

Triển khai giao thức SSH

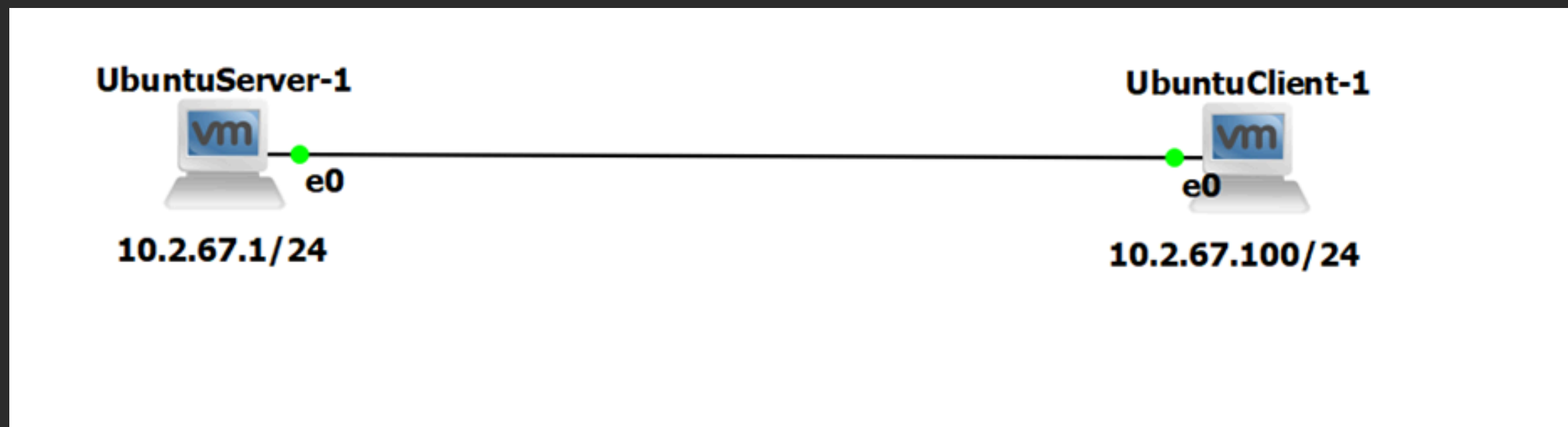
Nguyễn Đức Việt - AT190256



Giao thức Telnet

- Là giao thức mạng được sử dụng rộng rãi để truy cập và quản lý thiết bị từ xa

- SSH giúp bạn đăng nhập vào môi trường máy tính khác qua mạng và cho phép thực hiện các lệnh trên một máy từ xa
- Giao thức SSH mã hóa lưu lượng truy cập theo cả hai hướng, giúp bạn ngăn chặn việc đánh cắp mật khẩu



Thiết lập hệ thống

03

```
ubuntuuser@server:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.25.135 netmask 255.255.255.0 broadcast 192.168.25.255
    inet6 fe80::d32e:a2d6:ba0a:2637 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:6b:5d:09 txqueuelen 1000 (Ethernet)
    RX packets 2268 bytes 1226172 (1.2 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 601 bytes 60122 (60.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens34: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.2.67.1 netmask 255.255.255.0 broadcast 10.2.67.255
    inet6 fe80::901:243a:3e57:30bc prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:6b:5d:13 txqueuelen 1000 (Ethernet)
    RX packets 3100 bytes 376832 (376.8 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 844 bytes 74248 (74.2 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 728 bytes 96218 (96.2 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 728 bytes 96218 (96.2 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

SERVER: WIN2012

```
root@client:~# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.25.136 netmask 255.255.255.0 broadcast 192.168.25.255
    inet6 fe80::8636:cd4b:11b0:6f62 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:80:bd:3d txqueuelen 1000 (Ethernet)
    RX packets 2253 bytes 1220379 (1.2 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 649 bytes 63536 (63.5 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens34: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.2.67.100 netmask 255.255.255.0 broadcast 10.2.67.255
    inet6 fe80::22ca:881d:a2ea:e8ad prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:80:bd:47 txqueuelen 1000 (Ethernet)
    RX packets 3033 bytes 367431 (367.4 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 815 bytes 73732 (73.7 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

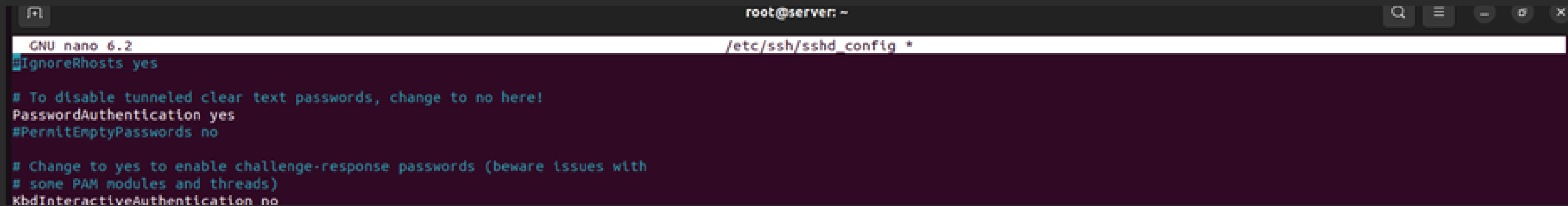
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 758 bytes 96202 (96.2 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 758 bytes 96202 (96.2 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

CLIENT: WIN7



Cấu hình miễn và Telnet

- apt-get install openssh-server
- Chỉnh sửa cấu hình ở file /etc/ssh/sshd_config TRÊN CẢ 2 MÁY



```
root@server: ~
GNU nano 6.2 /etc/ssh/sshd_config *
IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication yes
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
KbdInteractiveAuthentication no
```



Quá trình thực hiện SSH

05

Thực hiện
service sshd restart
trên cả 2 máy

```
root@server:~# service sshd restart
root@server:~# service sshd status
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2025-03-09 21:38:14 +07; 9s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Process: 3419 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 3421 (sshd)
    Tasks: 1 (limit: 2213)
   Memory: 1.7M
      CPU: 46ms
   CGroup: /system.slice/ssh.service
           └─3421 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Thg 3 09 21:3 root@server:~# service sshd restart
Thg 3 09 21:3 root@server:~# service sshd status
Thg 3 09 21:3 ● ssh.service - OpenBSD Secure Shell server
Thg 3 09 21:3    Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
Thg 3 09 21:3    Active: active (running) since Sun 2025-03-09 21:37:29 +07; 19s ago
Thg 3 09 21:3      Docs: man:sshd(8)
Thg 3 09 21:3            man:sshd_config(5)
Thg 3 09 21:3  Process: 3506 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
root@server:~# Main PID: 3507 (sshd)
Thg 3 09 21:3    Tasks: 1 (limit: 2213)
Thg 3 09 21:3   Memory: 1.7M
Thg 3 09 21:3      CPU: 60ms
Thg 3 09 21:3   CGroup: /system.slice/ssh.service
Thg 3 09 21:3           └─3507 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Thg 3 09 21:37:29 client systemd[1]: Starting OpenBSD Secure Shell server...
Thg 3 09 21:37:29 client sshd[3507]: Server listening on 0.0.0.0 port 22.
Thg 3 09 21:37:29 client sshd[3507]: Server listening on :: port 22.
Thg 3 09 21:37:29 client systemd[1]: Started OpenBSD Secure Shell server.
```

05



tại máy client: ubuntuserver@10.2.67.1

```
ubuntuserver@10.2.67.1's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-52-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

202 updates can be applied immediately.
144 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

New release '24.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sun Mar  9 17:09:16 2025 from client
ubuntuserver@server:~$
```



Bắt gói tin Wireshark

872	1062.344383	10.2.67.100	10.2.67.1	SSHv2	108 Client: Protocol (SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.11)
874	1062.365336	10.2.67.1	10.2.67.100	SSHv2	108 Server: Protocol (SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.11)
877	1062.365961	10.2.67.100	10.2.67.1	SSHv2	154 Client: Key Exchange Init
878	1062.368500	10.2.67.1	10.2.67.100	SSHv2	1178 Server: Key Exchange Init
879	1062.372302	10.2.67.100	10.2.67.1	SSHv2	114 Client: Elliptic Curve Diffie-Hellman Key Exchange Init
880	1062.381916	10.2.67.1	10.2.67.100	SSHv2	590 Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys,
948	1141.178896	10.2.67.100	10.2.67.1	SSHv2	108 Client: Protocol (SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.11)
950	1141.194635	10.2.67.1	10.2.67.100	SSHv2	108 Server: Protocol (SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.11)
953	1141.195468	10.2.67.100	10.2.67.1	SSHv2	154 Client: Key Exchange Init
954	1141.199804	10.2.67.1	10.2.67.100	SSHvv2	1178 Server: Key Exchange Init
955	1141.202226	10.2.67.100	10.2.67.1	SSHv2	114 Client: Elliptic Curve Diffie-Hellman Key Exchange Init
956	1141.209285	10.2.67.1	10.2.67.100	SSHv2	590 Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys,
958	1145.738172	10.2.67.100	10.2.67.1	SSHv2	82 Client: New Keys
960	1145.779420	10.2.67.100	10.2.67.1	SSHv2	110 Client: Encrypted packet (len=44)
962	1145.780322	10.2.67.1	10.2.67.100	SSHv2	110 Server: Encrypted packet (len=44)
964	1145.780964	10.2.67.100	10.2.67.1	SSHv2	134 Client: Encrypted packet (len=68)
965	1145.788479	10.2.67.1	10.2.67.100	SSHv2	118 Server: Encrypted packet (len=52)
967	1152.803030	10.2.67.100	10.2.67.1	SSHv2	214 Client: Encrypted packet (len=148)

Quá trình trên sử dụng SSH version2 để truy nhập vào server. xảy ra quá trình trao đổi khóa và mã hóa dữ liệu



Quá trình SSH truy cập từ Server từ Client được thấy rõ trong TCP Stream được mã hóa hoàn toàn



Kết luận

13

- Cung cấp xác thực mạnh mẽ và liên lạc an toàn qua các kênh không an toàn
- SSH cho phép người dùng đăng nhập vào một máy tính khác qua mạng không an toàn một cách an toàn
- Cung cấp quyền riêng tư cho dữ liệu của bạn thông qua mã hóa mạnh
- Tính toàn vẹn của thông tin liên lạc được thực hiện theo cách mà nó không bị thay đổi
- SSH không thể bảo vệ người sử dụng khỏi các tấn công được thực hiện thông qua các giao thức khác

