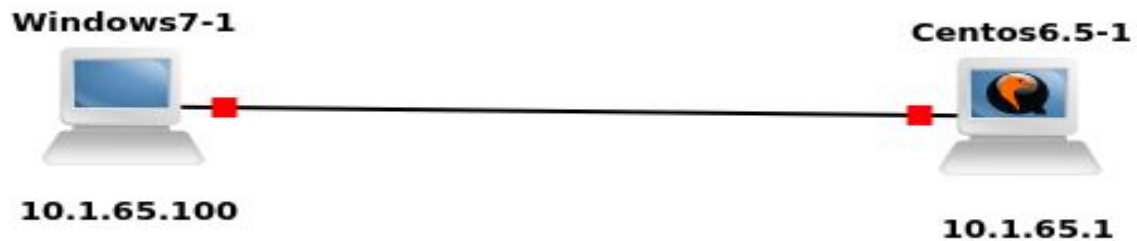


Nguyễn Văn Mạnh

Triển khai giao thức SSH

Mô hình mạng

— — —



Cài đặt

Tạo một vmnet cho vmware

Tạo vmnet2 cho vmware với:

Subnet ip: 10.1.65.0

Subnet mask: 255.255.255.0

Máy ảo window 7

Cài đặt máy ảo window 7, được cắm vào vmnet2.

Đặt địa chỉ ip: 10.1.65.100

Máy ảo Centos

Cài đặt máy ảo Centos, được cắm vào vmne2.

Địa chỉ ip: 10.1.65.1

Cài đặt một vmnet cho vmware

Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet IP Address
vmnet0	bridged	auto-bridging	—	—	—
vmnet1	host-only	none	vmnet1	yes	192.168.160.0
vmnet2	host-only	none	vmnet2	yes	10.1.65.0
vmnet3	host-only	none	vmnet3	no	172.16.1.0
vmnet4	host-only	none	vmnet4	yes	10.10.10.0
vmnet5	host-only	none	vmnet5	yes	172.16.10.0
vmnet8	NAT	NAT	vmnet8	yes	192.168.244.0

Add Network...

Remove Network

vmnet2

☐ Bridged (connect VMs directly to the external network)

Bridged to:

Automatic

Automatic Settings...

☐ NAT (share host's IP address with VMs)

NAT Settings...

☒ Host-only (connect VMs internally in a private network)

☒ Use local DHCP service to distribute IP addresses to VMs

☒ Connect a host virtual adapter (vmnet2) to this network

Subnet IP:

10 . 1 . 65 . 0

 Subnet mask:

255.255.255. 0

Leave blank to automatically select an unused subnet IP.

Help

Cancel

Save

Máy ảo win 7

Activities T7 Thg 3 2, 00:33 100%

Windows 7 - VMware Workstation

File Edit View VM Tabs Help

Library

Type here to search

- My Computer
 - Windows 7
 - CentOS6 64-bit
- Shared VMs

Windows 7 CentOS6 64-bit

Windows 7

Network Adapter cắm vào vmnet2

Start up this guest operating system

Edit virtual machine settings

▼ Devices

Memory	1,1 GB
Processors	1
Hard Disk (SCSI)	40 GB
CD/DVD (SATA)	...s7-pro-32bit.iso
Network Adapter	...m (/dev/vmnet2)
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

▼ Description

Type here to enter a description of this virtual machine.

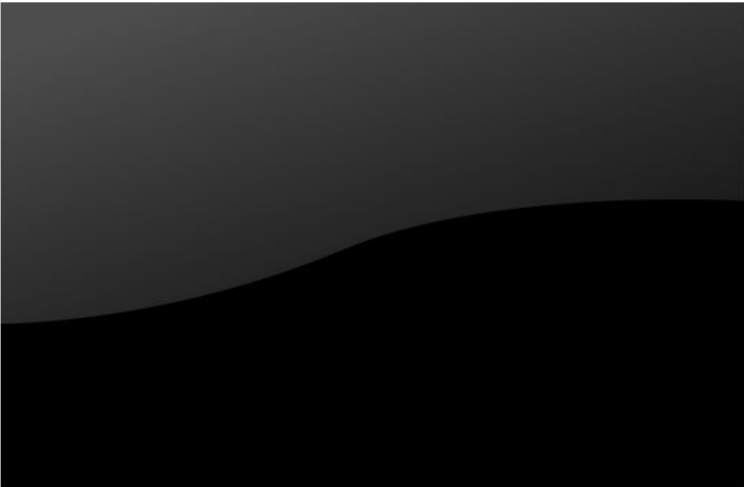
▼ Virtual Machine Details

State: Powered Off

Configuration file: /media/nguyenmanh/data/Windows 7/Windows 7.vmx

Hardware compatibility: Workstation 15.x virtual machine

Primary IP address: Network information is not available



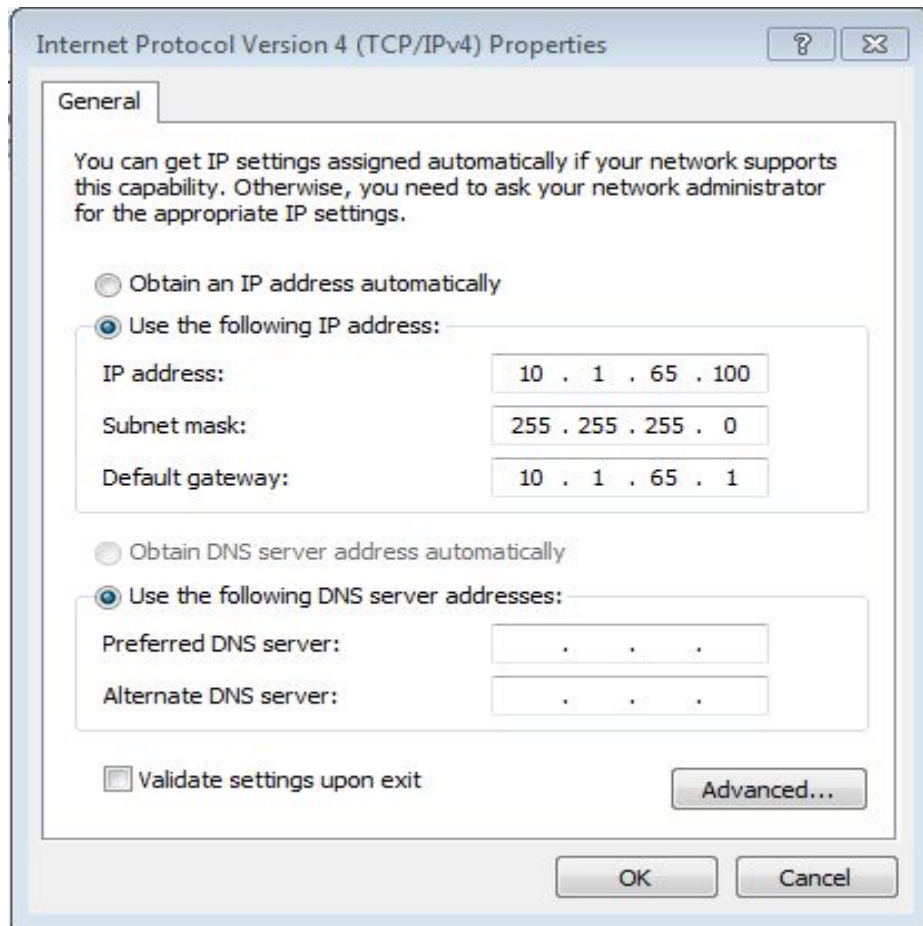
Máy ảo win 7

Cài đặt ip tĩnh cho win 7.

Địa chỉ ip: 10.1.65.100

Subnet mask: 255.255.255.0

Default gateway: 10.1.65.1



Máy ảo Centos










CentOS6 64-bit

 Start up this guest operating system

 Edit virtual machine settings

 Upgrade this virtual machine

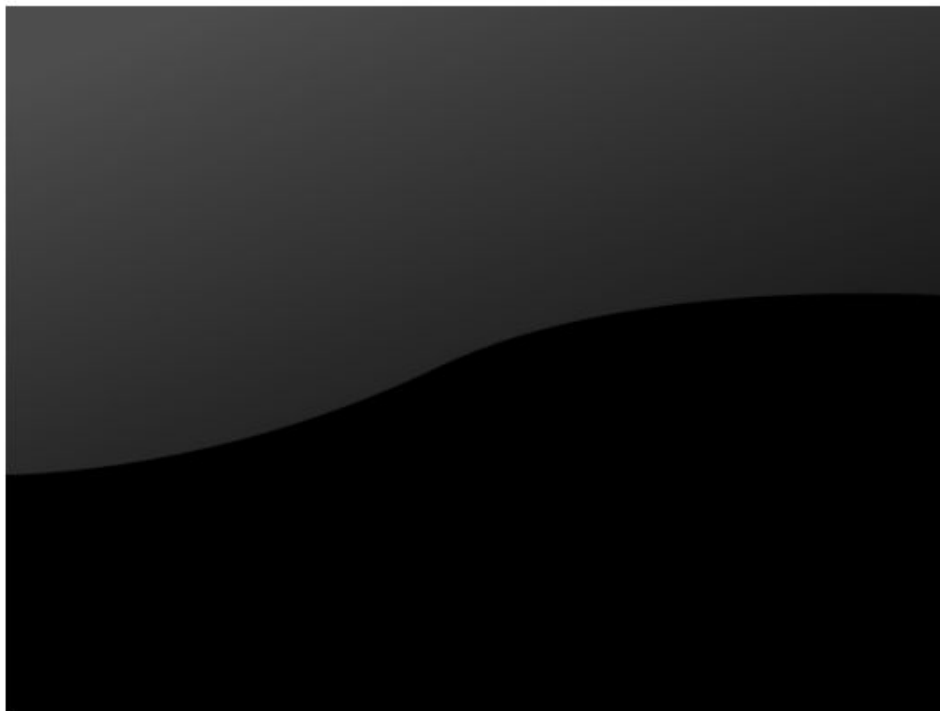
▼ Devices

 Memory	1,2 GB
 Processors	1
 Hard Disk (SCSI)	30 GB
 CD/DVD (IDE)	...6 64-minimal.iso
 Network Adapter	...m (/dev/vmnet2)
 USB Controller	Present
 Sound Card	Auto detect
 Printer	Present
 Display	Auto detect

▼ Description

Type here to enter a description of this virtual machine.

Máy ảo Centos cắm vào vmnet2



▼ Virtual Machine Details

State: Powered Off

Configuration file: /media/nguyenmanh/data/CentOS6 64-bit/CentOS6 64-bit.vmx

Máy ảo Centos

— — —

Cài đặt ip tĩnh cho centos.

Địa chỉ ip: 10.1.65.1

Subnet mask: 255.255.255.0

Default gateway: 10.1.65.1

```
[root@localhost ~]# sudo ifconfig eth0 10.1.65.1 netmask 255.255.255.0
[root@localhost ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:45:57:B3
          inet addr:10.1.65.1  Bcast:10.1.65.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe45:57b3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:39 errors:0 dropped:0 overruns:0 frame:0
          TX packets:28 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6695 (6.5 KiB)  TX bytes:3464 (3.3 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:240 (240.0 b)  TX bytes:240 (240.0 b)

[root@localhost ~]#
```


SSH xác thực bằng mật khẩu.

Trên máy window 7

Cài đặt ứng dụng có tên là
putty.

SSH vào máy centos bằng username
và mật khẩu.

Trên máy Centos

Mặc định Centos đã mở dịch vụ
ssh trên cổng 22.

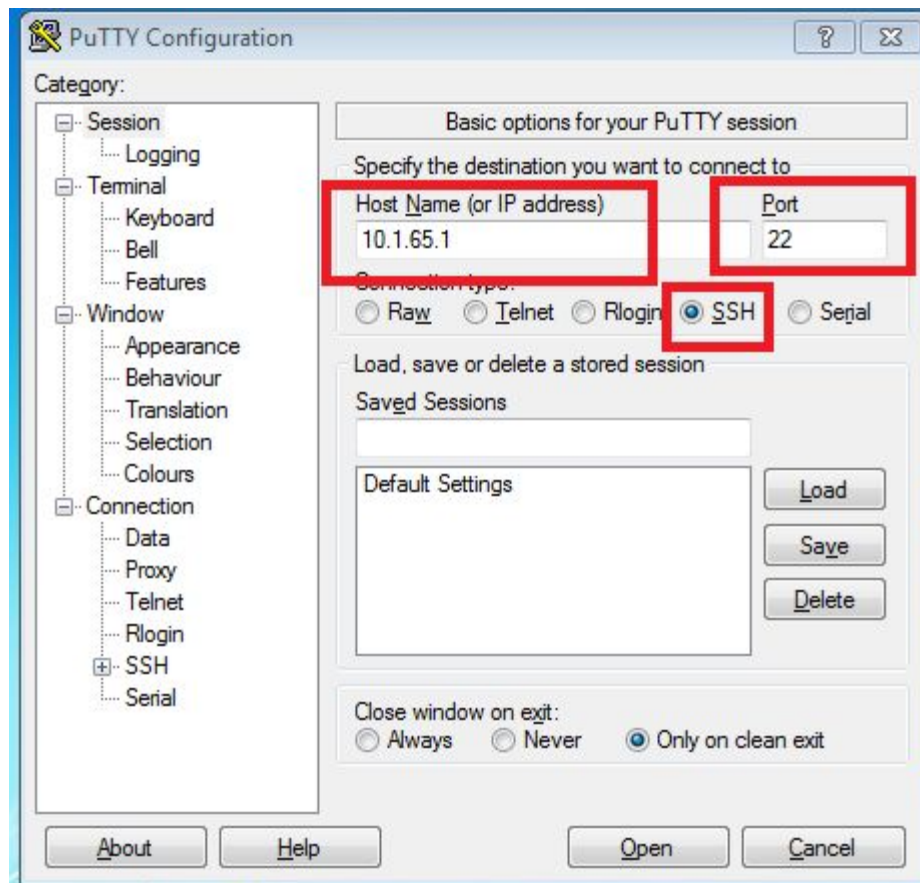
Trên wireshark

Lắng nghe trên interface vmnet2.

— — —

Trên máy window 7

Mở ứng dụng PuTTY và SSH vào địa chỉ của máy Centos (10.1.65.1) với cổng 22.



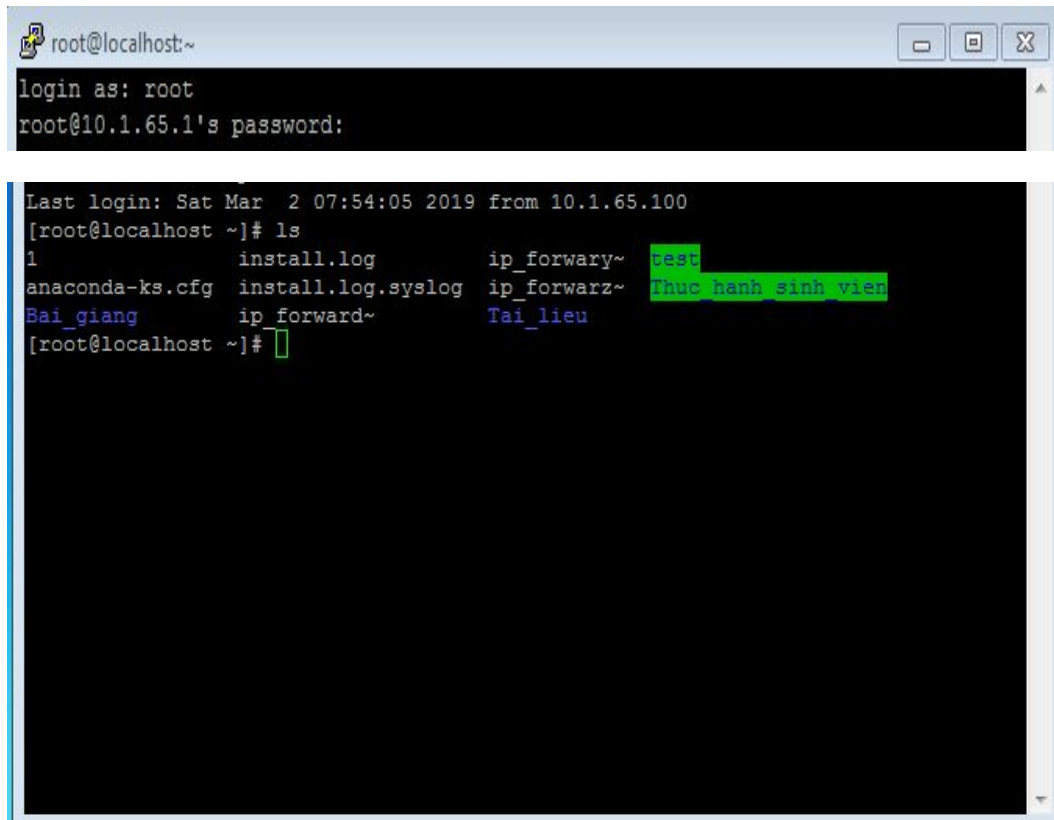
Trên máy window 7

— — —

Khi SSH được yêu cầu nhập tài khoản, mật khẩu để xác thực.

Sau khi nhập đúng tài khoản, mật khẩu, đã vào được Centos.

Bây giờ chạy một lệnh nào đó (ví dụ: `ls`) để kiểm tra.



```
root@localhost~
login as: root
root@10.1.65.1's password:

Last login: Sat Mar  2 07:54:05 2019 from 10.1.65.100
[root@localhost ~]# ls
1                  install.log          ip_forwary~      test
anaconda-ks.cfg    install.log.syslog  ip_forwarz~      Thuc_hanh_sinh_vien
Bai_giang          ip_forward~        Tai_lieu
```

Trên Wireshark

Welcome to Wireshark

Capture

...using this filter:



Enter a capture filter ...

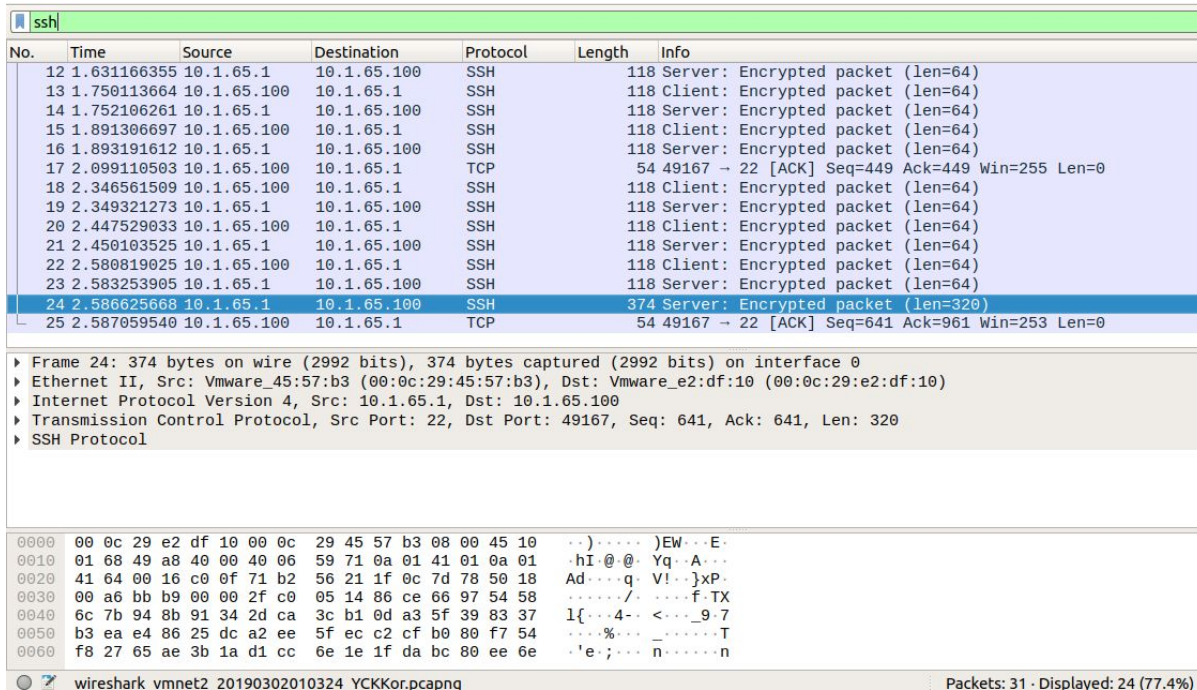
All interfaces shown

wlo1	
vmnet1	
vmnet2	
vmnet3	
vmnet4	
vmnet5	
vmnet8	
any	
Loopback: lo	
enp8s0	
virbr0	
docker0	
br-f11459b38e68	
br-0af671dfd990	
bluetooth0	
nflog	
nfqueue	
usbmon1	
usbmon2	

Learn

Trên wireshark

Bạn sẽ chặn bắt được các gói tin ssh trên wireshark, nhưng các gói tin này đều ở dạng mã hóa.



No.	Time	Source	Destination	Protocol	Length	Info
12	1.631166355	10.1.65.1	10.1.65.100	SSH	118	Server: Encrypted packet (len=64)
13	1.750113664	10.1.65.100	10.1.65.1	SSH	118	Client: Encrypted packet (len=64)
14	1.752106261	10.1.65.1	10.1.65.100	SSH	118	Server: Encrypted packet (len=64)
15	1.891306697	10.1.65.100	10.1.65.1	SSH	118	Client: Encrypted packet (len=64)
16	1.893191612	10.1.65.1	10.1.65.100	SSH	118	Server: Encrypted packet (len=64)
17	2.099110503	10.1.65.100	10.1.65.1	TCP	54	49167 → 22 [ACK] Seq=449 Ack=449 Win=255 Len=0
18	2.346561509	10.1.65.100	10.1.65.1	SSH	118	Client: Encrypted packet (len=64)
19	2.349321273	10.1.65.1	10.1.65.100	SSH	118	Server: Encrypted packet (len=64)
20	2.447529033	10.1.65.100	10.1.65.1	SSH	118	Client: Encrypted packet (len=64)
21	2.450103525	10.1.65.1	10.1.65.100	SSH	118	Server: Encrypted packet (len=64)
22	2.580819025	10.1.65.100	10.1.65.1	SSH	118	Client: Encrypted packet (len=64)
23	2.583253905	10.1.65.1	10.1.65.100	SSH	118	Server: Encrypted packet (len=64)
24	2.586625668	10.1.65.1	10.1.65.100	SSH	374	Server: Encrypted packet (len=320)
25	2.587059540	10.1.65.100	10.1.65.1	TCP	54	49167 → 22 [ACK] Seq=641 Ack=961 Win=253 Len=0

▶ Frame 24: 374 bytes on wire (2992 bits), 374 bytes captured (2992 bits) on interface 0
▶ Ethernet II, Src: Vmware_45:57:b3 (00:0c:29:45:57:b3), Dst: Vmware_e2:df:10 (00:0c:29:e2:df:10)
▶ Internet Protocol Version 4, Src: 10.1.65.1, Dst: 10.1.65.100
▶ Transmission Control Protocol, Src Port: 22, Dst Port: 49167, Seq: 641, Ack: 641, Len: 320
▶ SSH Protocol

0000	00 0c 29 e2 df 10 00 0c	29 45 57 b3 08 00 45 10	..).....)EW...E..
0010	01 68 49 a8 40 00 40 06	59 71 0a 01 41 01 0a 01	.hI.@.@.Yq..A...
0020	41 64 00 16 c0 0f 71 b2	56 21 1f 0c 7d 78 50 18	Ad....q.V!...}xP
0030	00 a6 bb b9 00 00 2f c0	05 14 86 ce 66 97 54 58/.f.TX
0040	6c 7b 94 8b 91 34 2d ca	3c b1 0d a3 5f 39 83 37	l{...4...<..._9.7
0050	b3 ea e4 86 25 dc a2 ee	5f ec c2 cf b0 80 f7 54	...%..._.....T
0060	f8 27 65 ae 3b 1a d1 cc	6e 1e 1f da bc 80 ee 6e	.!e;...n.....n

wireshark vmnet2 20190302010324 YCKKor.pcapng Packets: 31 · Displayed: 24 (77.4%)

SSH bằng mã khóa công khai

Trên máy window 7

Cài đặt ứng dụng có tên là putty và Putty gen.

SSH vào máy centos bằng mã khóa công khai.

Trên máy Centos

Mặc định Centos đã mở dịch vụ ssh trên cổng 22.

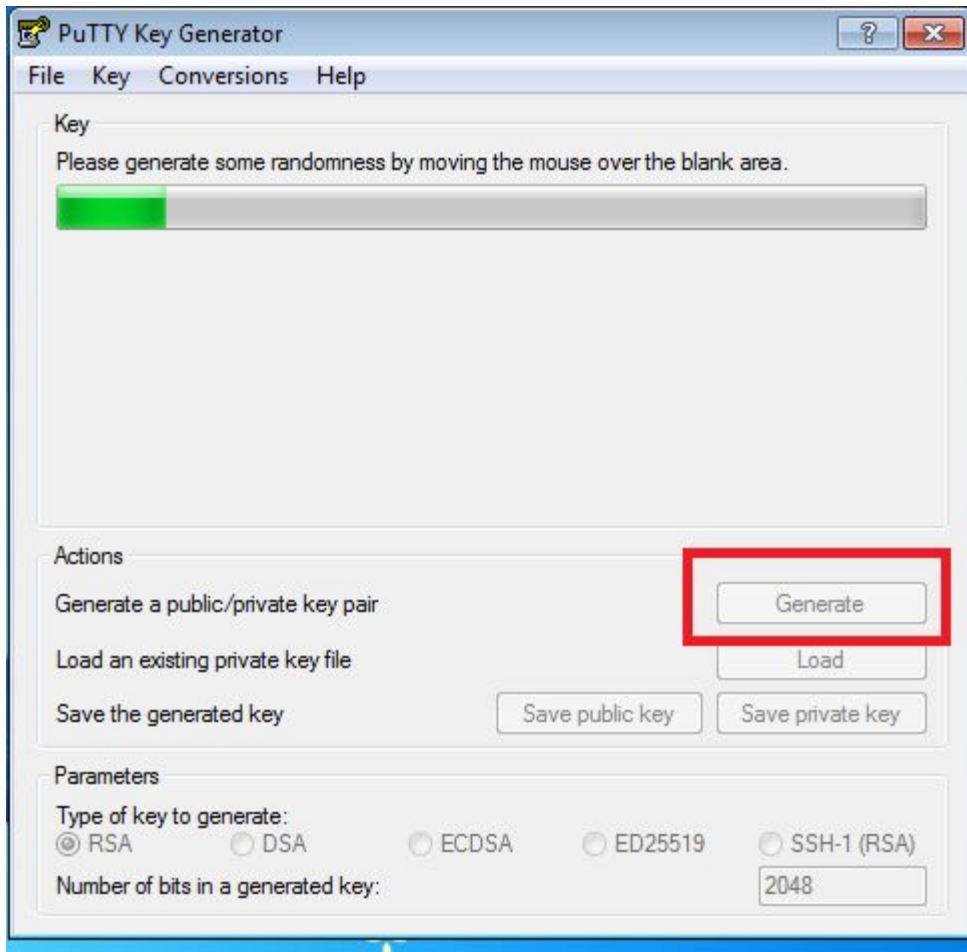
Thêm mã khóa công khai của máy window 7.

Trên wireshark

Lắng nghe trên interface vmnet2.

Trên máy window 7

Mở ứng dụng Putty gen, chọn vào mục generate để tạo key.



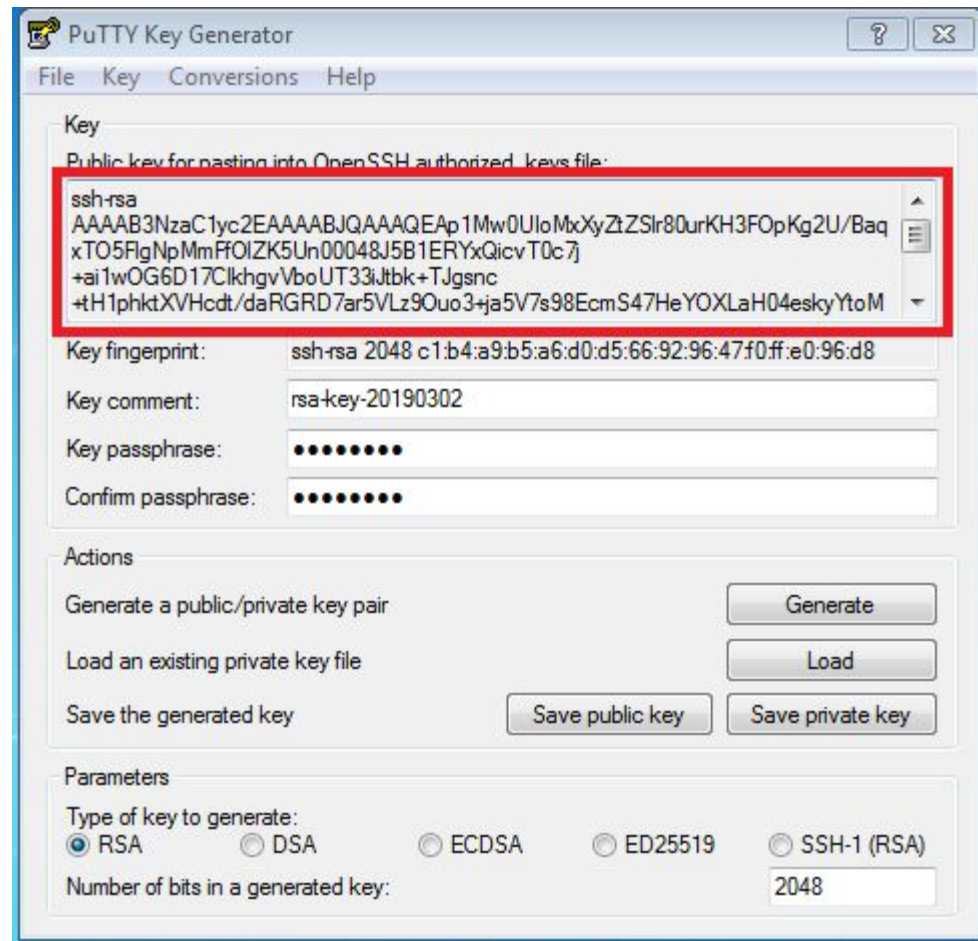
Trên máy window 7

Nhập mật khẩu cho **Key passphrase** và **Confirm passphrase** nếu như bạn muốn sử dụng mật khẩu cho khóa riêng tư.

Nhấn **save public key** để lưu mã khóa công khai của bạn.

Nhấn **save private key** để lưu khóa bí mật của bạn.

Copy mã **public key**.



Trên máy Centos.

— — —

Tạo thư mục **.ssh** trong thư mục **Home** của **user**.

Tạo file **authorized_keys** trong thư mục **.ssh**

```
[root@localhost ~]# mkdir ~/.ssh
```

```
[root@localhost ~]# nano ~/.ssh/authorized_keys
```

Trên máy Centos

— — —

Thêm **public key** copy từ
window 7 vào file
authorized_keys.

Thiết lập quyền cho thư mục
.ssh và file
authorized_keys.

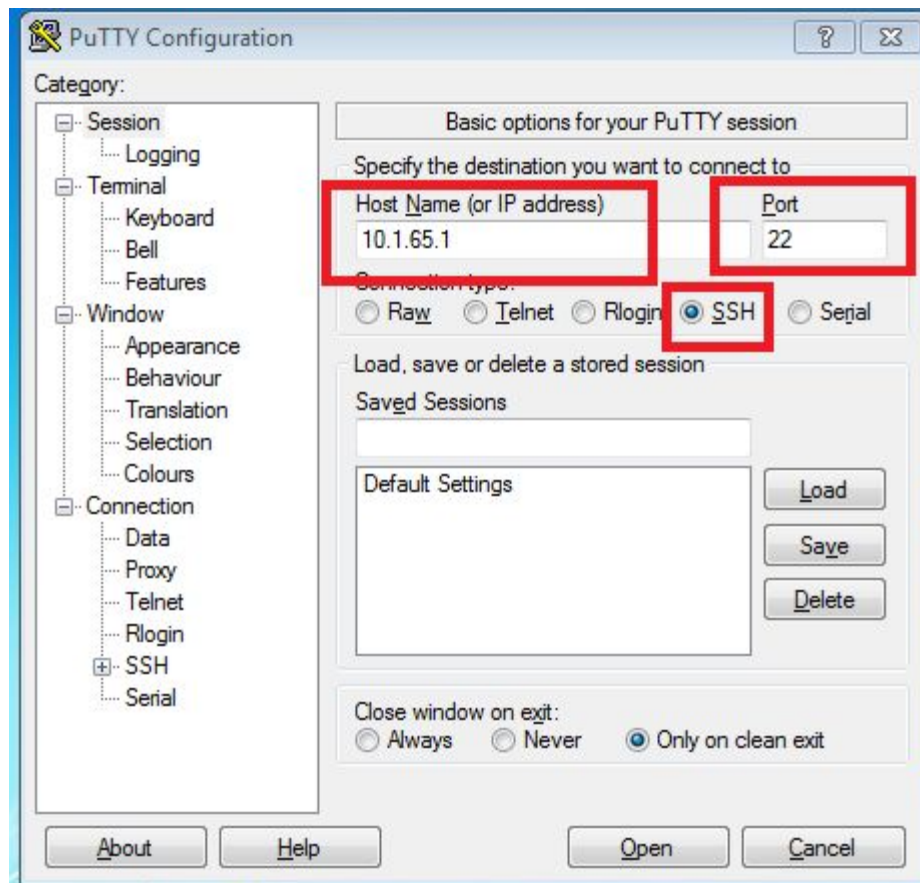
```
GNU nano 2.0.9      File: /root/.ssh/authorized_keys      Modified
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAp1Mw0UIoMxXyZtZS1r80urKH3F0pKg2U/BaqxT05Flg$

^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^U Next Page  ^U UnCut Text ^T To Spell
```

```
[root@localhost ~]# chmod 700 ~/.ssh
[root@localhost ~]# chmod 600 ~/.ssh/authorized_keys
```

Trên máy window 7

Mở ứng dụng PuTTY và SSH vào địa chỉ của máy Centos (10.1.65.1) với cổng 22.

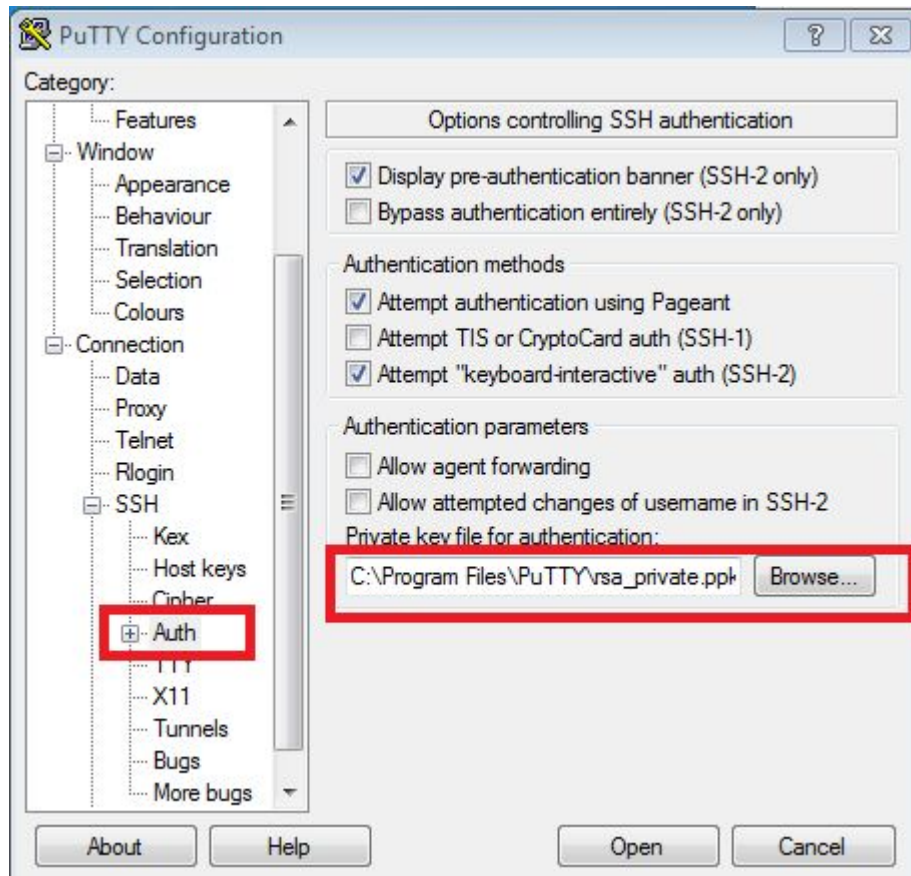


Trên máy window 7

Chọn SSH -> Auth

Chọn file **private key** đã lưu.

Bấm open để SSH.



khẩu nữa.

```
root@localhost:~  
login as: root  
Authenticating with public key "rsa-key-20190302"  
Last login: Sat Mar  2 08:45:35 2019 from 10.1.65.100  
[root@localhost ~]# ls  
1          install.log          ip_forwary~  test  
anaconda-ks.cfg  install.log.syslog  ip_forwarz~  Thuc_hanh_sinh_vien  
Bai_giang      ip_forward~        Tai_lieu  
[root@localhost ~]#
```

Trên wireshark

Trên wireshark đã bắt được các gói tin SSH nhưng tất cả dữ liệu đều đã được mã hóa.

ssh						
No.	Time	Source	Destination	Protocol	Length	Info
12	1.631166355	10.1.65.1	10.1.65.100	SSH	118	Server: Encrypted packet (len=64)
13	1.750113664	10.1.65.100	10.1.65.1	SSH	118	Client: Encrypted packet (len=64)
14	1.752106261	10.1.65.1	10.1.65.100	SSH	118	Server: Encrypted packet (len=64)
15	1.891306697	10.1.65.100	10.1.65.1	SSH	118	Client: Encrypted packet (len=64)
16	1.893191612	10.1.65.1	10.1.65.100	SSH	118	Server: Encrypted packet (len=64)
17	2.099110503	10.1.65.100	10.1.65.1	TCP	54	49167 → 22 [ACK] Seq=449 Ack=449 Win=255 Len=0
18	2.346561509	10.1.65.100	10.1.65.1	SSH	118	Client: Encrypted packet (len=64)
19	2.349321273	10.1.65.1	10.1.65.100	SSH	118	Server: Encrypted packet (len=64)
20	2.447529033	10.1.65.100	10.1.65.1	SSH	118	Client: Encrypted packet (len=64)
21	2.450103525	10.1.65.1	10.1.65.100	SSH	118	Server: Encrypted packet (len=64)
22	2.580819025	10.1.65.100	10.1.65.1	SSH	118	Client: Encrypted packet (len=64)
23	2.583253905	10.1.65.1	10.1.65.100	SSH	118	Server: Encrypted packet (len=64)
24	2.586625668	10.1.65.1	10.1.65.100	SSH	374	Server: Encrypted packet (len=320)
25	2.587059540	10.1.65.100	10.1.65.1	TCP	54	49167 → 22 [ACK] Seq=641 Ack=961 Win=253 Len=0
▶ Frame 24: 374 bytes on wire (2992 bits), 374 bytes captured (2992 bits) on interface 0						
▶ Ethernet II, Src: Vmware_45:57:b3 (00:0c:29:45:57:b3), Dst: Vmware_e2:df:10 (00:0c:29:e2:df:10)						
▶ Internet Protocol Version 4, Src: 10.1.65.1, Dst: 10.1.65.100						
▶ Transmission Control Protocol, Src Port: 22, Dst Port: 49167, Seq: 641, Ack: 641, Len: 320						
▶ SSH Protocol						
0000 00 0c 29 e2 df 10 00 0c 29 45 57 b3 08 00 45 10 ..).....)EW...E.						
0010 01 68 49 a8 40 00 00 06 59 71 0a 01 41 01 0a 01 .hI.@.@.Yq..A...						
0020 41 64 00 16 c0 0f 71 b2 56 21 1f 0c 7d 78 50 18 Ad...q. V!...}xP.						
0030 00 a6 bb b9 00 00 2f c0 05 14 86 ce 66 97 54 58/....f-TX						
0040 6c 7b 94 8b 91 34 2d ca 3c b1 0d a3 5f 39 83 37 l{...4-...<..._9-7						
0050 b3 ea e4 86 25 dc a2 ee 5f ec c2 cf b0 80 f7 54%..._.....T						
0060 f8 27 65 ae 3b 1a d1 cc 6e 1e 1f da bc 80 ee 6e .'e.;...n.....n						
wireshark vmnet2 20190302010324 YCKKor.pcapng						
Packets: 31 · Displayed: 24 (77.4%)						

▶ Frame 34: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface 0	
▶ Ethernet II, Src: Vmware_e2:df:10 (00:0c:29:e2:df:10), Dst: Vmware_c0:00:02 (00:50:56:c0:00:02)	
▶ Internet Protocol Version 4, Src: 10.1.65.100, Dst: 10.1.65.1	
▶ Transmission Control Protocol, Src Port: 49167, Dst Port: 22, Seq: 641, Ack: 961, Len: 64	
▼ SSH Protocol	
Packet Length (encrypted): 69018d0b	
Encrypted Packet: 8b65b032d6a2005713910ada65e03ae06e716636e4385709...	

Trên đây là toàn bộ bài làm về SSH

Liên hệ

— — —

Nguyễn Văn Mạnh

Lớp: AT12c

Mã sinh viên: AT120336

Mail: nguyenmanh0397@gmail.com

SĐT: 0329653569

