Mô tả tính năng SSH tunnel

1. Mục tiêu

SSH tunnel được sử dụng:

- Quản trị viên có thể truy cập vào AP ở các mạng cục bộ khác nhau.
- Truy cập vào AP mà không cần phải mở port modem.

2. Yêu cầu

Server và AP phải cài đặt một số phần mềm dưới đây để có thể thiết lập được tunnel

- Phần mềm máy chủ SSH- SSH server
- Phần mềm tạo và giải mã hex file (xxd tool – Dùng cho mục đích tạo và giải mã keypair do server tạo ra)

3. Cấu hình và thao tác với tunnel

3.1. Quy trình thiết lập tunnel giữa server và AP

Bước 1: Server lựa chọn một unused port.

Bước 2: Server chủ động tạo keypair: public key cho server, private key cho AP. Private key được tạo thành công sẽ được trả về dưới dạng chuỗi kí tự

Bước 3: Server copy chuỗi kí tự, tạo thành file, và gửi xuống AP thông qua TMS server

Bước 4: AP nhận private key từ TMS server, chuyển đổi private key về định dạng ban đầu

Bước 5: AP tiến hành tạo SSH tunnel tới server

Bước 6: Sau khi AP tạo tunnel thành công, lúc này server đã có thể truy cập ngược vào AP bằng cách khởi tạo phiên SSH tới remote port (unsused port đã chọn ở bước 1).

Bước 7: Server nhập password để có thể truy cập vào AP

Bước 8: Sau khi thao tác xong các công việc ở AP, admin của thể hủy tunnel đã thiết lập

3.2. Mô tả chi tiết cấu hình và thao tác với tunnel

- Đầu tiên ta cần cấu hình cho server có thể xác thực dùng keypair
  - Mở file **/etc/ssh/sshd_config**.
    - Enable comment **PubkeyAuthentication yes**
    - Điền đường dẫn tới nơi lưu trữ keypair khi tạo ra. Mặc định việc cấu hình như sau.

```
PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
AuthorizedKeysFile      .ssh/authorized_keys
```

    - Thêm cấu hình thuật toán trao đổi khóa vào file cấu hình.
      - Việc thêm cấu hình thuật toán trao đổi khóa này là do server và AP đang sử dụng hai loại SSH khác nhau (server đang chạy openSSH, còn AP đang chạy Dropbear SSH) nên cấu hình mặc định của server không hỗ trợ các giải thuật trao đổi khóa đã cũ.

```
#Legacy changes
KexAlgorithms +diffie-hellman-group14-sha1,diffie-hellman-group1-sha1
```

  - Server khởi động lại service sshd để nạp lại các thay đổi trong file cấu hình.

    sudo service sshd restart

- Server lựa chọn một unused port

```
tramtn@HOANG:~/backdoor$ ./tunnel-server -g
Unused local port: 32768
```

- Server chủ động tạo ra hai key: public key cho server và private key cho AP
  - Private key được trả về dưới dạng chuỗi kí tự. Admin copy chuỗi kí tự này và gửi xuống AP qua TMS server.

```
tramtn@HOANG:~/backdoor$ ./tunnel-server -i
Key is created successfuly in /home/tramtn/.ssh
/home/tramtn/.ssh/authorized_keys is public key
/home/tramtn/.ssh/id_dropbear is private key
/home/tramtn/.ssh/id_dropbear_hex is private key in hex format. This is for AP
Please copy /home/tramtn/.ssh/id_dropbear_hex content for AP
000000077373682d72736100000003010001000010100 8bec00cb04b7ae
016ccccc34289eccfa26c2f6f02efca7f6873b0315e1e3c138c44d89b75d
05a36c43f4777a63c1493c4a9f3f6ea2fea6eee62fbeda15038e67724584
57f0ebb510a74686be6d3f23d4c9fa8ced3762ef6a5d3cc4e347c8b1616b
1c447f3323739dd77c314d7a8a887b705c8619f96313d42de2454a6a5ae0
19c4ebedcb4692ae36a78bda4204292a2ded7a77d85e3531bbc49b089f19
65e9d7f4bb0417ec55e94323a65987dcc855a1ec9717c535ccc63ccdf6cb
d9781aacfc612693de6fd391455e427a3a13b92908d89880caffa8043f98
c354285979bcaf27219f087ea1e45fd1629e108ea76442ae6435ddd65764
dc1412bec3a97e3f9d0000010013a98ef4f88d3d410b027e81a7e1a4e954
301a9666ebef4877f965761a3fb0a3e306085fc18d2cc966854092ecd8b9
0b656b1a75582753db0772d72d7b3d7c31f23f6d99140c736dcb2be07c7b
0a9fe4e39b3759906a713d6fabbdf93859adff84173d52e8a347387b9302
b4a20f3c9da80d00753ef3dad1fabeacc107d00c64ad6dce806b8db01fa6
d1bcd7b0410c4095d2e7cebe251c27ac848428f836e910e45c38811bcb97
e46ff308ffa437dbcb31e77a0c0de6a8962302995c3c99175e431f5ba3c8
6d21923688bc308aa612f3c04fa7c599f8a7a2537101af2571430da68d99
271acb992d8012bcaaf898425e7a813405cf3fd4a2918c1111c99e6d8b00
00008100c2f1d30e82e85183aed4c260ada07658293c5e01af6bdc2c30c2
c6ba9e78f7a54cdf4a9eb788bb1c1de63bec97ced185c22461135da16c9d
54766196e724191d67ff77033bb71194dc4ff54a07bafcd8a197f43bdf54
6068edab049a53e4ff9b48fe90e252b44fc8c921ccd1a4196fe2f837f3cc
62314db6cf746dbf2e3f79770000008100b7be9798ce8f1da19d191dc2ec
ccd1ddcc432b98d5bc14972951e4d03828db053582b896b4710349bb5d8c
2dfa5dd2949eca0dec0a28320801056ddd4614f27bc3c02bf5d155f130c6
949d0ee0ee76db6241e98c4fddf4f3ac3d438e52f523d8d2b81cee823f47
168f45bb15e147160ec4e68380bba3c78cf27cbf75e746148b
```

- AP nhận chuỗi private key từ server (chuỗi private key sẽ được lưu trữ trong file). Sau đó AP chuyển đổi format của key và dùng key này để thiết lập tunnel đến remote port ở server
    - Chuyển đổi format của private key (file hex chứa chuỗi private key nhận được từ server)

      ```
      root@vthomeap:~# tunnel -r hex
      Private key is created successfully
      ```

    - Dùng private key đã chuyển đổi format để thiết lập tunnel đến remote port của server

```
root@vthomeap:~# tunnel -s -L 45.35.14.82 -rp 32768 -lp 22 -p 22 -u tramtn
URL       : 45.35.14.82
username  : tramtn
rp        : 32768
lp        : 22
p         : 22
dbclient:
Host '45.35.14.82' key accepted unconditionally.
(ssh-rsa fingerprint md5 ac:8d:49:39:6b:29:a1:46:63:9e:a4:b7:79:29:88:5d)

Start tunnel successfully with 5341
```

- Sau khi AP thiết lập thành công tunnel, server tiến hành phiên ssh tới remote port, remote port chính là unused port đã chọn ở bước 1

```
tramtn@HOANG:~/backdoor$ ./tunnel-server -c 32768
dbclient:
Host '127.0.0.1' key accepted unconditionally.
(ssh-rsa fingerprint sha1!! 49:74:5f:88:22:64:8f:fc:87:88:56:02:90:c0:47:5f:ee:52
:7b:15)

root@127.0.0.1's password:
```

- Sau đó, admin tiến hành nhập password của AP để có thể truy cập vào AP.

```
tramtn@HOANG:~/backdoor$ ./tunnel-server -c 32768
dbclient:
Host '127.0.0.1' key accepted unconditionally.
(ssh-rsa fingerprint sha1!! 3c:4a:cb:a1:b6:76:3a:d5:8c:8f:5d:4e:f8:44:bd:84:27:a7:92:61)

root@127.0.0.1's password:


BusyBox v1.23.2 (2023-02-03 09:51:58 UTC) built-in shell (ash)

  _______                     ________        __
 |       |.-----.-----.-----.|  |  |  |.----.|  |_
 |   -   ||  _  |  -__|     ||  |  |  ||   _||   _|
 |_______||   __|_____|__|__||________||__|  |____|
          |__| W I R E L E S S   F R E E D O M
 -----------------------------------------------------
 CHAOS CALMER (Chaos Calmer, unknown)
 -----------------------------------------------------
  * 1 1/2 oz Gin           Shake with a glassful
  * 1/4 oz Triple Sec      of broken ice and pour
  * 3/4 oz Lime Juice      unstrained into a goblet.
  * 1 1/2 oz Orange Juice
  * 1 tsp. Grenadine Syrup
 -----------------------------------------------------
 SDK Revision : 0d4ff16a
 -----------------------------------------------------
root@vthomeap:~#
```

- Sau khi thao tác xong các việc ở AP, admin có thể hủy tunnel đã thiết lập ngay tại console của AP

```
root@vthomeap:~# tunnel -k

dbclient: Connection to root@127.0.0.1:32768 exited: Remote closed the connection
```