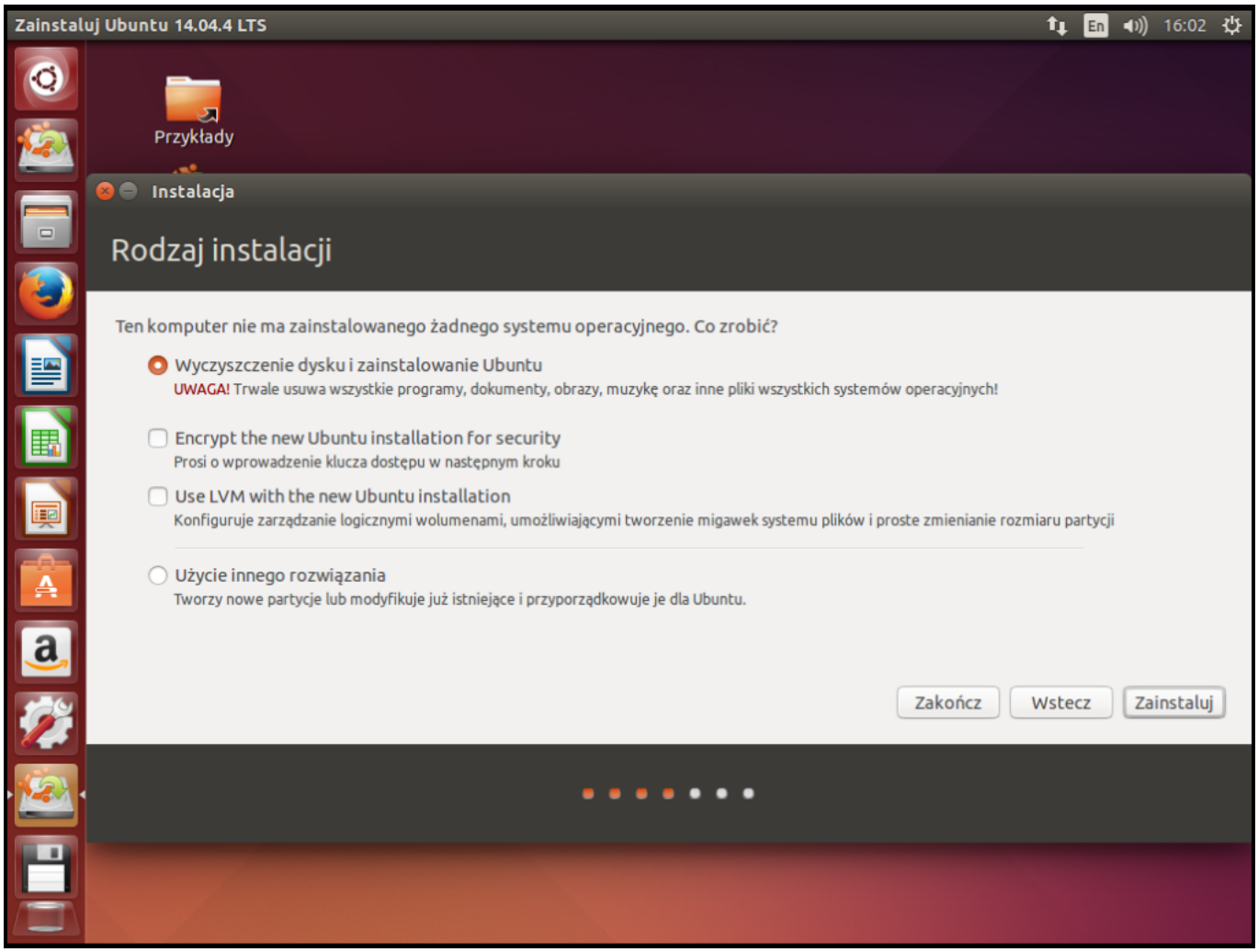


Warto pobrać przy instalacji aktualizacje dla naszego systemu.

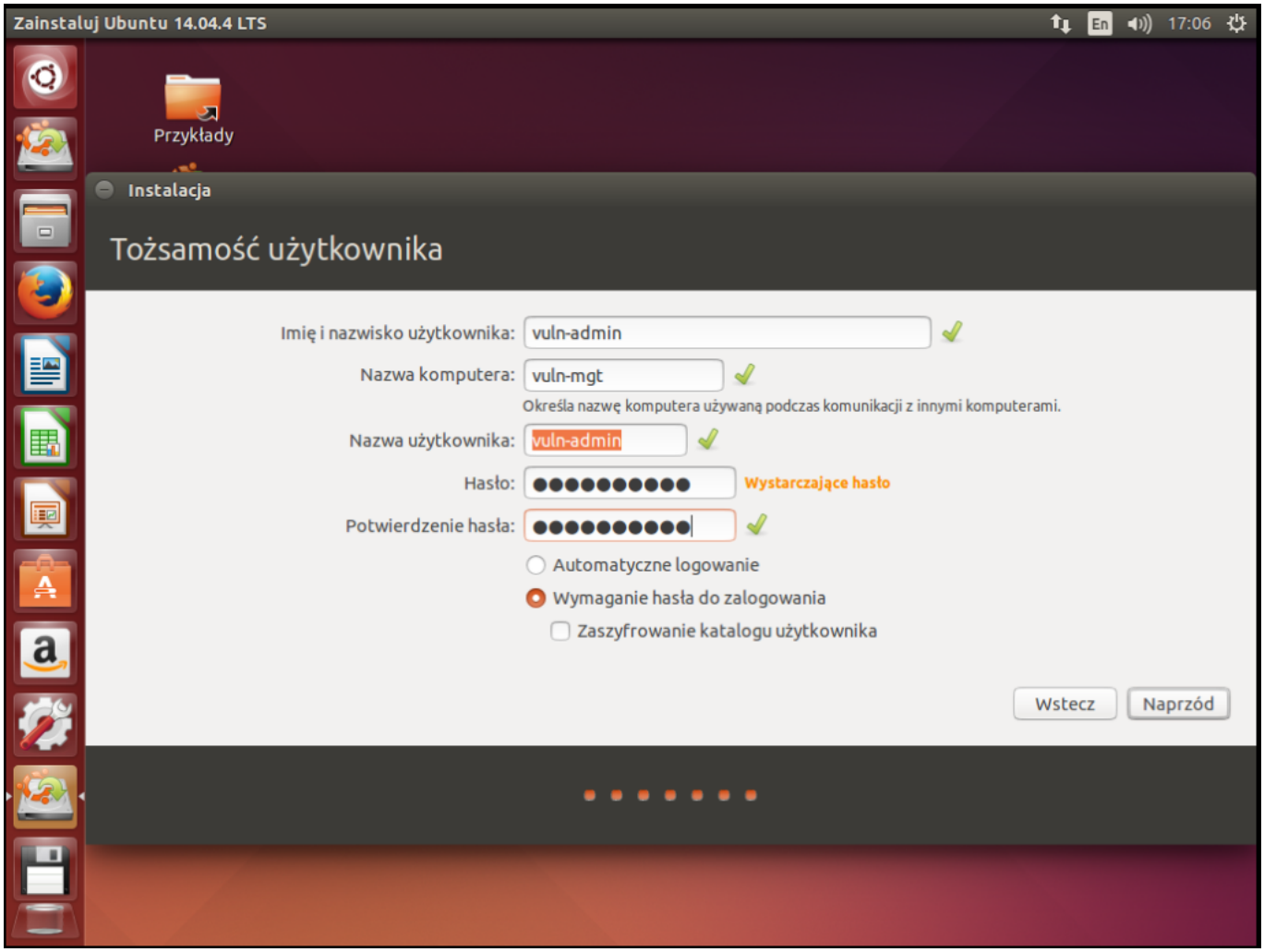


Zap

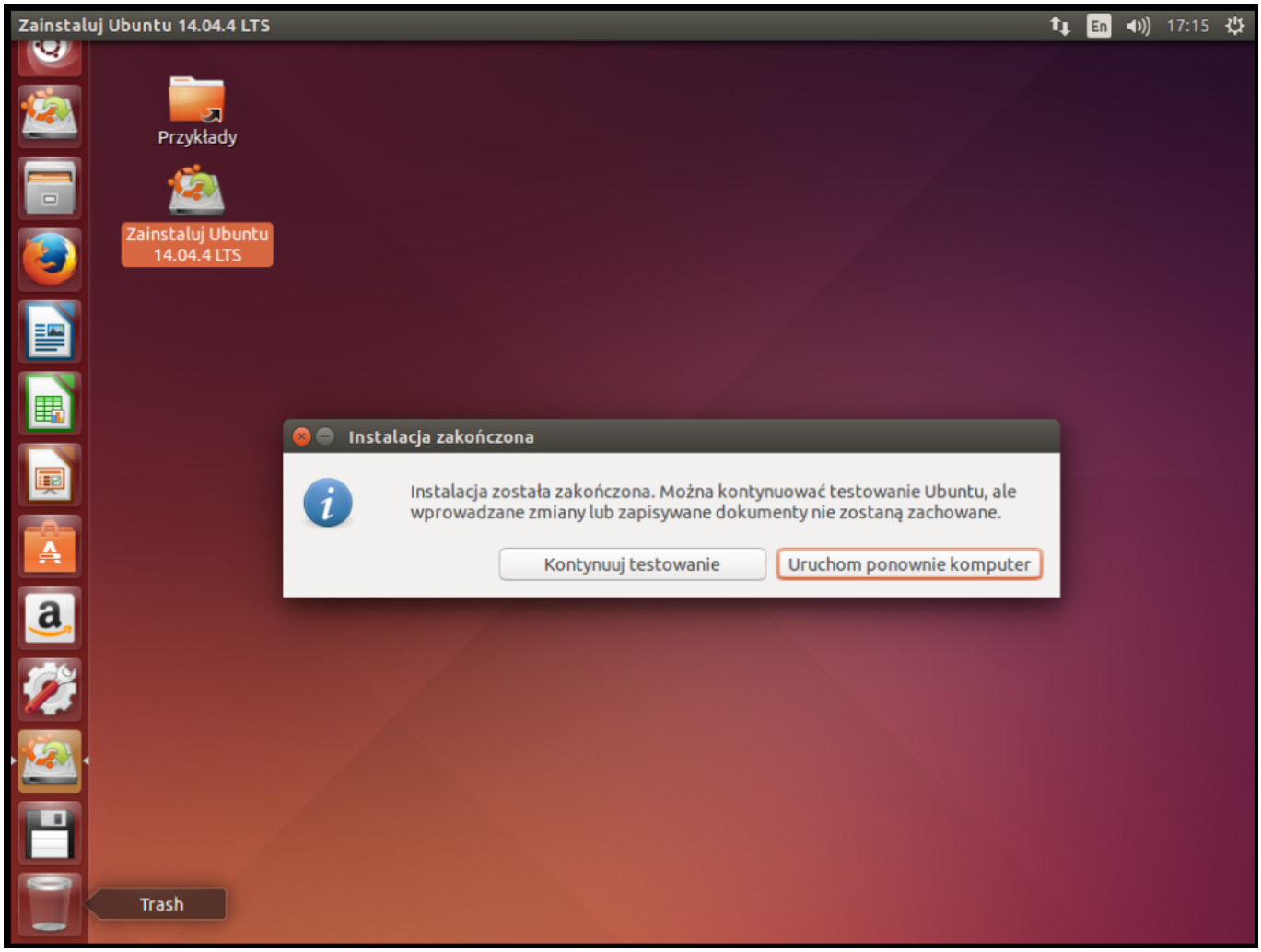
isujemy zmiany na dyskach i przechodzimy dalej.



Rozpoczynamy instalację.



W trakcie informacji zostaniemy poproszeni o utworzenie użytkownika i określenie hostname naszej maszyny.



Po zakończeniu instalacji, restartujemy maszynę i zabieramy się za instalacje Nexpose oraz konfiguracje.

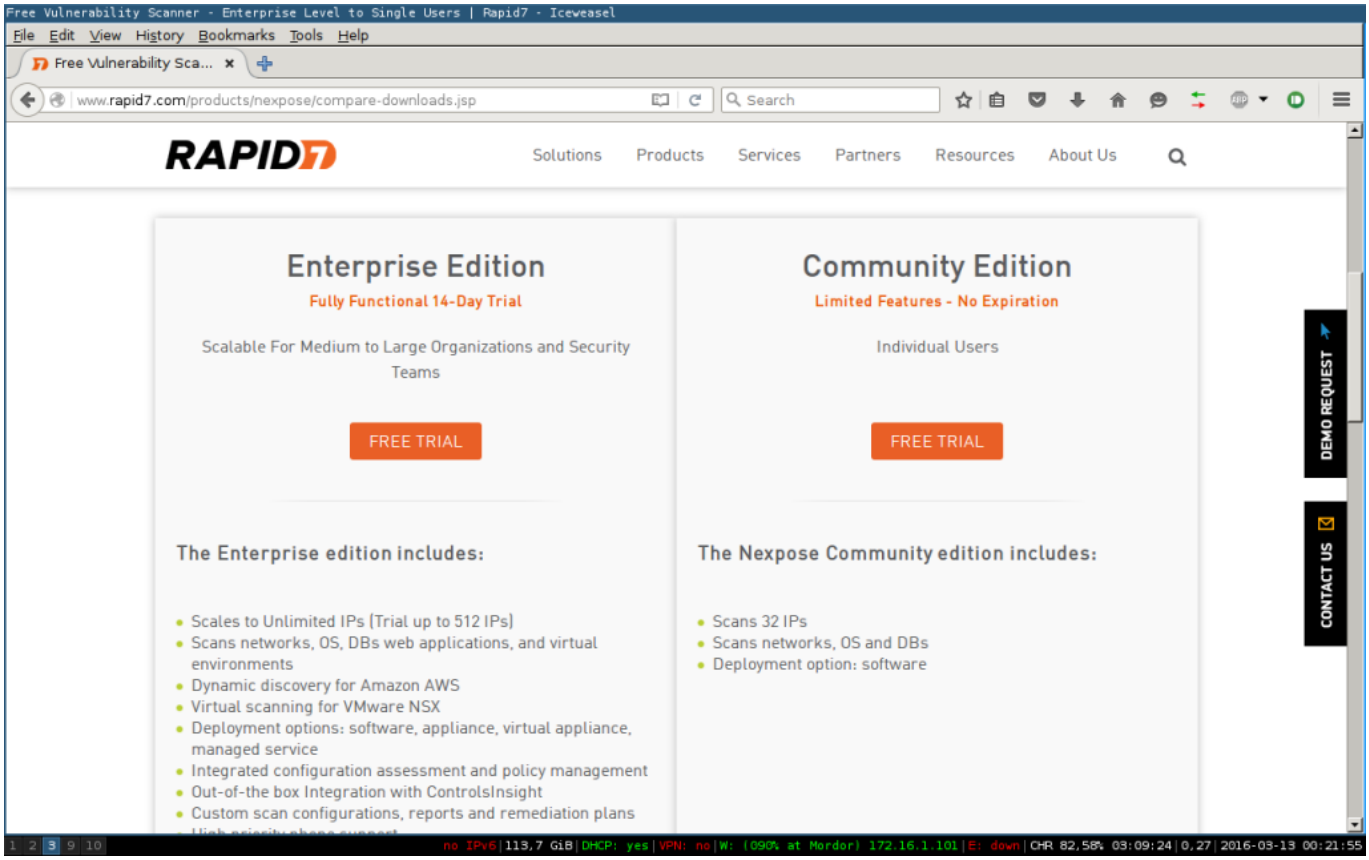
Instalacja Nexpose na wirtualnej maszynie.

Za pomocą protokołu SSH łączymy się z maszyną którą przed chwilą zainstalowaliśmy.

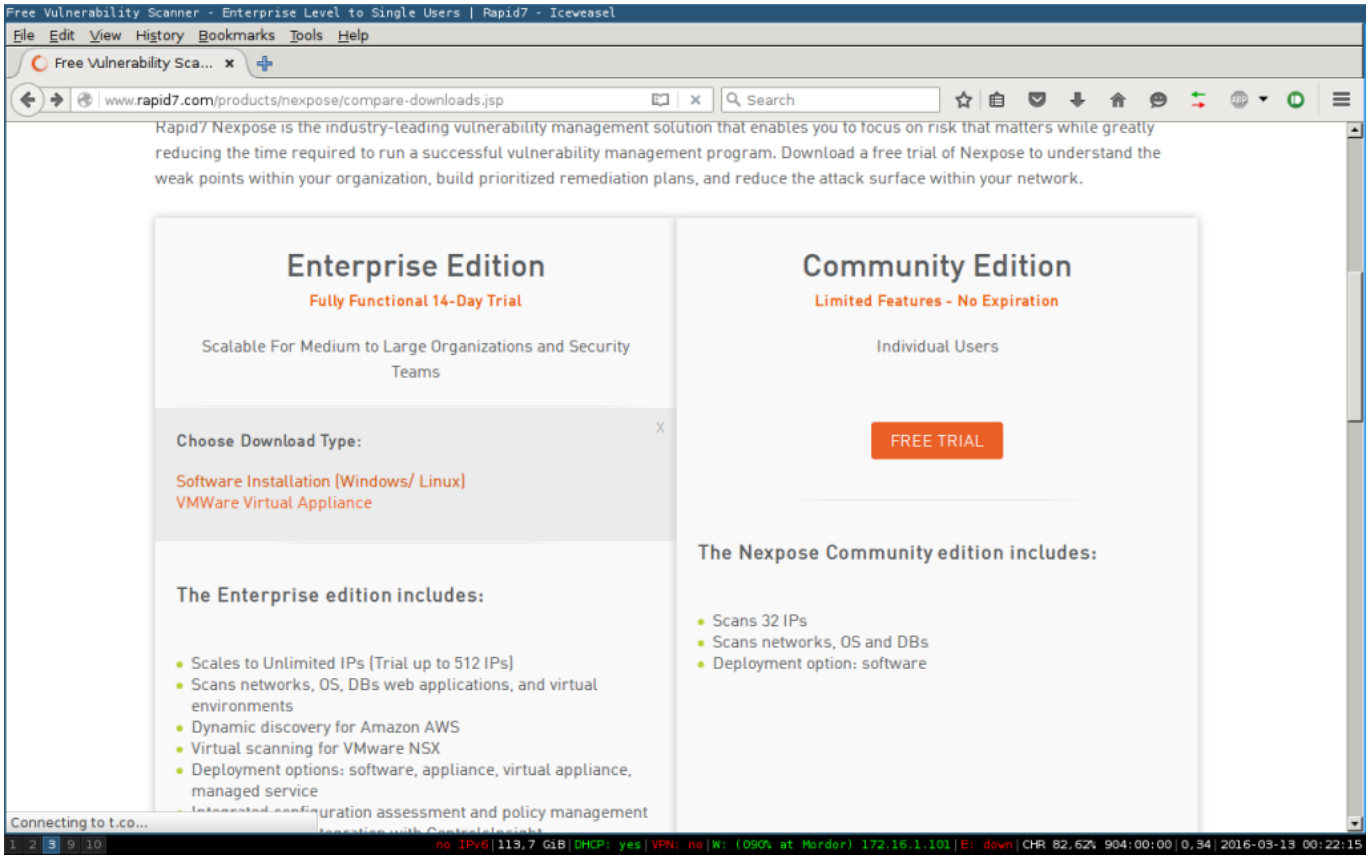
```
Plik  Edycja  Widok  Wyszukiwanie  Terminal  Pomoc
pht@dyed-fox:~$ ssh vuln-admin@nexpose.s-m-s.pl
The authenticity of host 'nexpose.s-m-s.pl (172.16.4.5)' can't be established.
ECDSA key fingerprint is SHA256:fDHM6plsaErwPgg5NEykFjgeiE47IW78kEiiZXkuflE.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'nexpose.s-m-s.pl,172.16.4.5' (ECDSA) to the list of known ho
sts.
vuln-admin@nexpose.s-m-s.pl's password:
Welcome to Ubuntu 14.04.4 LTS (GNU/Linux 4.2.0-27-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

57 packages can be updated.
53 updates are security updates.

Last login: Sat Mar 12 23:45:22 2016 from 172.16.1.101
vuln-admin@vuln-mgt:~$ sudo apt-get update
[sudo] password for vuln-admin:
Ign.  http://extras.ubuntu.com trusty InRelease
Pobieranie:1 http://extras.ubuntu.com trusty Release.gpg [72 B]
Stary http://extras.ubuntu.com trusty Release
Stary http://extras.ubuntu.com trusty/main Sources
Stary http://extras.ubuntu.com trusty/main amd64 Packages
Stary http://extras.ubuntu.com trusty/main i386 Packages
Ign.  http://extras.ubuntu.com trusty/main Translation-pl_PL
Ign.  http://extras.ubuntu.com trusty/main Translation-pl
Ign.  http://extras.ubuntu.com trusty/main Translation-en
Ign.  http://pl.archive.ubuntu.com trusty InRelease
Pobieranie:2 http://pl.archive.ubuntu.com trusty-updates InRelease [65,9 kB]
Pobieranie:3 http://security.ubuntu.com trusty-security InRelease [65,9 kB]
Pobieranie:4 http://pl.archive.ubuntu.com trusty-backports InRelease [65,9 kB]
Stary http://pl.archive.ubuntu.com trusty Release.gpg
Pobieranie:5 http://pl.archive.ubuntu.com trusty-updates/main Sources [262 kB]
Pobieranie:6 http://security.ubuntu.com trusty-security/main Sources [106 kB]
Pobieranie:7 http://pl.archive.ubuntu.com trusty-updates/restricted Sources [5352 B]
Pobieranie:8 http://pl.archive.ubuntu.com trusty-updates/universe Sources [151 kB]
Pobieranie:9 http://pl.archive.ubuntu.com trusty-updates/multiverse Sources [5946 B]
Pobieranie:10 http://pl.archive.ubuntu.com trusty-updates/main amd64 Packages [713 kB]
Pobieranie:11 http://security.ubuntu.com trusty-security/restricted Sources [4035 B]
Pobieranie:12 http://security.ubuntu.com trusty-security/universe Sources [34,0 kB]
Pobieranie:13 http://security.ubuntu.com trusty-security/multiverse Sources [2750 B]
Pobieranie:14 http://pl.archive.ubuntu.com trusty-updates/restricted amd64 Packages [15,
9 kB]
Pobieranie:15 http://pl.archive.ubuntu.com trusty-updates/universe amd64 Packages [339 k
B]
Pobieranie:16 http://security.ubuntu.com trusty-security/main amd64 Packages [431 kB]
Pobieranie:17 http://pl.archive.ubuntu.com trusty-updates/multiverse amd64 Packages [13,
2 kB]
Pobieranie:18 http://pl.archive.ubuntu.com trusty-updates/main i386 Packages [692 kB]
Pobieranie:19 http://pl.archive.ubuntu.com trusty-updates/restricted i386 Packages [15,6
 kB]
Pobieranie:20 http://pl.archive.ubuntu.com trusty-updates/universe i386 Packages [340 kB
]
```

Wykonujemy update systemu, dla pewności, że posiadamy najnowsze pakiety.

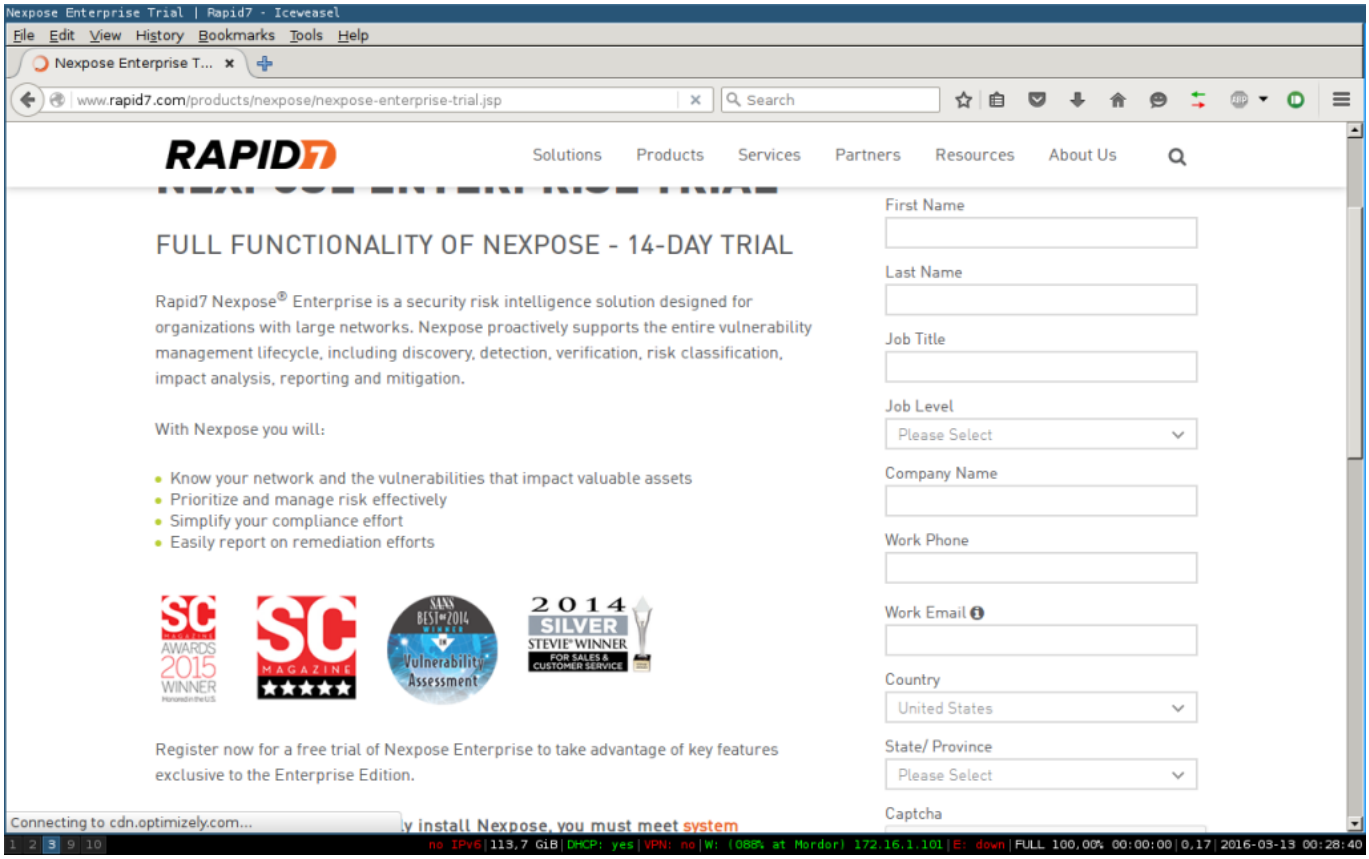
Z strony Rapid7 pobieramy plik instalacyjny Nexpose. Na potrzeby artykułów, aby pokazać pełen zakres możliwości, pobieramy wersje „Enterprise”.



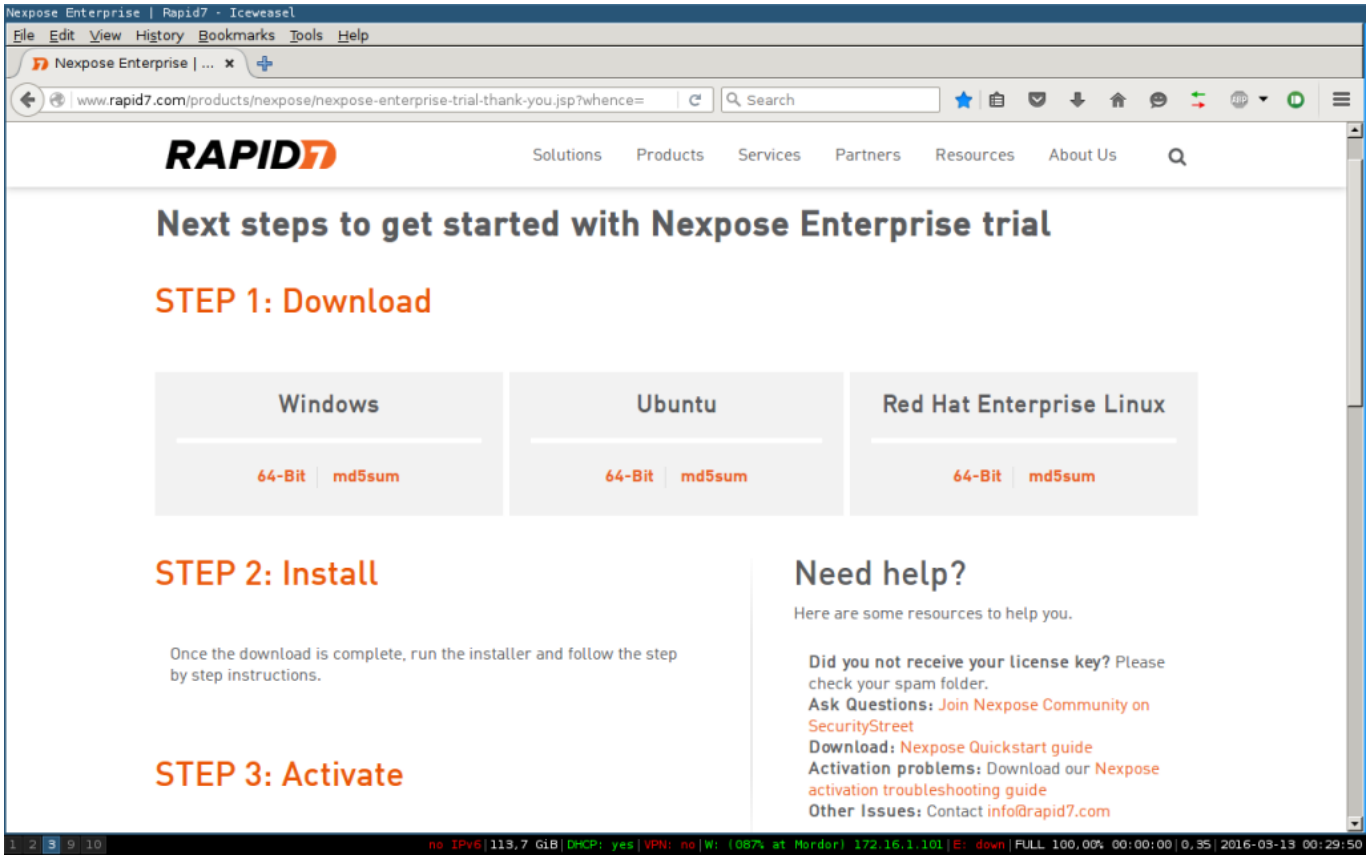
Wybieramy „Software Installation”, możemy również pobrać już gotowy obraz wirtualnej maszyny i wgrać go do naszego serwera wirtualizacji.



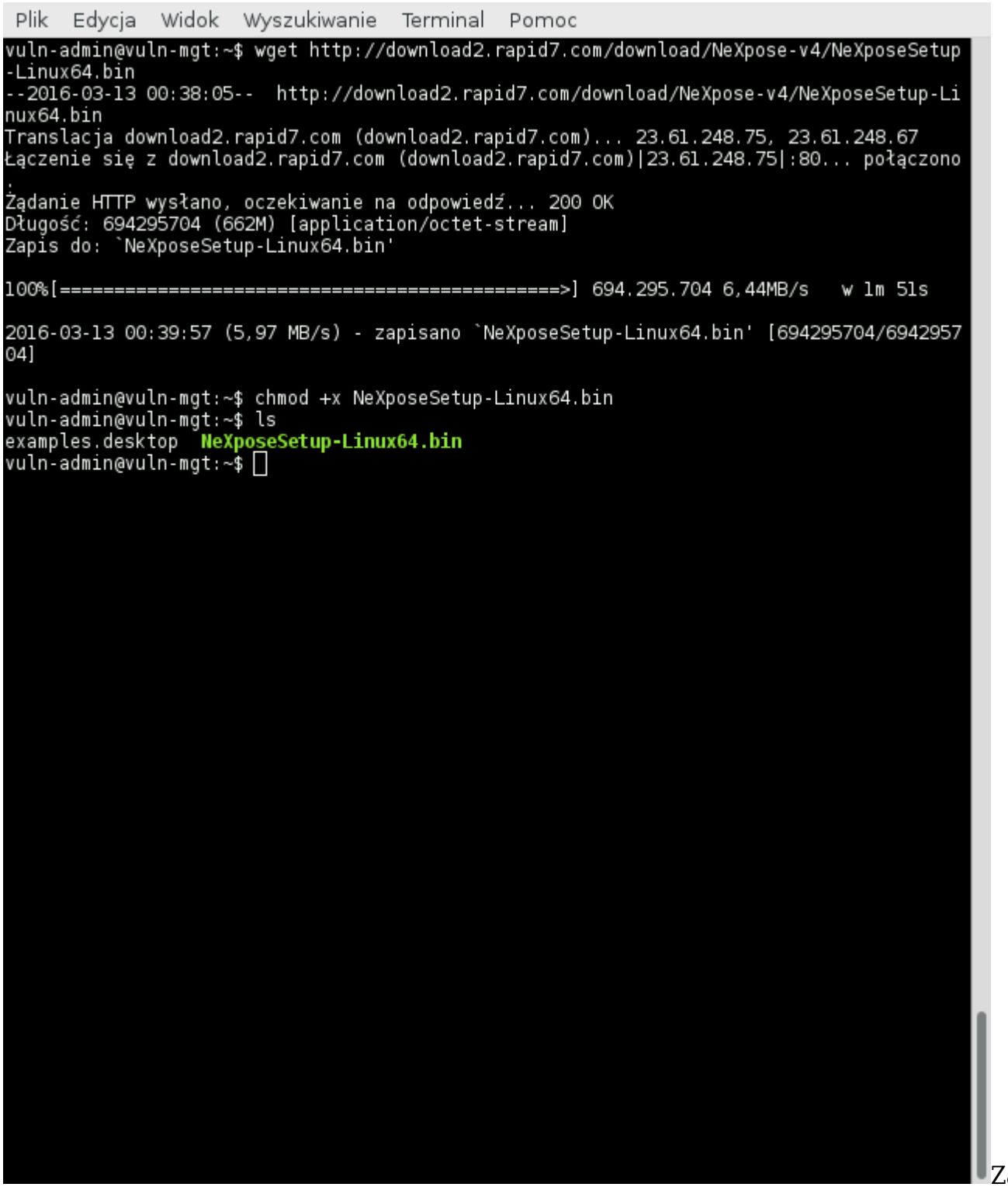
Następnym krokiem jaki musimy wykonać to wypełnienie krótkiego formularza rejestracyjnego, który zapewni nam darmową dwutygodniową licencje.



Wybieramy wersje pliku instalacyjnego względem systemu na maszynie na której będziemy instalować Nexpose.

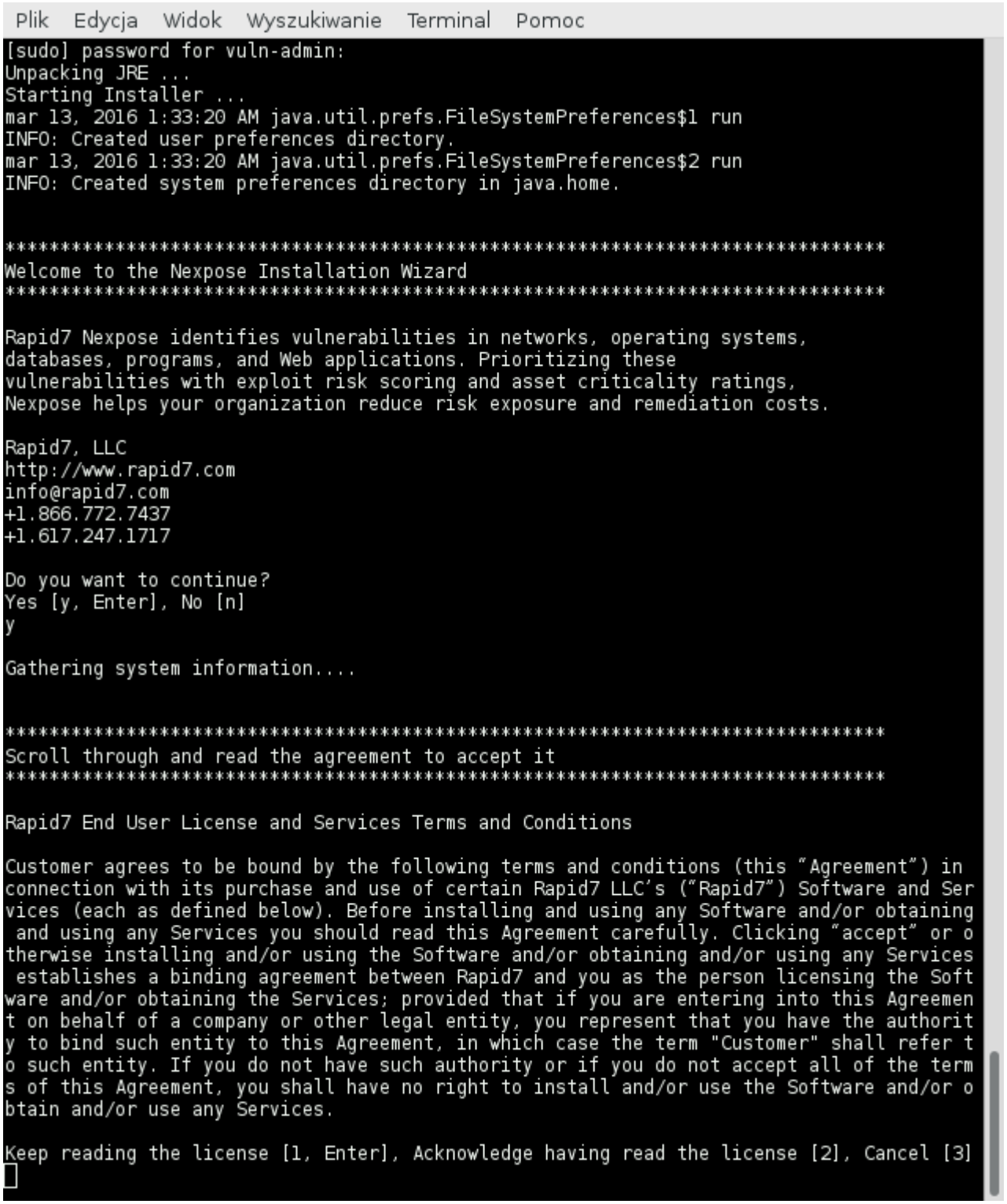


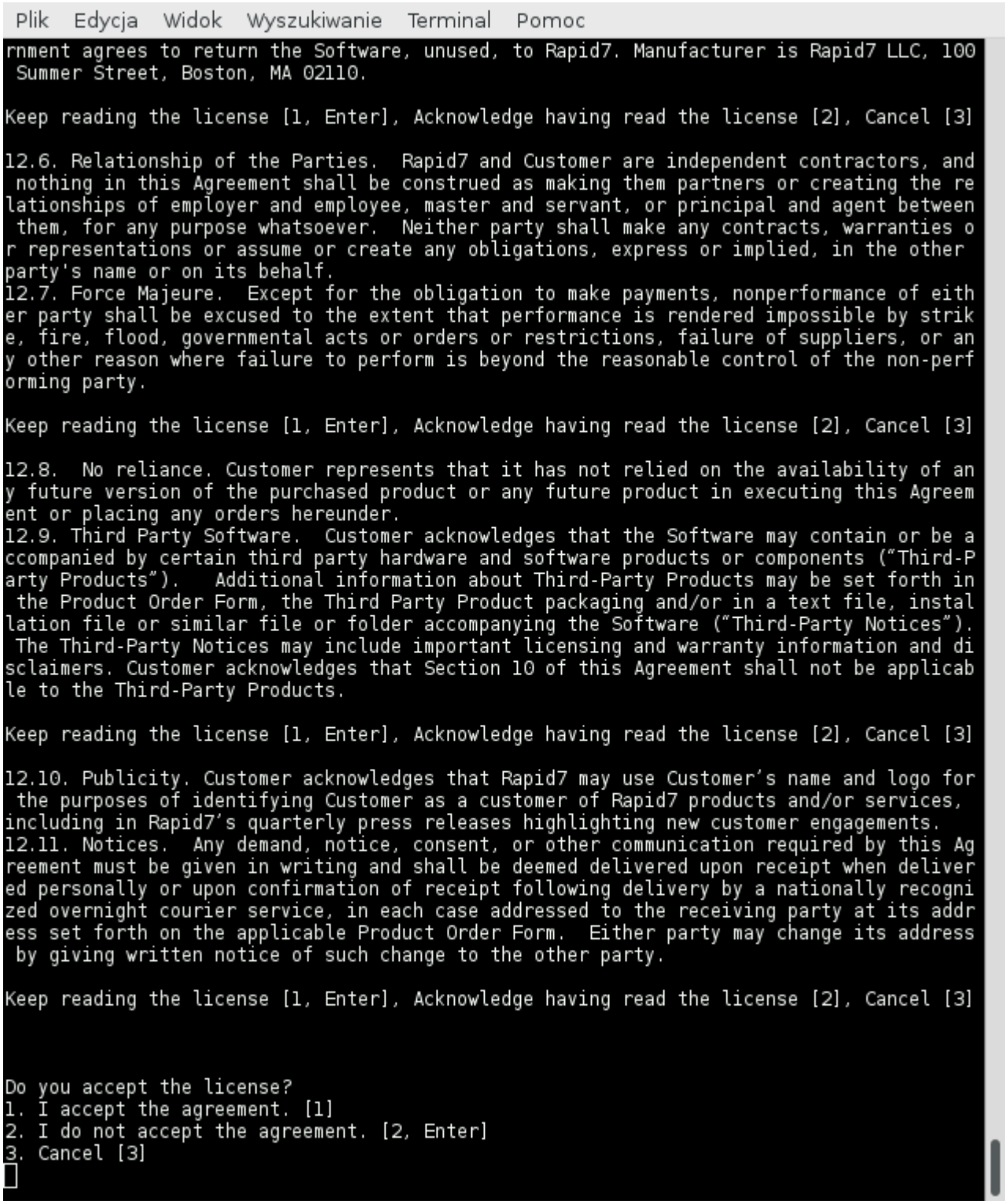
Klikamy prawym na link do pliku instalacyjnego i kopiujemy jego wartość. Użyjemy tego do pobrania instalki na naszą maszynę.

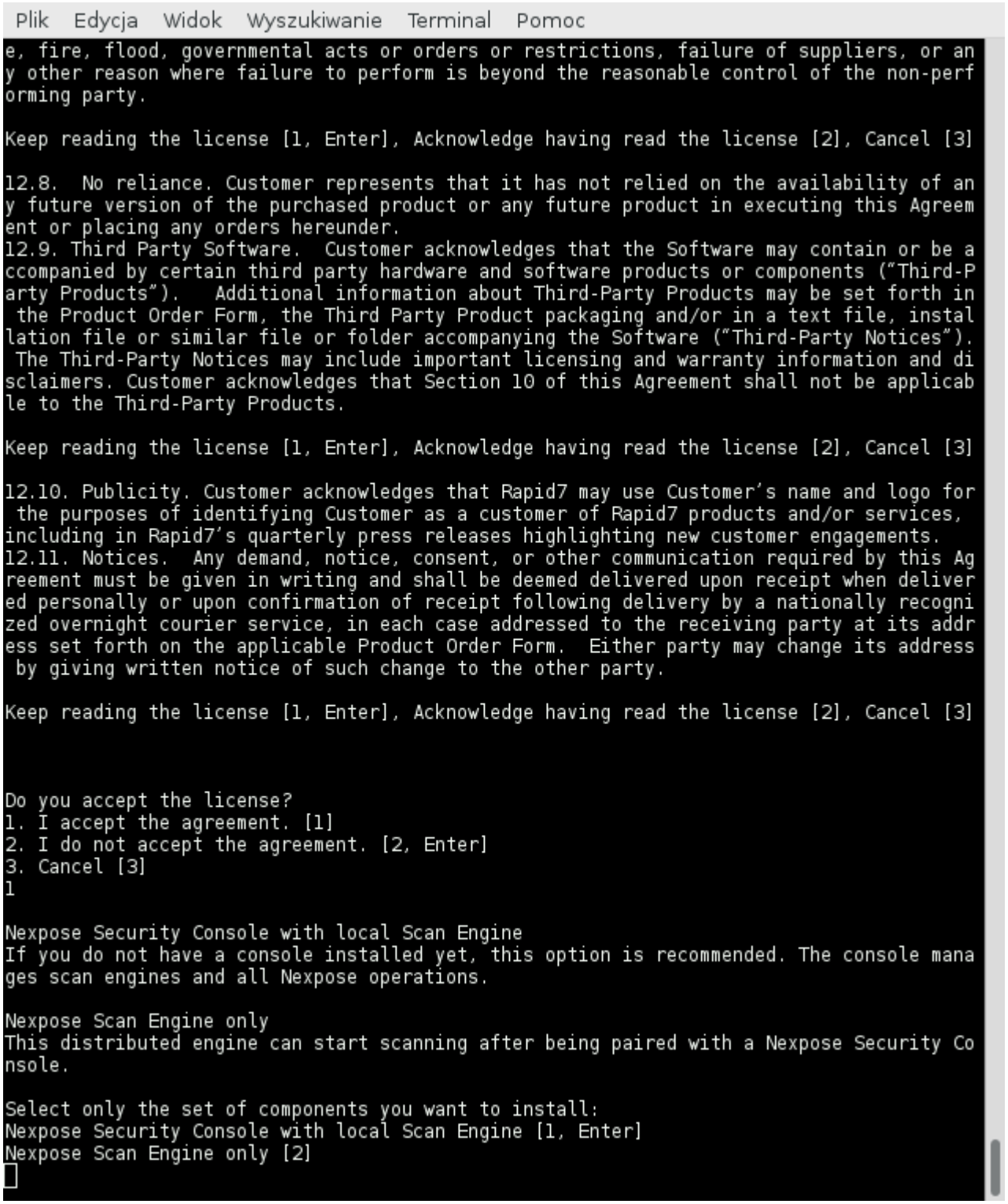


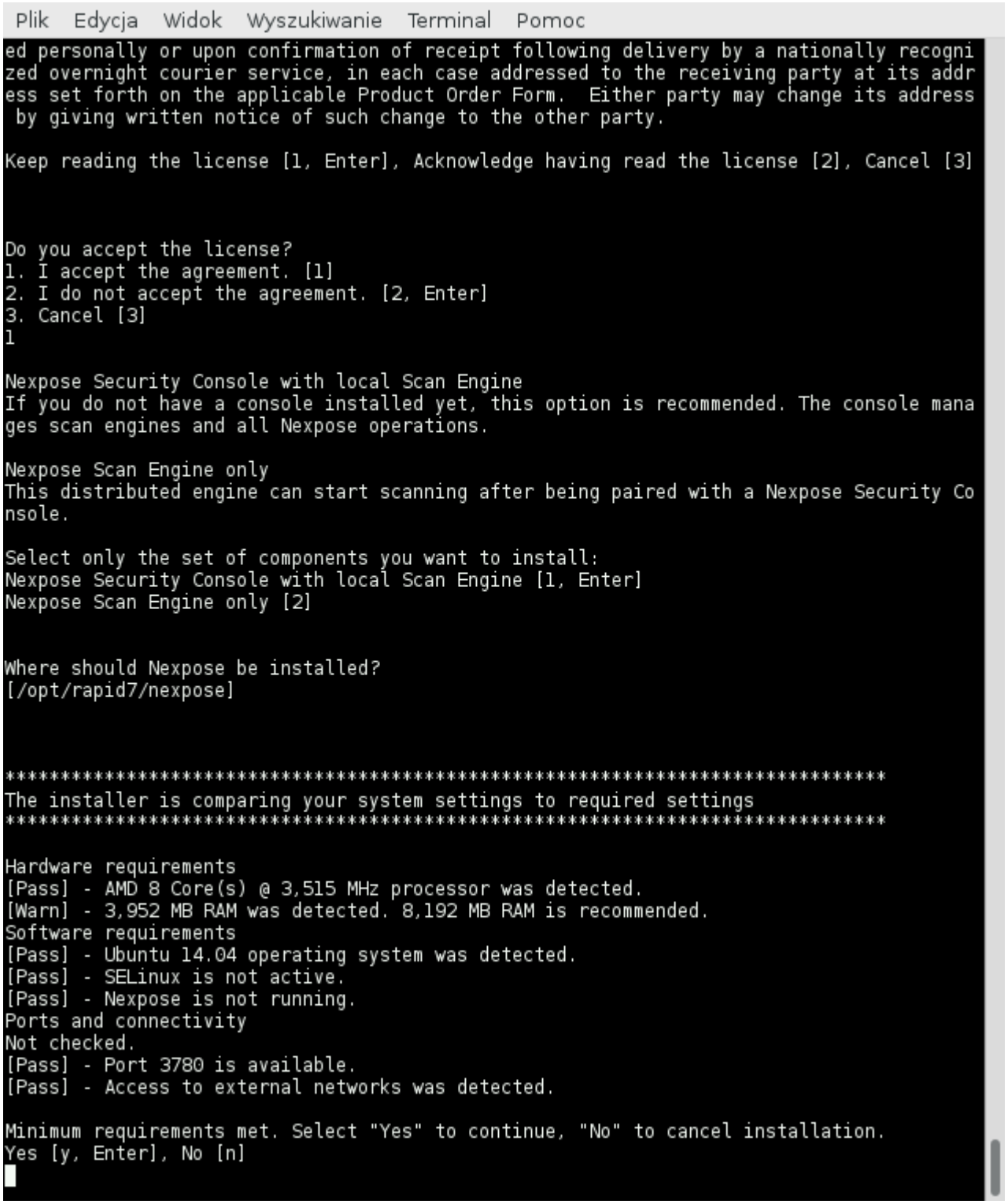
Za pomocą narzędzia wget pobieramy, po czym nadajemy mu uprawnienia do wykonywania.

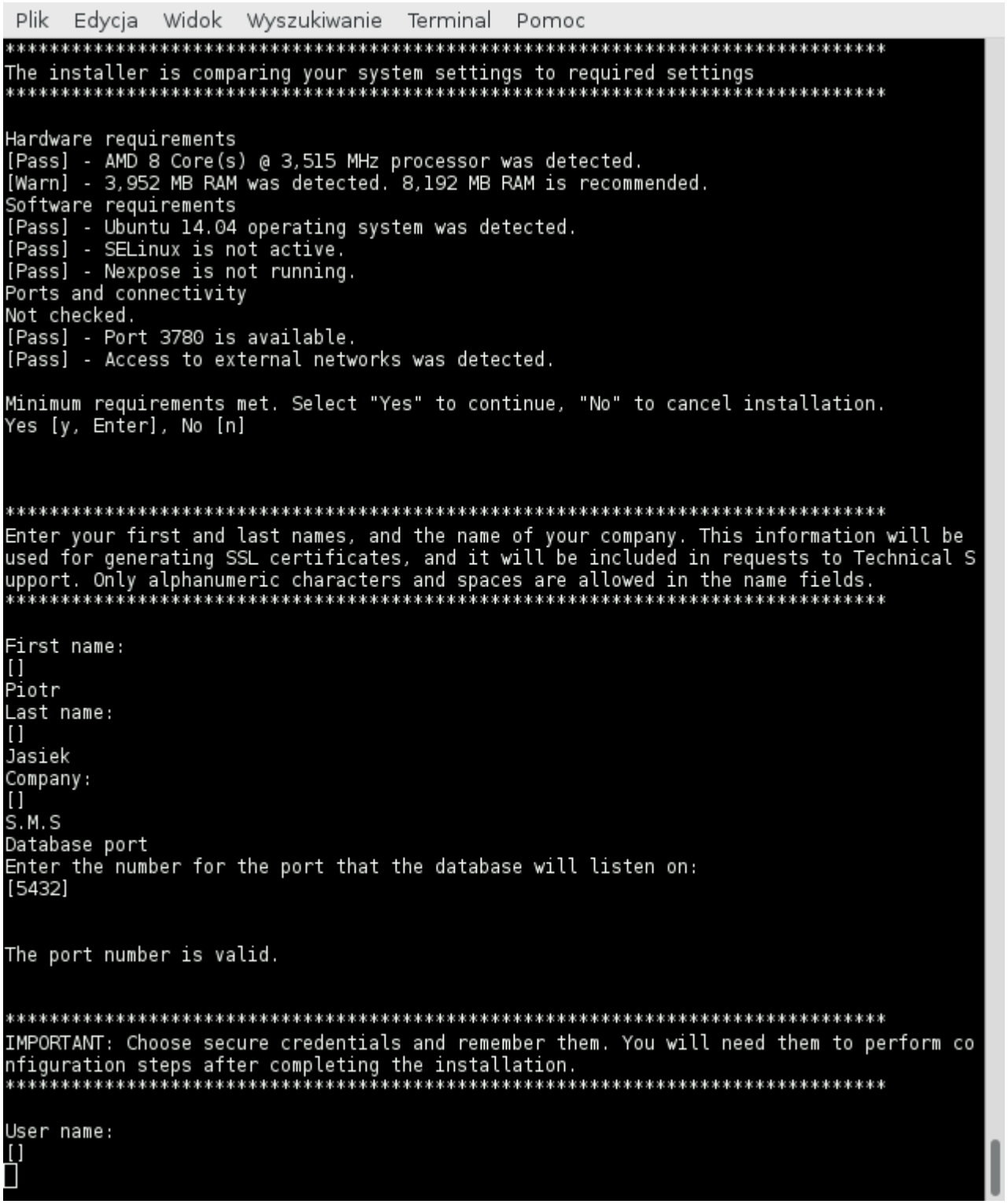
Uruchamiamy instalacje jako root i postępujemy zgodnie z dalszymi instrukcjami.

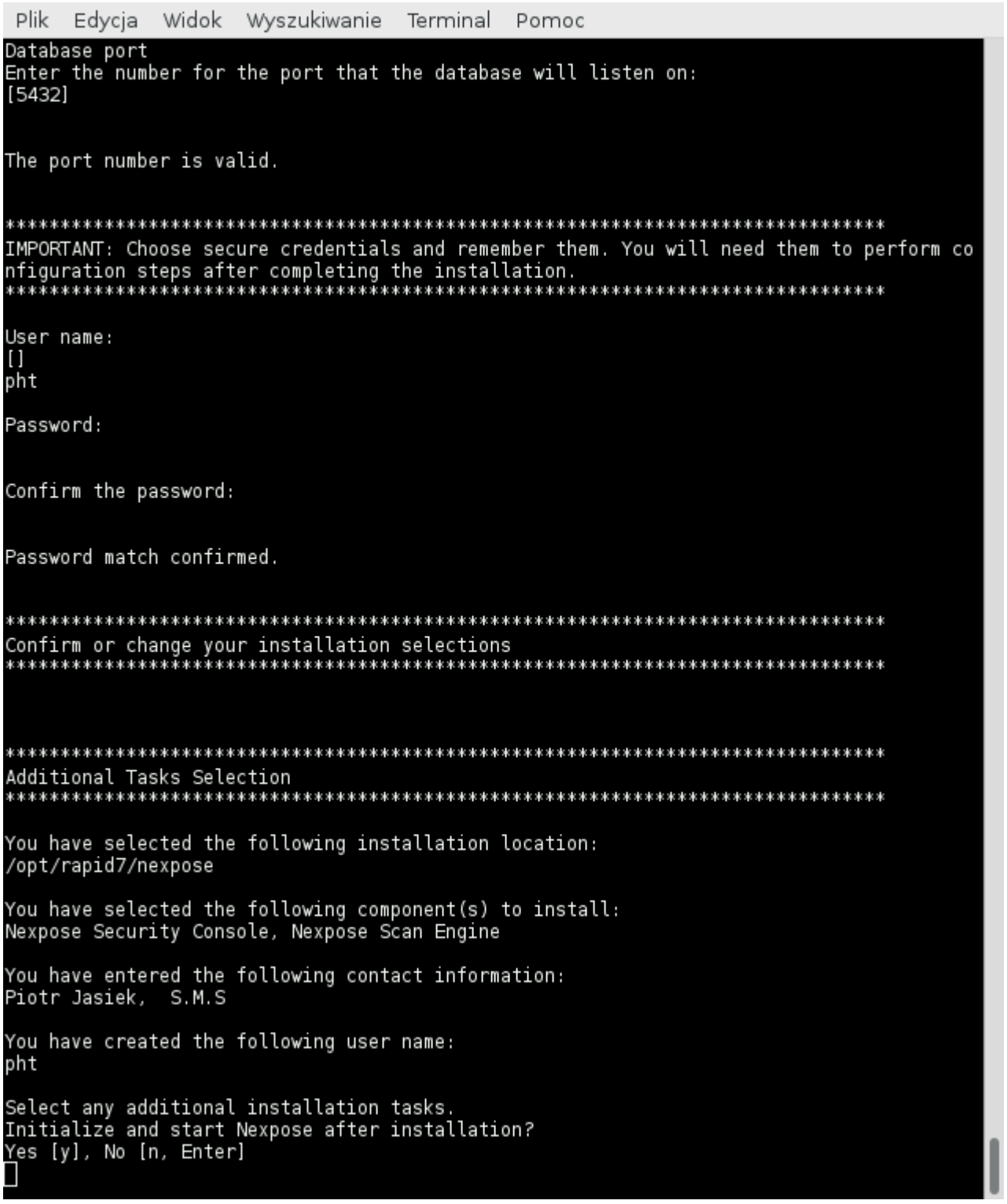



Plik Edycja Widok Wyszukiwanie Terminal Pomoc
rnment agrees to return the Software, unused, to Rapid7. Manufacturer is Rapid7 LLC, 100
Summer Street, Boston, MA 02110.
Keep reading the license [1, Enter], Acknowledge having read the license [2], Cancel [3]
12.6. Relationship of the Parties. Rapid7 and Customer are independent contractors, and
nothing in this Agreement shall be construed as making them partners or creating the re
lationships of employer and employee, master and servant, or principal and agent between
them, for any purpose whatsoever. Neither party shall make any contracts, warranties o
r representations or assume or create any obligations, express or implied, in the other
party's name or on its behalf.
12.7. Force Majeure. Except for the obligation to make payments, nonperformance of eith
er party shall be excused to the extent that performance is rendered impossible by strik
e, fire, flood, governmental acts or orders or restrictions, failure of suppliers, or an
y other reason where failure to perform is beyond the reasonable control of the non-perf
orming party.
Keep reading the license [1, Enter], Acknowledge having read the license [2], Cancel [3]
12.8. No reliance. Customer represents that it has not relied on the availability of an
y future version of the purchased product or any future product in executing this Agreem
ent or placing any orders hereunder.
12.9. Third Party Software. Customer acknowledges that the Software may contain or be a
ccompanied by certain third party hardware and software products or components (“Third-P
arty Products”). Additional information about Third-Party Products may be set forth in
the Product Order Form, the Third Party Product packaging and/or in a text file, instal
lation file or similar file or folder accompanying the Software (“Third-Party Notices”).
The Third-Party Notices may include important licensing and warranty information and di
sclaimers. Customer acknowledges that Section 10 of this Agreement shall not be applicab
le to the Third-Party Products.
Keep reading the license [1, Enter], Acknowledge having read the license [2], Cancel [3]
12.10. Publicity. Customer acknowledges that Rapid7 may use Customer’s name and logo for
the purposes of identifying Customer as a customer of Rapid7 products and/or services,
including in Rapid7’s quarterly press releases highlighting new customer engagements.
12.11. Notices. Any demand, notice, consent, or other communication required by this Ag
reement must be given in writing and shall be deemed delivered upon receipt when deliver
ed personally or upon confirmation of receipt following delivery by a nationally recogni
zed overnight courier service, in each case addressed to the receiving party at its addr
ess set forth on the applicable Product Order Form. Either party may change its address
by giving written notice of such change to the other party.
Keep reading the license [1, Enter], Acknowledge having read the license [2], Cancel [3]
Do you accept the license?
1. I accept the agreement. [1]
2. I do not accept the agreement. [2, Enter]
3. Cancel [3]


Plik Edycja Widok Wyszukiwanie Terminal Pomoc
e, fire, flood, governmental acts or orders or restrictions, failure of suppliers, or an
y other reason where failure to perform is beyond the reasonable control of the non-perf
orming party.
Keep reading the license [1, Enter], Acknowledge having read the license [2], Cancel [3]
12.8. No reliance. Customer represents that it has not relied on the availability of an
y future version of the purchased product or any future product in executing this Agreem
ent or placing any orders hereunder.
12.9. Third Party Software. Customer acknowledges that the Software may contain or be a
ccompanied by certain third party hardware and software products or components ("Third-P
arty Products"). Additional information about Third-Party Products may be set forth in
the Product Order Form, the Third Party Product packaging and/or in a text file, instal
lation file or similar file or folder accompanying the Software ("Third-Party Notices").
The Third-Party Notices may include important licensing and warranty information and di
sclaimers. Customer acknowledges that Section 10 of this Agreement shall not be applicab
le to the Third-Party Products.
Keep reading the license [1, Enter], Acknowledge having read the license [2], Cancel [3]
12.10. Publicity. Customer acknowledges that Rapid7 may use Customer's name and logo for
the purposes of identifying Customer as a customer of Rapid7 products and/or services,
including in Rapid7's quarterly press releases highlighting new customer engagements.
12.11. Notices. Any demand, notice, consent, or other communication required by this Ag
reement must be given in writing and shall be deemed delivered upon receipt when deliver
ed personally or upon confirmation of receipt following delivery by a nationally recogni
zed overnight courier service, in each case addressed to the receiving party at its addr
ess set forth on the applicable Product Order Form. Either party may change its address
by giving written notice of such change to the other party.
Keep reading the license [1, Enter], Acknowledge having read the license [2], Cancel [3]
Do you accept the license?
1. I accept the agreement. [1]
2. I do not accept the agreement. [2, Enter]
3. Cancel [3]
1
Nexpose Security Console with local Scan Engine
If you do not have a console installed yet, this option is recommended. The console mana
ges scan engines and all Nexpose operations.
Nexpose Scan Engine only
This distributed engine can start scanning after being paired with a Nexpose Security Co
nsole.
Select only the set of components you want to install:
Nexpose Security Console with local Scan Engine [1, Enter]
Nexpose Scan Engine only [2]


Plik Edycja Widok Wyszukiwanie Terminal Pomoc
ed personally or upon confirmation of receipt following delivery by a nationally recogni
zed overnight courier service, in each case addressed to the receiving party at its addr
ess set forth on the applicable Product Order Form. Either party may change its address
by giving written notice of such change to the other party.
Keep reading the license [1, Enter], Acknowledge having read the license [2], Cancel [3]
Do you accept the license?
1. I accept the agreement. [1]
2. I do not accept the agreement. [2, Enter]
3. Cancel [3]
1
Nexpose Security Console with local Scan Engine
If you do not have a console installed yet, this option is recommended. The console mana
ges scan engines and all Nexpose operations.
Nexpose Scan Engine only
This distributed engine can start scanning after being paired with a Nexpose Security Co
nsole.
Select only the set of components you want to install:
Nexpose Security Console with local Scan Engine [1, Enter]
Nexpose Scan Engine only [2]
Where should Nexpose be installed?
[/opt/rapid7/nexpose]
****
The installer is comparing your system settings to required settings
****
Hardware requirements
[Pass] - AMD 8 Core(s) @ 3,515 MHz processor was detected.
[Warn] - 3,952 MB RAM was detected. 8,192 MB RAM is recommended.
Software requirements
[Pass] - Ubuntu 14.04 operating system was detected.
[Pass] - SELinux is not active.
[Pass] - Nexpose is not running.
Ports and connectivity
Not checked.
[Pass] - Port 3780 is available.
[Pass] - Access to external networks was detected.
Minimum requirements met. Select "Yes" to continue, "No" to cancel installation.
Yes [y, Enter], No [n]

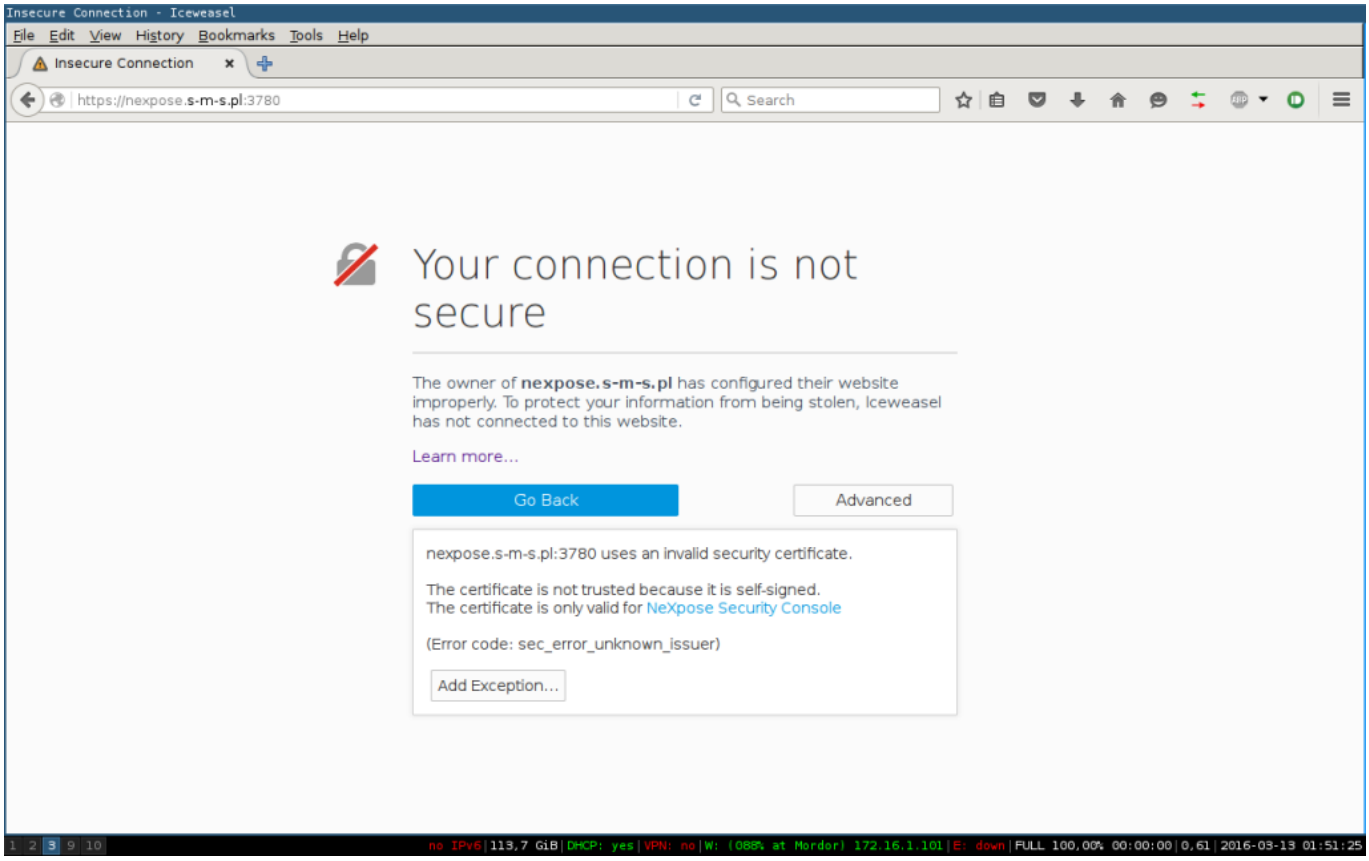

Plik Edycja Widok Wyszukiwanie Terminal Pomoc
The installer is comparing your system settings to required settings
Hardware requirements
[Pass] - AMD 8 Core(s) @ 3,515 MHz processor was detected.
[Warn] - 3,952 MB RAM was detected. 8,192 MB RAM is recommended.
Software requirements
[Pass] - Ubuntu 14.04 operating system was detected.
[Pass] - SELinux is not active.
[Pass] - Nexpose is not running.
Ports and connectivity
Not checked.
[Pass] - Port 3780 is available.
[Pass] - Access to external networks was detected.
Minimum requirements met. Select "Yes" to continue, "No" to cancel installation.
Yes [y, Enter], No [n]
Enter your first and last names, and the name of your company. This information will be
used for generating SSL certificates, and it will be included in requests to Technical S
upport. Only alphanumeric characters and spaces are allowed in the name fields.
First name:
[]
Piotr
Last name:
[]
Jasiek
Company:
[]
S.M.S
Database port
Enter the number for the port that the database will listen on:
[5432]
The port number is valid.
IMPORTANT: Choose secure credentials and remember them. You will need them to perform co
nfiguration steps after completing the installation.
User name:
[]


Plik Edycja Widok Wyszukiwanie Terminal Pomoc
Database port
Enter the number for the port that the database will listen on:
[5432]
The port number is valid.
IMPORTANT: Choose secure credentials and remember them. You will need them to perform co
nfiguration steps after completing the installation.
User name:
[]
pht
Password:
Confirm the password:
Password match confirmed.
Confirm or change your installation selections
Additional Tasks Selection
You have selected the following installation location:
/opt/rapid7/nexpose
You have selected the following component(s) to install:
Nexpose Security Console, Nexpose Scan Engine
You have entered the following contact information:
Piotr Jasiek, S.M.S
You have created the following user name:
pht
Select any additional installation tasks.
Initialize and start Nexpose after installation?
Yes [y], No [n, Enter]

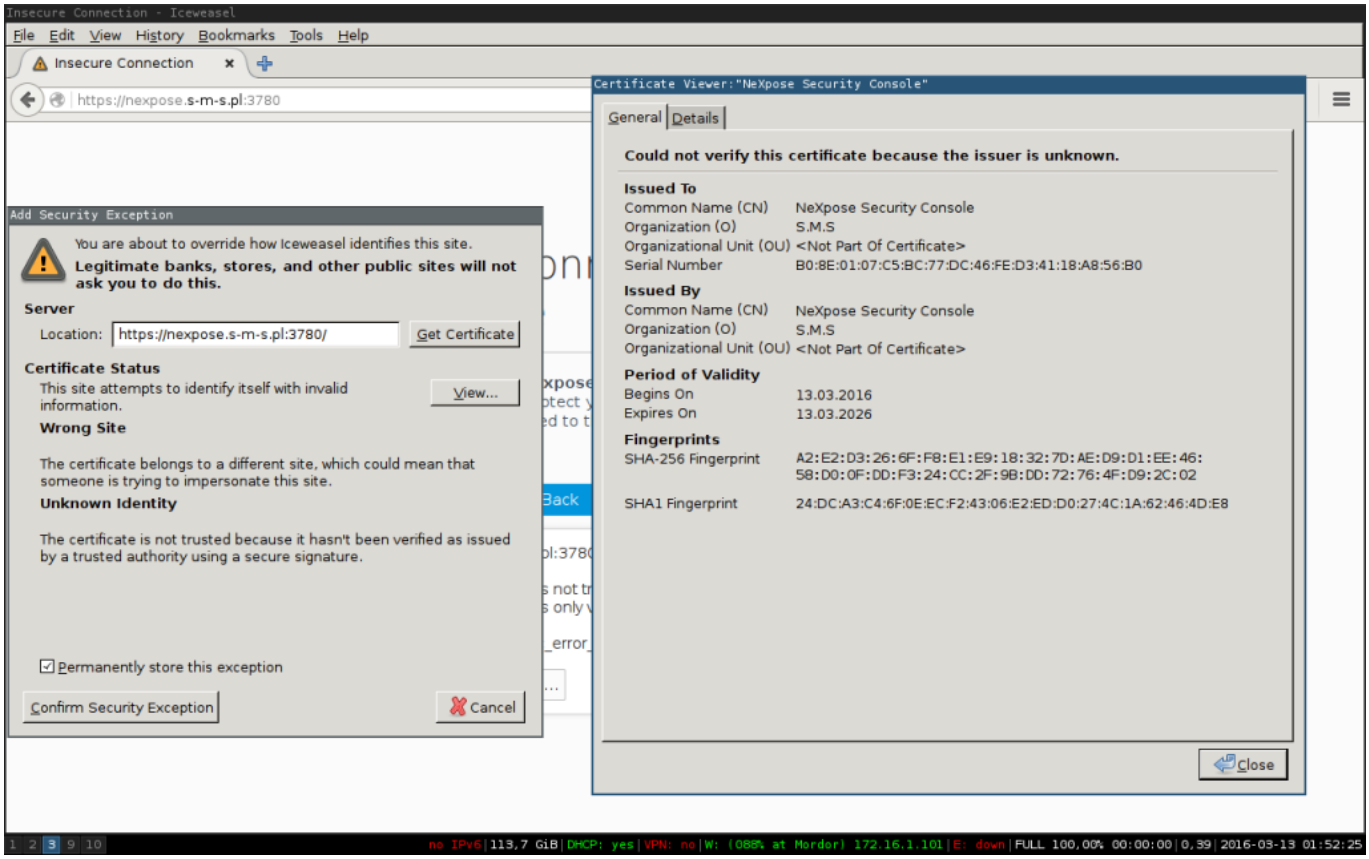
```
Plik  Edycja  Widok  Wyszukiwanie  Terminal  Pomoc

You have selected the following component(s) to install:
Nexpose Security Console, Nexpose Scan Engine

You have entered the following contact information:
Piotr Jasiek,  S.M.S

You have created the following user name:
pht

Select any additional installation tasks.
Initialize and start Nexpose after installation?
Yes [y], No [n, Enter]




********************************************************************************
Extracting files...
********************************************************************************

Extracting files...



********************************************************************************
Installation is complete!
********************************************************************************

Installation is complete!

If you chose to start Nexpose as part of the installation, then it is already running.

Using the credentials you created during installation, log onto Nexpose at https://local
host:3780.

To start scanning, click the *Home* tab in the Nexpose Security Console Web interface. F
or quick-start help, click the *Help* link.

You can start Nexpose manually by executing
/opt/rapid7/nexpose/nsc/nsc.sh.

NOTE: If you did not select the option to start Nexpose as part of the installation, Nex
pose will take 10 to 30 minutes to initialize during first-time startup depending on you
r system capabilities.

Nexpose is configured to start automatically. See the installation guide if you wish to
modify start modes.


[Enter]
```

Konfiguracja z poziomu webpanelu.

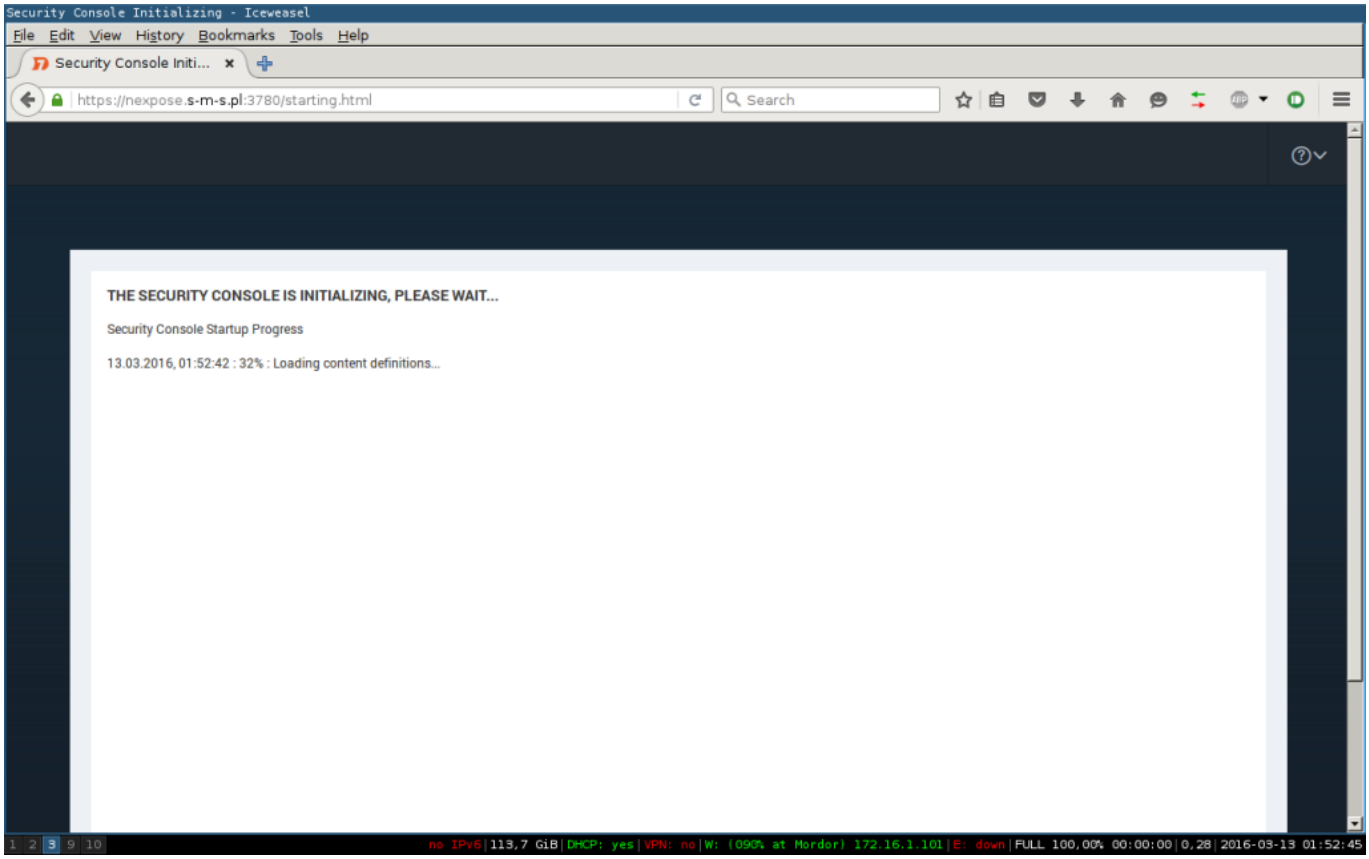
Następnie przechodzimy do web-panelu. W naszym przypadku panel znajduje się pod adresem https://nexpose.s-m-s.pl:3780.



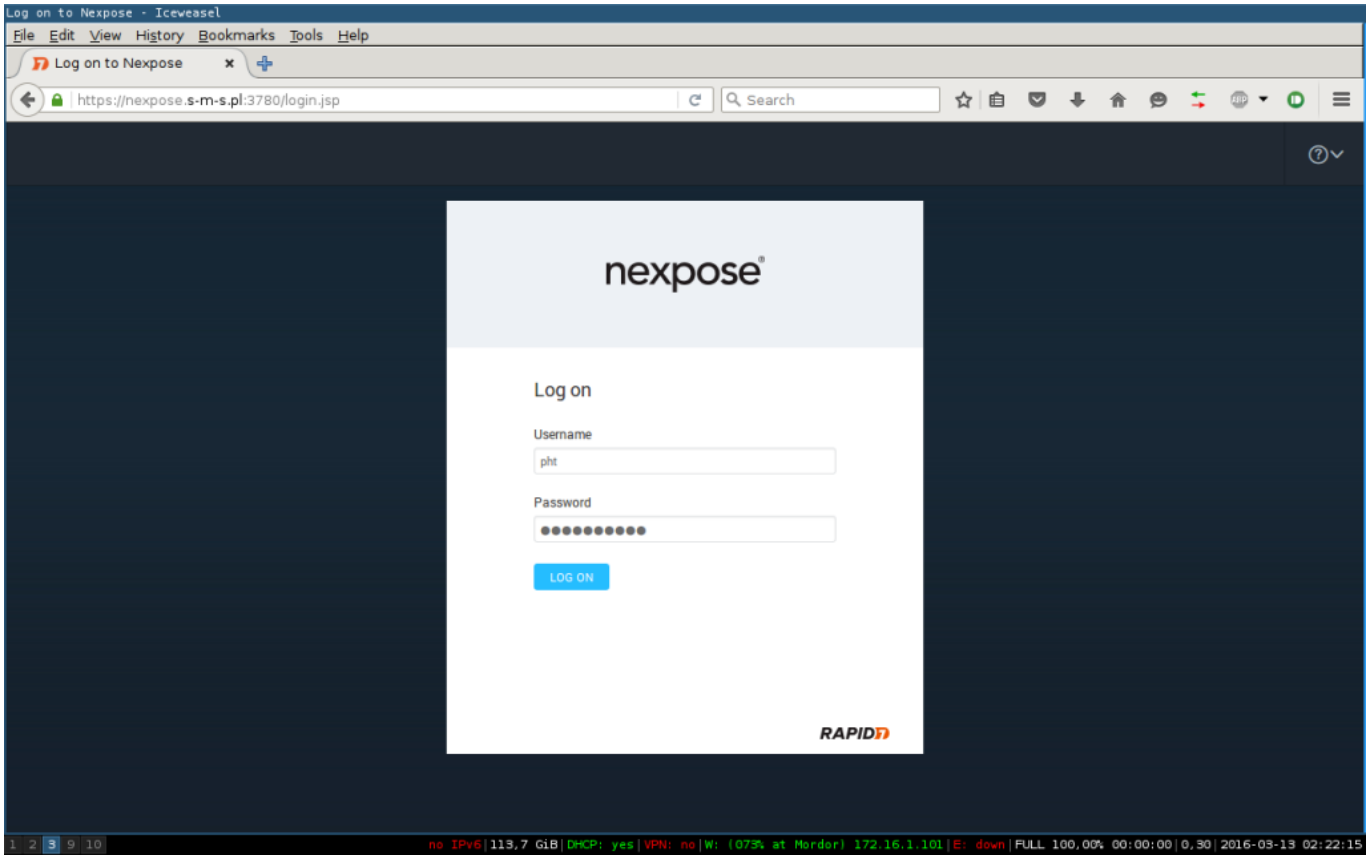
Jak widzimy nasz panel identyfikuje się certyfikatem SSL typu „self-signed”.



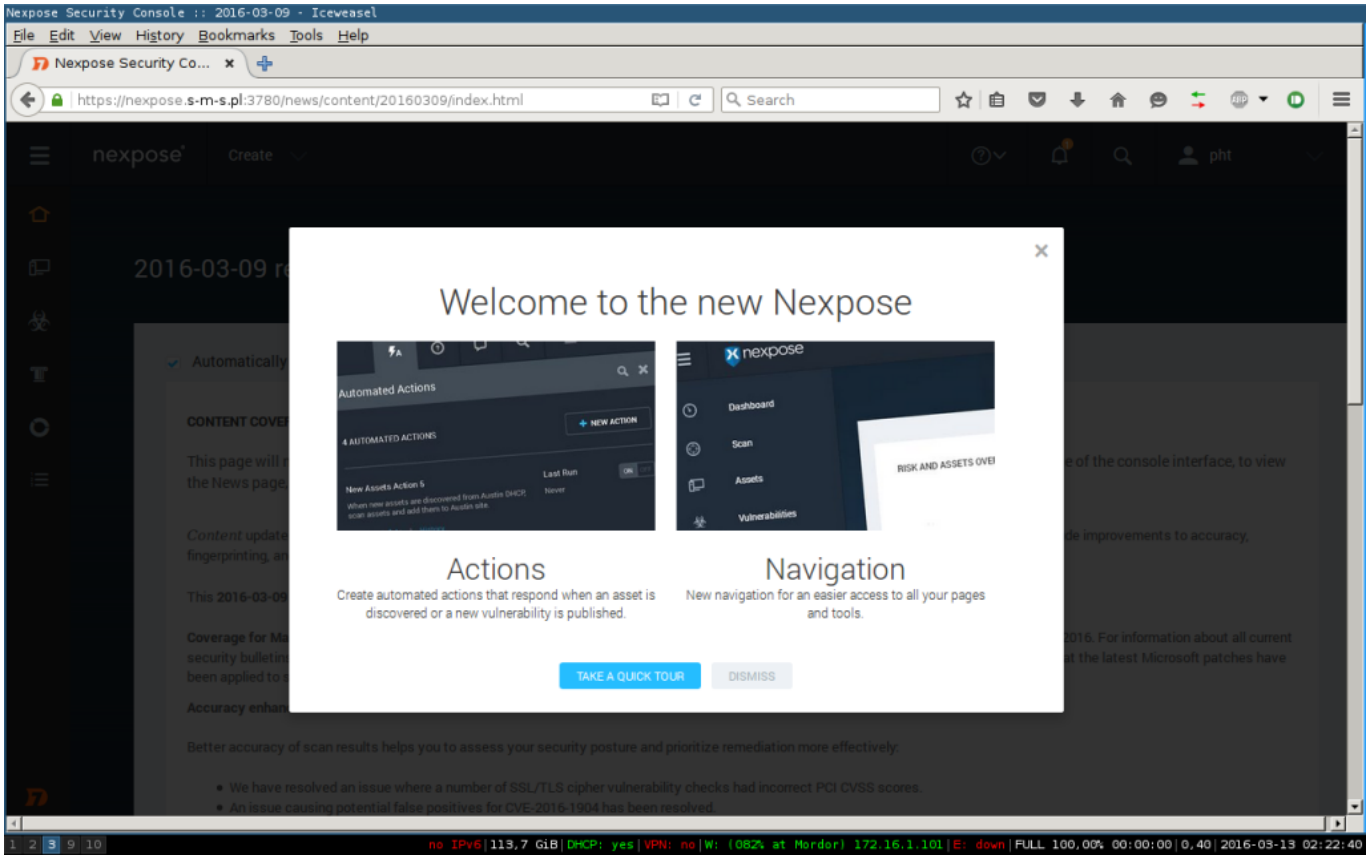
Sprawdzamy, czy przedstawiony certyfikat na pewno jest tym, który wygenerowaliśmy podczas instalacji i dodajemy wyjątek bezpieczeństwa.



Pierwsze uruchomienie może trwać od 10 do 30 minut, jest to zależne jakimi zasobami pamięci dysponuje maszyna na której zainstalowaliśmy Nexpose. Według vendora minimalna ilość pamięci RAM to 8 GB, my daliśmy 4 GB. Do działań laboratoryjnych owe 4 GB starczy bez problemu, natomiast, do seryjnej pracy zaleca się, aby maszyna na której będzie instalowany Nexpose miała 8 GB i więcej RAM-u.

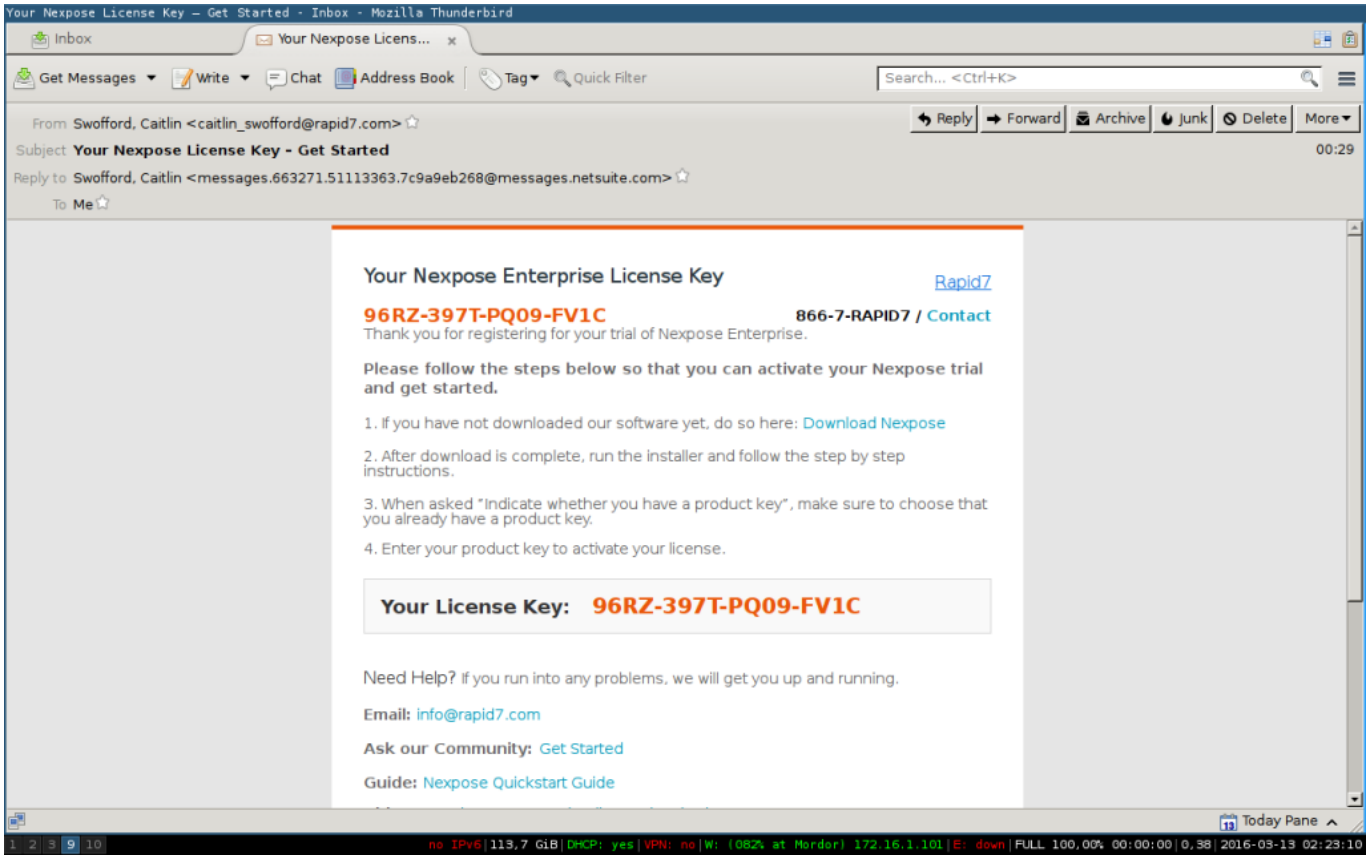


Podczas instalacji podaliśmy login i hasło dla nowego użytkownika. Czas skorzystać z tych danych.

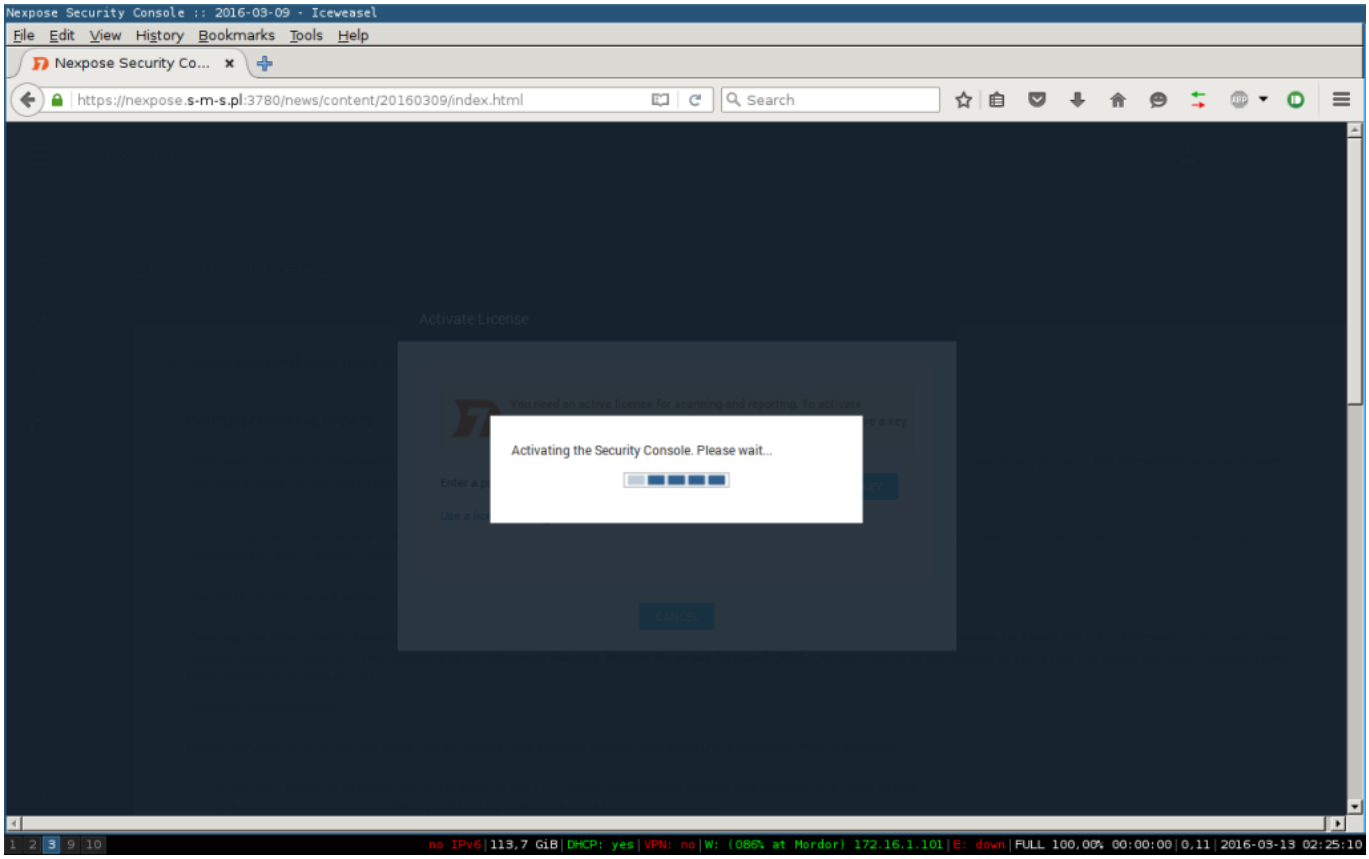


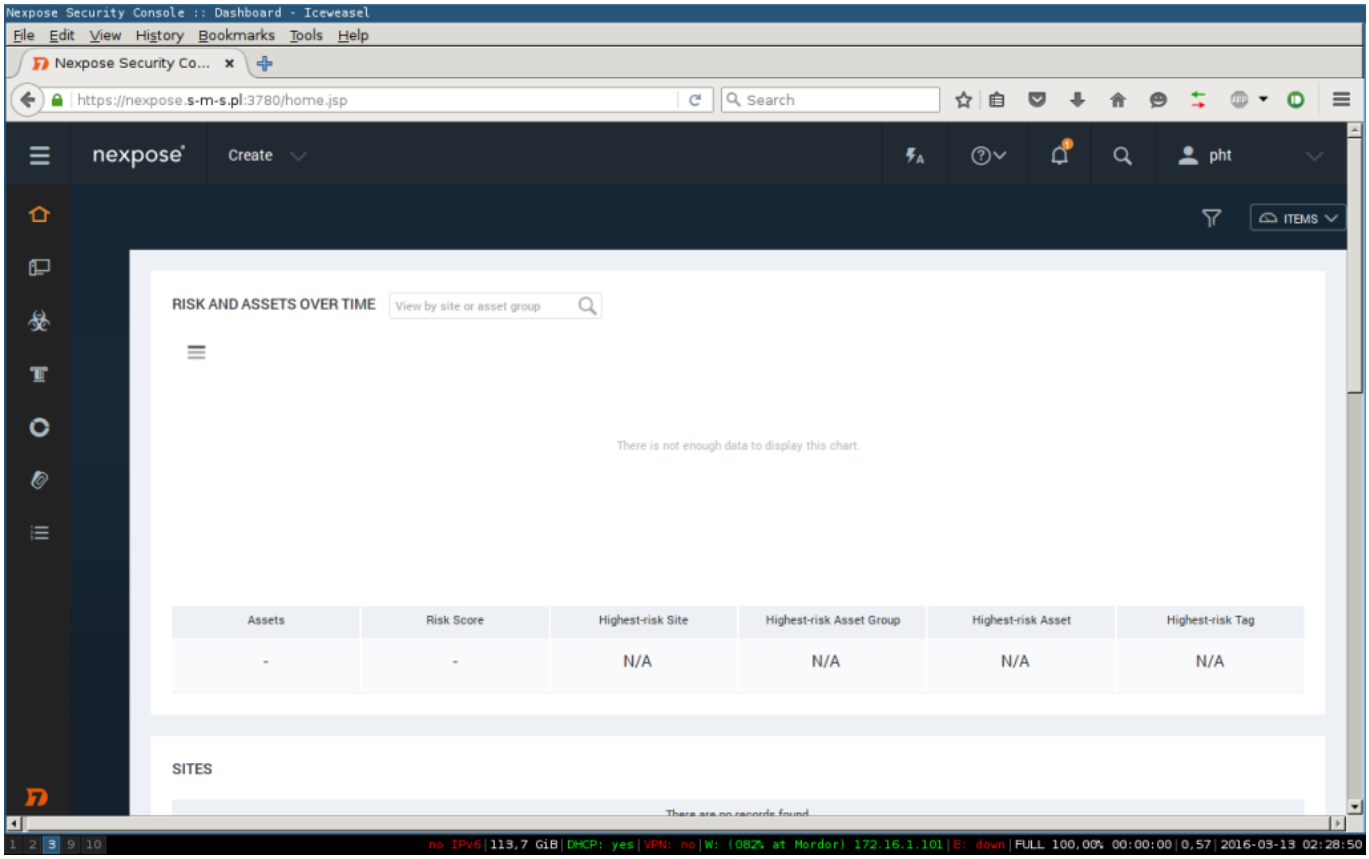
Możemy skorzystać z wbudowanego samouczka, który oprowadzi nas po panelu Nexpose i pokaże co i gdzie możemy znaleźć.

Po zalogowaniu również zostaniemy poproszeni o podanie klucza licencyjnego. Jeżeli podaliśmy prawidłowy email podczas rejestracji, powinniśmy mieć na nim maila od Rapid7 z licencją.



Przypominamy, że licencja, którą otrzymujemy na maila po rejestracji na stronie Rapid7 jest darmowa i ograniczona czasowo. Trwa ona 14 dni. Po zakończeniu licencji, możemy odnowić licencje, korzystając z tych samych danych co poprzednio.


Nexpose Security Console :: 2016-03-09 - Iceweasel
File Edit View History Bookmarks Tools Help
Nexpose Security Co...
https://nexpose.s-m-s.pl:3780/news/content/20160309/index.html
Search
Activate License
Activating the Security Console. Please wait...
1 2 3 9 10
no IPv6 | 113,7 GiB | DHCP: yes | VPN: no | W: (086% at Mordor) 172.16.1.101 | E: down | FULL 100,00% 00:00:00 | 0,11 | 2016-03-13 02:25:10



Po zakończeniu aktywacji przed naszymi oczami ukazuje się gotowy panel. To wszystko jeżeli chodzi o konfiguracje samego oprogramowania w przypadku manualnej instalacji.

Poprawki bezpieczeństwa.

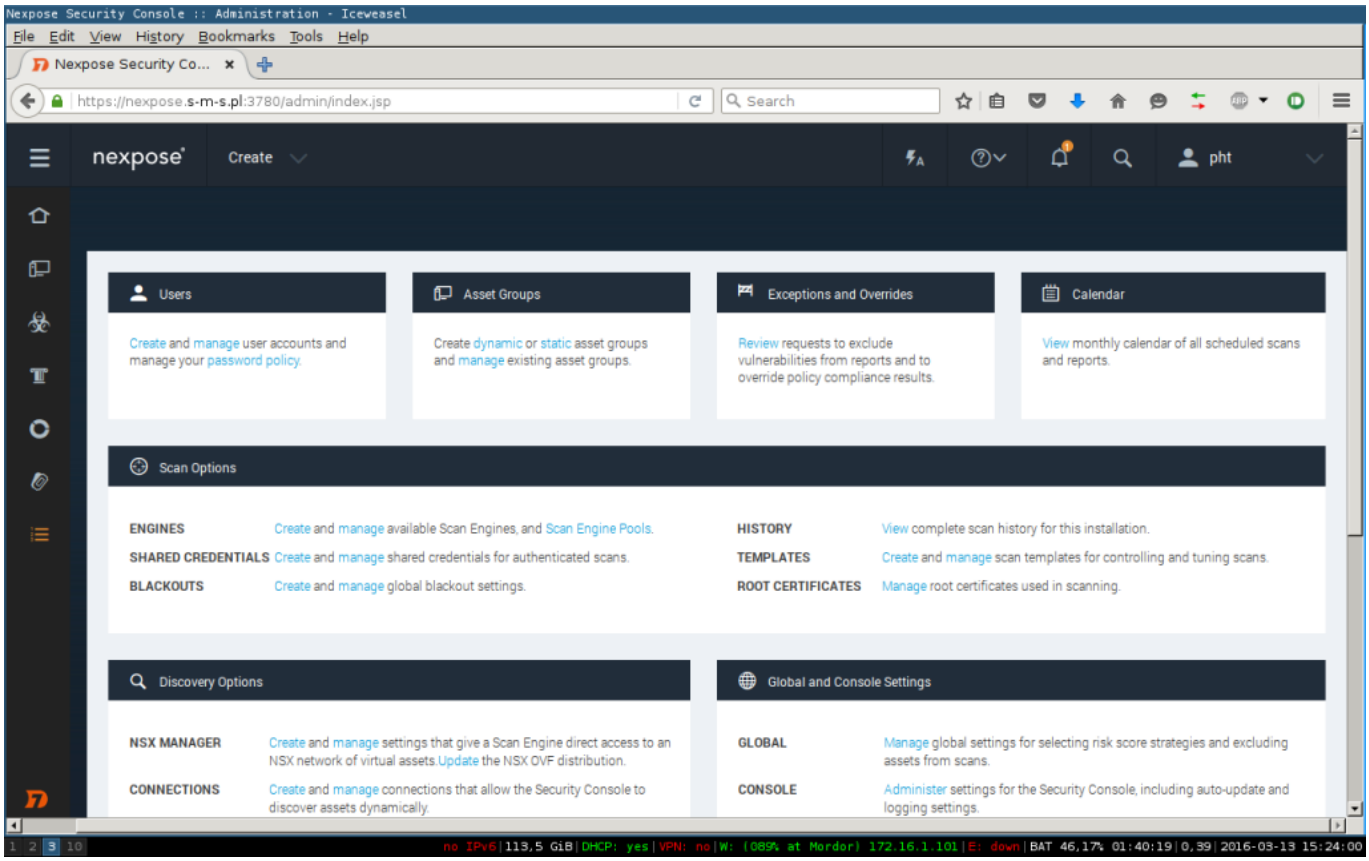
Jeżeli ktoś wybrał instalacje z gotowego obrazu maszyny wirtualnej, powinien pamiętać o kilku, istotnych rzeczach. Pierwszą z nich jest fakt, iż domyślnymi danymi dostępowymi są:

- dla OS: nexpose:nexpose
- dla samego web panelu: nxadmin:nxpassword

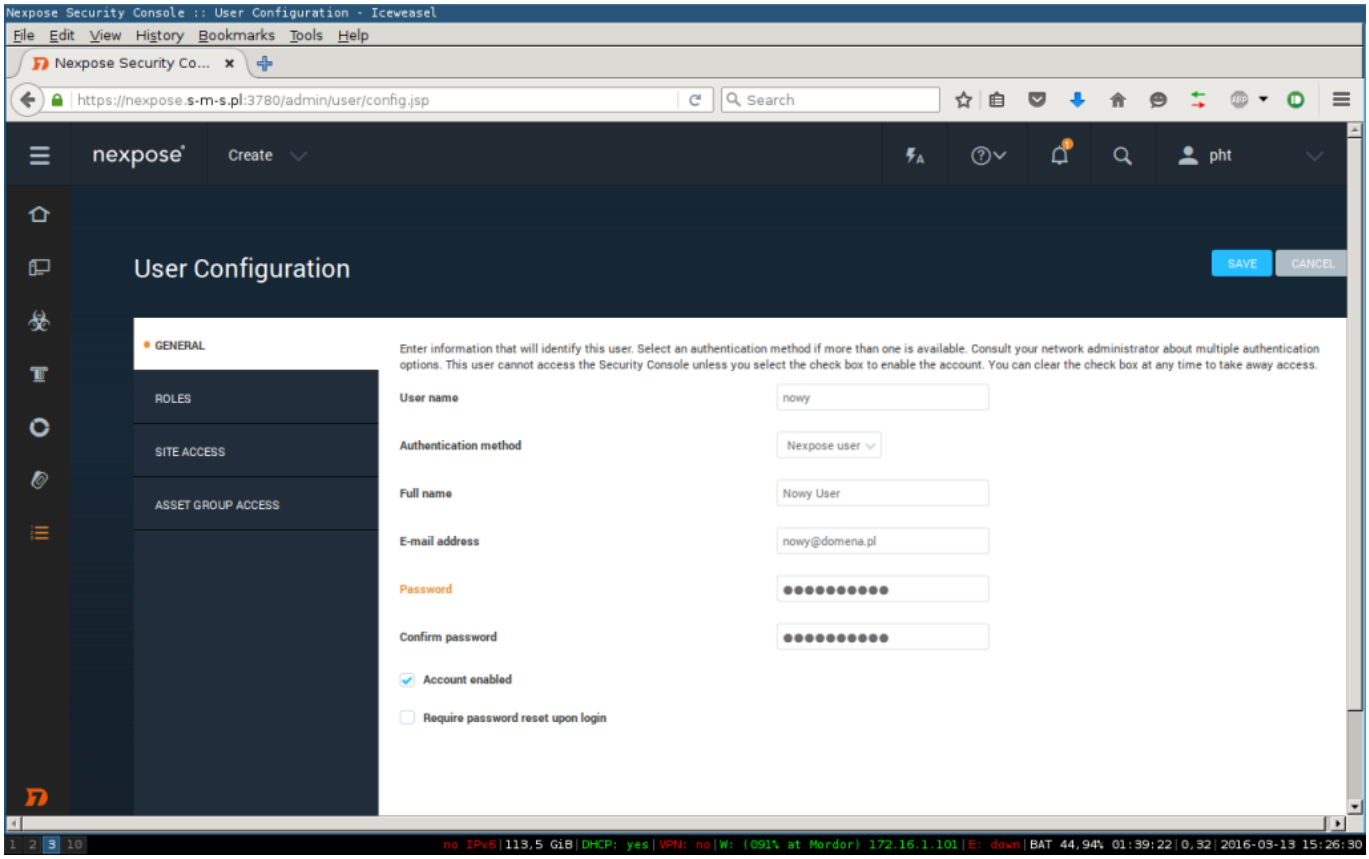
Dane te, należy niezwłocznie zmienić zaraz po zakończeniu powyższych czynności.

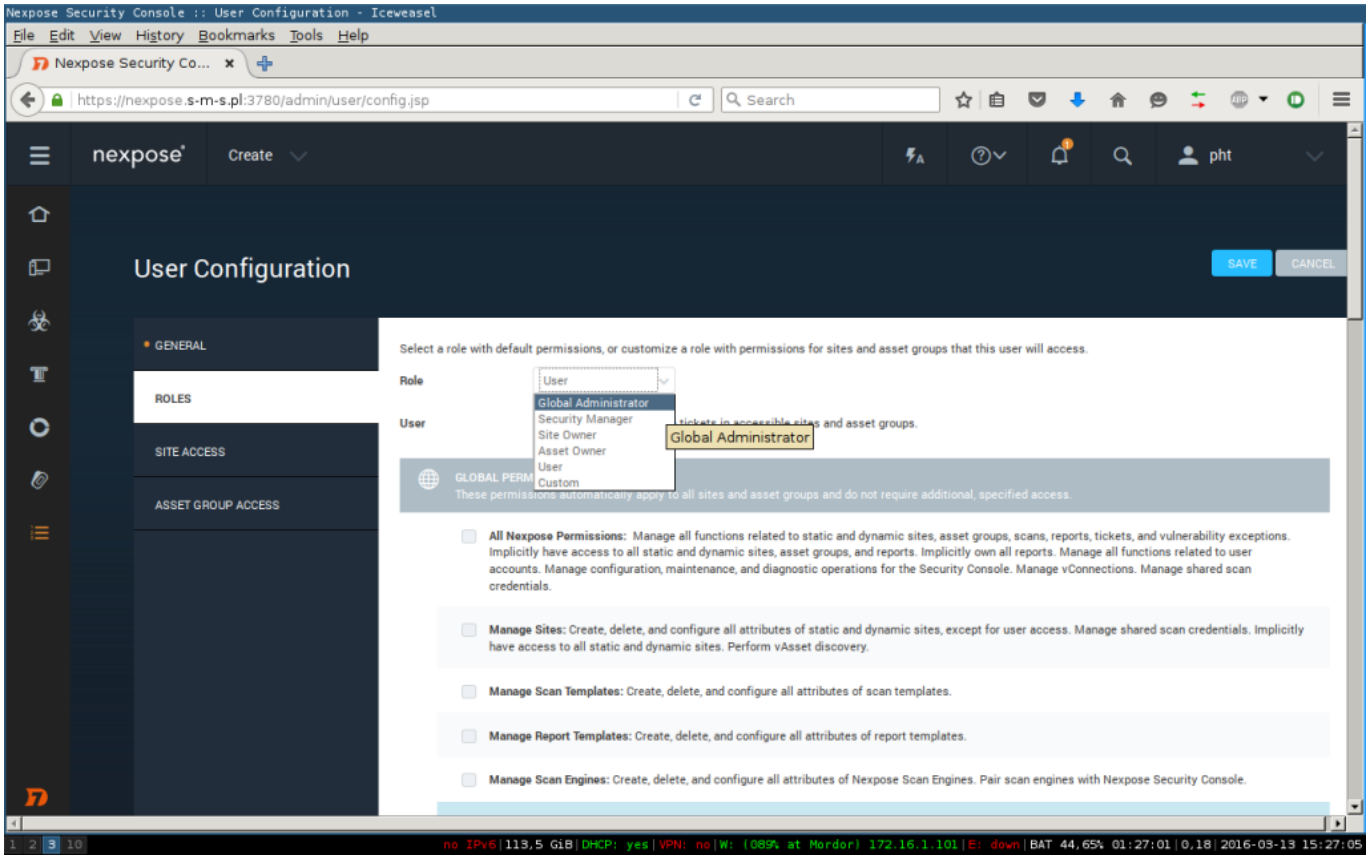
Aby zmienić dane dostępowe do panelu Nexpose, możemy zrobić to na dwa sposoby. Dodać nowego użytkownika i zablokować domyślnego, lub po prostu zmienić hasło dla domyślnego

usera. Działania te wykonujemy w zakładce „Administracja”

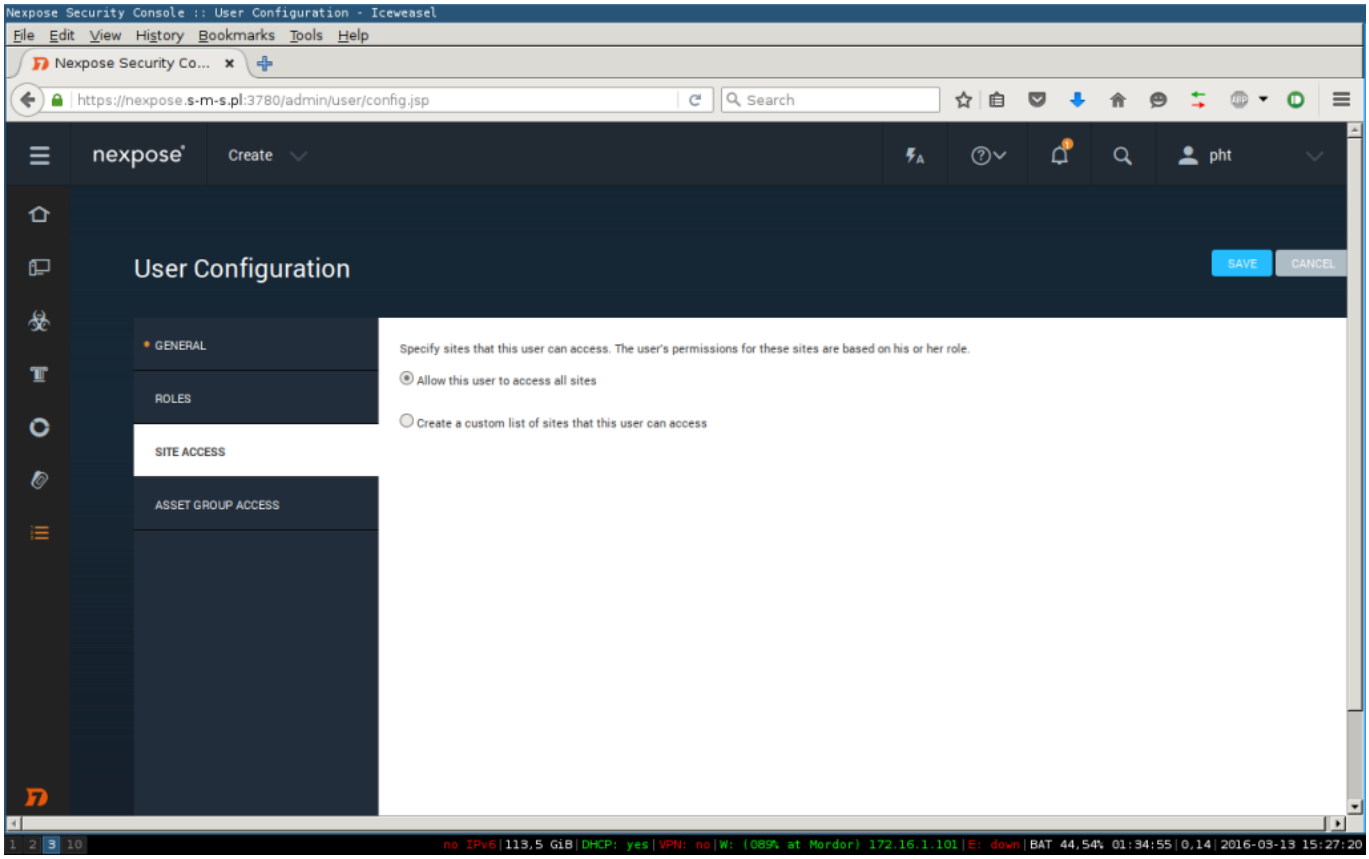


By utworzyć użytkownika, wybieramy „Create” w zakładce „Users”.

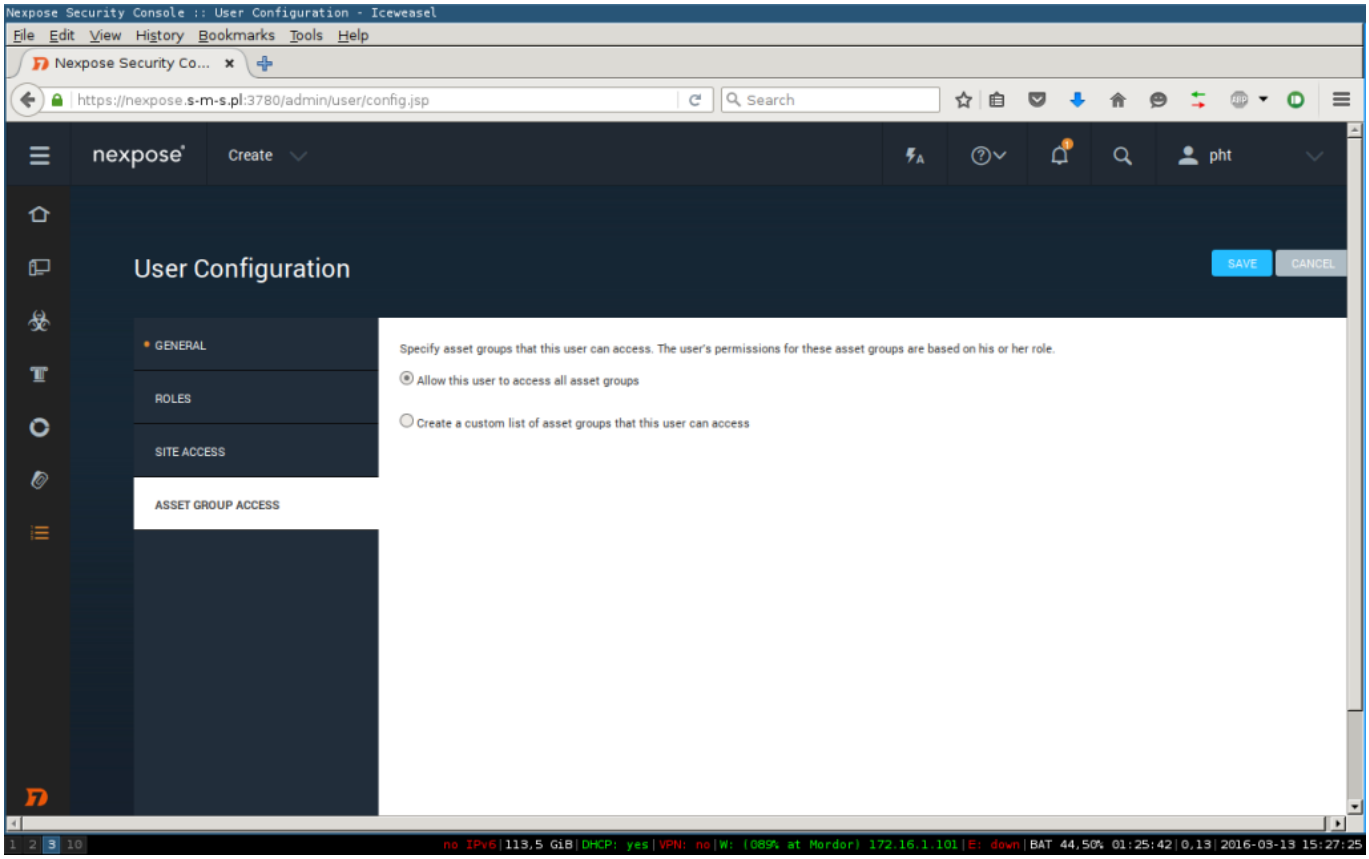

Nexpose Security Console :: User Configuration - Iceweasel
File Edit View History Bookmarks Tools Help
Nexpose Security Co...
https://nexpose.s-m-s.pl:3780/admin/user/config.jsp
Search
nexpose
Create
pht
User Configuration
SAVE
CANCEL
GENERAL
ROLES
SITE ACCESS
ASSET GROUP ACCESS
Enter information that will identify this user. Select an authentication method if more than one is available. Consult your network administrator about multiple authentication options. This user cannot access the Security Console unless you select the check box to enable the account. You can clear the check box at any time to take away access.
User name
nowy
Authentication method
Nexpose user
Full name
Nowy User
E-mail address
nowy@domena.pl
Password
Confirm password
Account enabled
Require password reset upon login

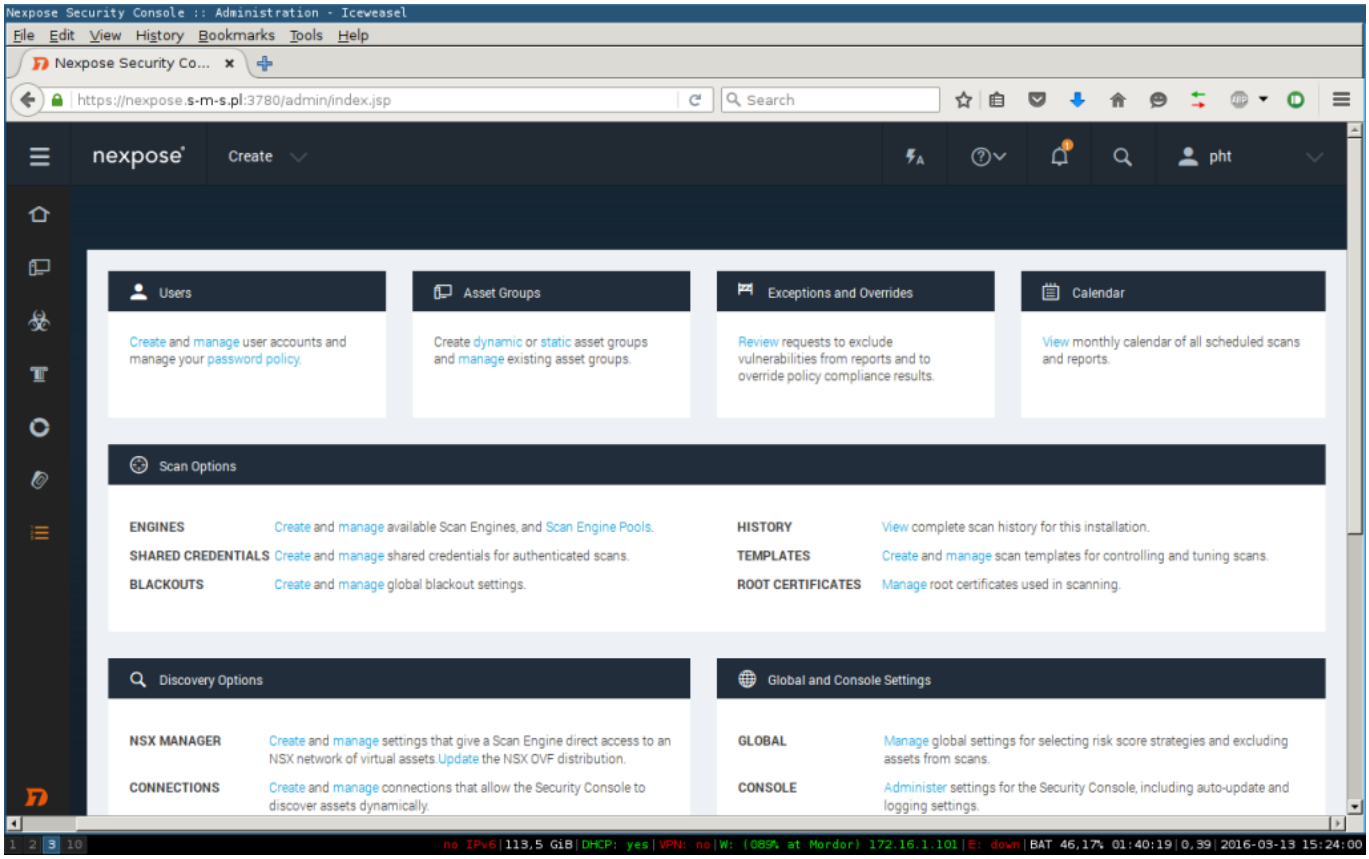


Wybieramy rodzaj uprawnień nowego użytkownika. Możemy skorzystać z gotowych szablonów lub stworzyć własny zakres uprawnień. Zachęcamy do zapoznania się z listą uprawnień.

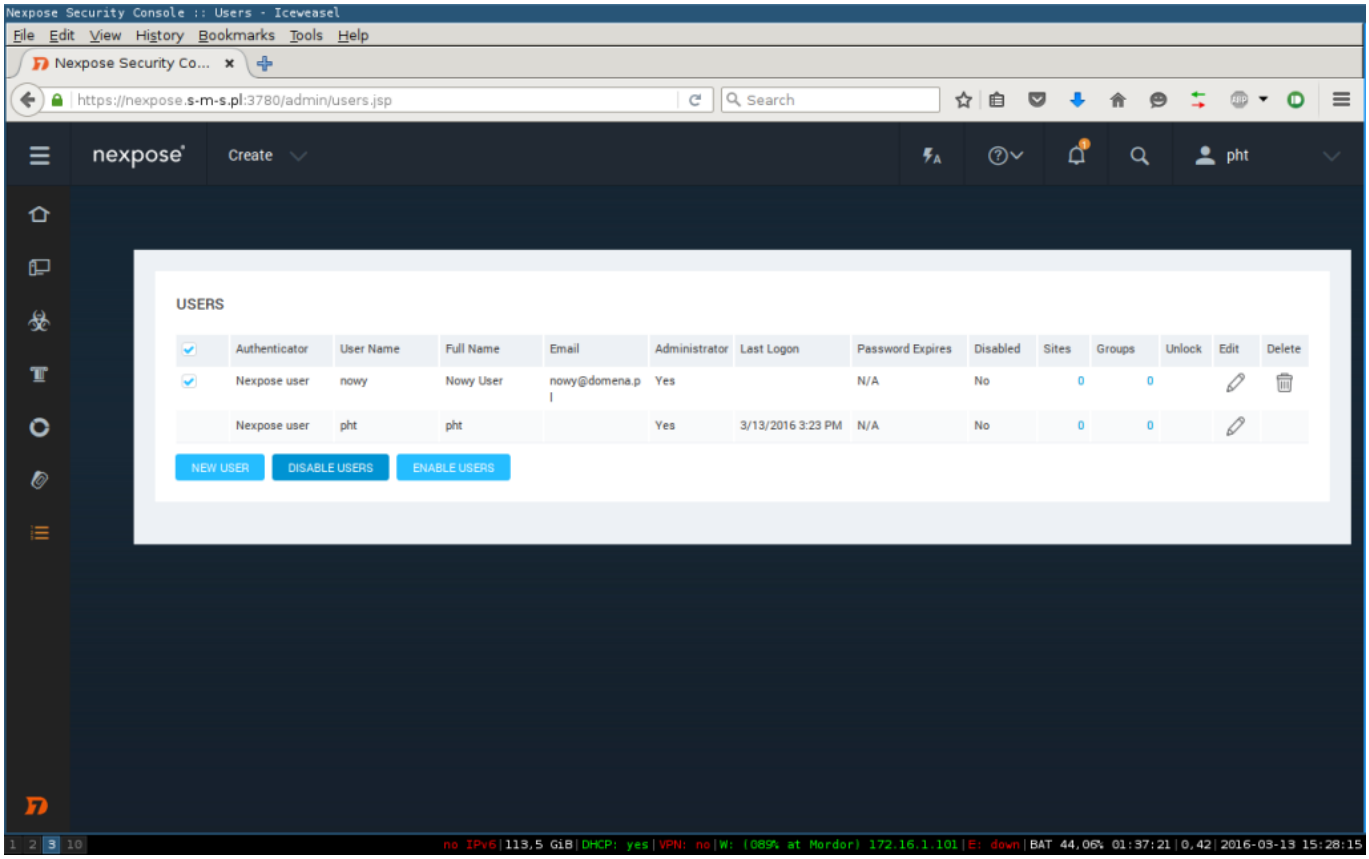


Wybieramy dostęp do działów „site” oraz „asset group” o których więcej napiszemy w następnym artykule z serii.


Nexpose Security Console :: User Configuration - Iceweasel
File Edit View History Bookmarks Tools Help
Nexpose Security Co...
https://nexpose.s-m-s.pl:3780/admin/user/config.jsp
Search
nexpose
Create
pht
User Configuration
SAVE
CANCEL
GENERAL
ROLES
SITE ACCESS
ASSET GROUP ACCESS
Specify asset groups that this user can access. The user's permissions for these asset groups are based on his or her role.
Allow this user to access all asset groups
Create a custom list of asset groups that this user can access



Aby edytować użytkowników przechodzimy do zakładki „manage” w dziale „Users”.



Aby wyłączyć użytkownika należy zaznaczyć go i kliknąć „Disable”.

I to na tyle ogólnej konfiguracji – na ciąg dalszy zapraszamy już niedługo!