Mô phỏng tấn công brute-force và cấu hình Fail2Ban để bảo vệ SSH

1.Cài đặt máy nạn nhân (CentOS 9)

- Cài đặt SSH server

```
sudo dnf install -y openssh-server
sudo systemctl enable sshd –now
sudo systemctl status sshd
```

- Cài đặt fail2ban

```
sudo dnf install -y epel-release
sudo dnf install -y fail2ban
sudo systemctl enable fail2ban --now
```

- Cấu hình fail2ban cho SSH

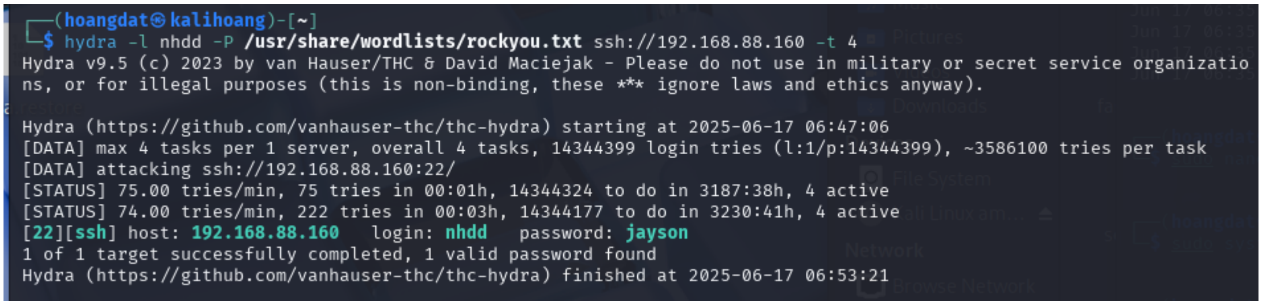
```
sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
sudo nano /etc/fail2ban/jail.local
```

```
Thêm vào [sshd]
[sshd]
enabled = true
port    = ssh
logpath = %(sshd_log)s
backend = systemd
maxretry = 3
findtime = 300
bantime = 600
```

- Khởi động lại dịch vụ

  sudo systemctl restart fail2ban

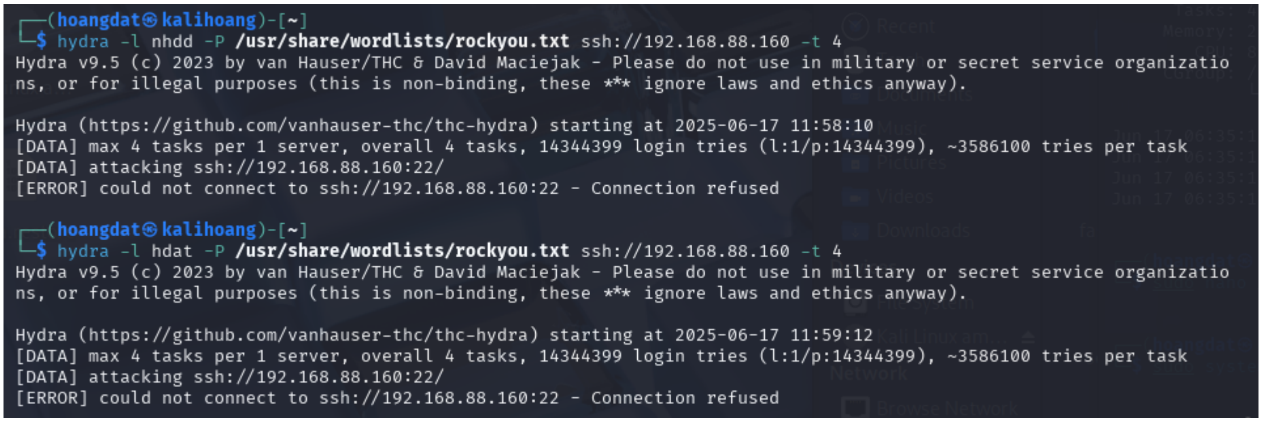
2.Thử tấn công brute-force bằng kali khi chưa cấu hình fail2ban



```
┌──(hoangdat㉿kalihoang)-[~]
└─$ hydra -l nhdd -P /usr/share/wordlists/rockyou.txt ssh://192.168.88.160 -t 4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-17 06:47:06
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.88.160:22/
[STATUS] 75.00 tries/min, 75 tries in 00:01h, 14344324 to do in 3187:38h, 4 active
[STATUS] 74.00 tries/min, 222 tries in 00:03h, 14344177 to do in 3230:41h, 4 active
[22][ssh] host: 192.168.88.160   login: nhdd   password: jayson
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-17 06:53:21
```

3. Thử tấn công brute-force bằng kali khi đã cấu hình fail2ban



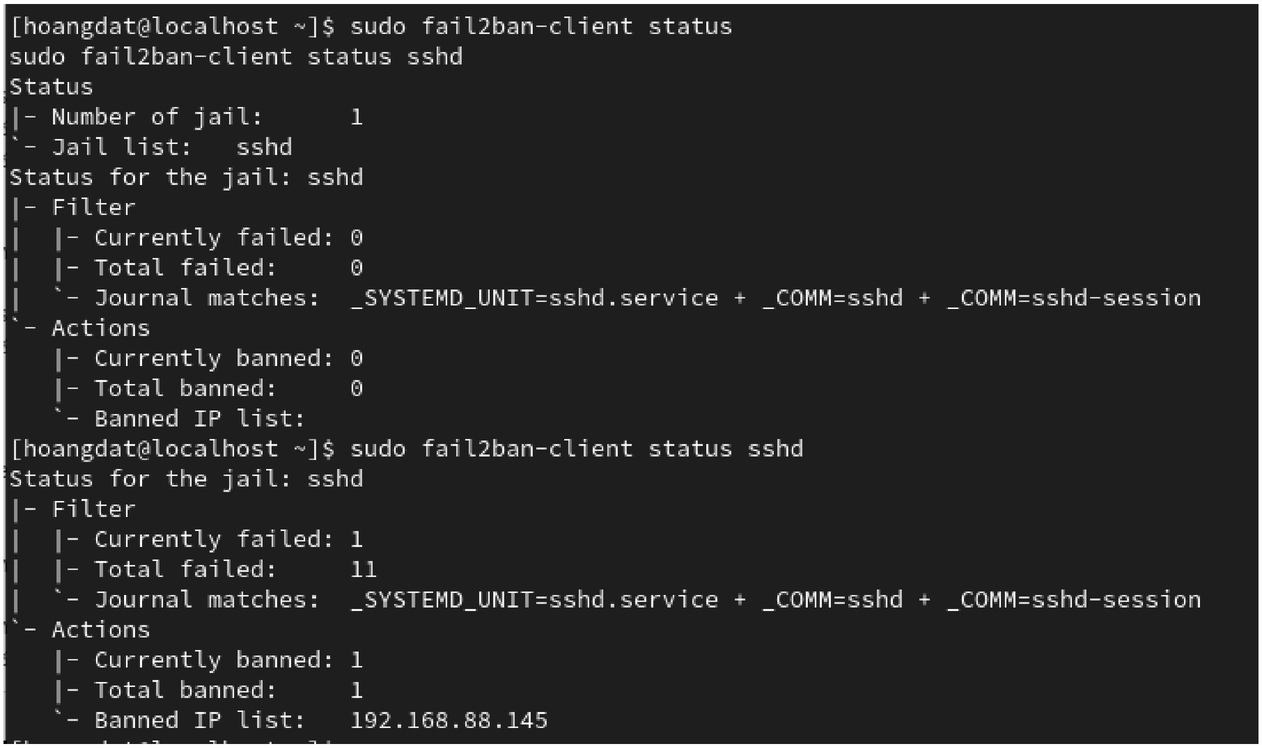
```
┌──(hoangdat㉿kalihoang)-[~]
└─$ hydra -l nhdd -P /usr/share/wordlists/rockyou.txt ssh://192.168.88.160 -t 4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-17 11:58:10
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.88.160:22/
[ERROR] could not connect to ssh://192.168.88.160:22 - Connection refused

┌──(hoangdat㉿kalihoang)-[~]
└─$ hydra -l hdat -P /usr/share/wordlists/rockyou.txt ssh://192.168.88.160 -t 4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-17 11:59:12
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.88.160:22/
[ERROR] could not connect to ssh://192.168.88.160:22 - Connection refused
```

4. Xem trạng thái sshd



```
[hoangdat@localhost ~]$ sudo fail2ban-client status
sudo fail2ban-client status sshd
Status
|- Number of jail:      1
`- Jail list:   sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
[hoangdat@localhost ~]$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 1
|  |- Total failed:     11
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
   |- Currently banned: 1
   |- Total banned:     1
   `- Banned IP list:   192.168.88.145
```

Xuất hiện IP 192.168.88.145 - ip của máy tấn công (Kali) trong danh sách ip bị chặn

5.Log ghi nhận tấn công

```
[hoangdat@localhost ~]$ sudo journalctl -xe | grep sshd
Jun 17 23:09:26 localhost.localdomain sshd[23867]: error: maximum authentication attempts
exceeded for nhdd from 192.168.88.145 port 41110 ssh2 [preauth]
Jun 17 23:09:26 localhost.localdomain sshd[23867]: Disconnecting authenticating user nhdd
192.168.88.145 port 41110: Too many authentication failures [preauth]
Jun 17 23:09:26 localhost.localdomain sshd[23867]: PAM 5 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:09:26 localhost.localdomain sshd[23867]: PAM service(sshd) ignoring max retries; 6
> 3
Jun 17 23:09:26 localhost.localdomain sshd[23865]: error: maximum authentication attempts
exceeded for nhdd from 192.168.88.145 port 41096 ssh2 [preauth]
```

```
Jun 17 23:09:26 localhost.localdomain sshd[23865]: Disconnecting authenticating user nhdd
192.168.88.145 port 41096: Too many authentication failures [preauth]
Jun 17 23:09:26 localhost.localdomain sshd[23865]: PAM 5 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:09:26 localhost.localdomain sshd[23865]: PAM service(sshd) ignoring max retries; 6
> 3
Jun 17 23:09:26 localhost.localdomain sshd[23896]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:09:26 localhost.localdomain sshd[23897]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:09:26 localhost.localdomain sshd[23900]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:09:26 localhost.localdomain sshd[23898]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:09:27 localhost.localdomain sshd[23896]: Failed password for nhdd from
192.168.88.145 port 37216 ssh2
Jun 17 23:09:27 localhost.localdomain sshd[23897]: Failed password for nhdd from
192.168.88.145 port 37214 ssh2
Jun 17 23:09:27 localhost.localdomain sshd[23900]: Failed password for nhdd from
192.168.88.145 port 37248 ssh2
Jun 17 23:09:27 localhost.localdomain sshd[23898]: Failed password for nhdd from
192.168.88.145 port 37242 ssh2
Jun 17 23:09:31 localhost.localdomain sshd[23896]: Failed password for nhdd from
192.168.88.145 port 37216 ssh2
Jun 17 23:09:31 localhost.localdomain sshd[23897]: Failed password for nhdd from
192.168.88.145 port 37214 ssh2
Jun 17 23:09:31 localhost.localdomain sshd[23900]: Failed password for nhdd from
192.168.88.145 port 37248 ssh2
Jun 17 23:09:31 localhost.localdomain sshd[23898]: Failed password for nhdd from
192.168.88.145 port 37242 ssh2
Jun 17 23:09:33 localhost.localdomain sshd[23896]: Failed password for nhdd from
192.168.88.145 port 37216 ssh2
Jun 17 23:09:33 localhost.localdomain sshd[23897]: Failed password for nhdd from
192.168.88.145 port 37214 ssh2
Jun 17 23:09:33 localhost.localdomain sshd[23900]: Failed password for nhdd from
192.168.88.145 port 37248 ssh2
Jun 17 23:09:33 localhost.localdomain sshd[23898]: Failed password for nhdd from
192.168.88.145 port 37242 ssh2
Jun 17 23:09:36 localhost.localdomain sshd[23896]: Failed password for nhdd from
192.168.88.145 port 37216 ssh2
Jun 17 23:09:36 localhost.localdomain sshd[23900]: Failed password for nhdd from
192.168.88.145 port 37248 ssh2
Jun 17 23:09:36 localhost.localdomain sshd[23897]: Failed password for nhdd from
192.168.88.145 port 37214 ssh2
Jun 17 23:09:36 localhost.localdomain sshd[23898]: Failed password for nhdd from
192.168.88.145 port 37242 ssh2
Jun 17 23:09:39 localhost.localdomain sshd[23896]: Failed password for nhdd from
192.168.88.145 port 37216 ssh2
```

```
Jun 17 23:09:39 localhost.localdomain sshd[23900]: Failed password for nhdd from
192.168.88.145 port 37248 ssh2
Jun 17 23:09:39 localhost.localdomain sshd[23897]: Failed password for nhdd from
192.168.88.145 port 37214 ssh2
Jun 17 23:09:39 localhost.localdomain sshd[23898]: Failed password for nhdd from
192.168.88.145 port 37242 ssh2
Jun 17 23:09:41 localhost.localdomain sshd[23896]: Failed password for nhdd from
192.168.88.145 port 37216 ssh2
Jun 17 23:09:41 localhost.localdomain sshd[23900]: Failed password for nhdd from
192.168.88.145 port 37248 ssh2
Jun 17 23:09:41 localhost.localdomain sshd[23898]: Failed password for nhdd from
192.168.88.145 port 37242 ssh2
Jun 17 23:09:41 localhost.localdomain sshd[23897]: Failed password for nhdd from
192.168.88.145 port 37214 ssh2
Jun 17 23:09:42 localhost.localdomain sshd[23896]: error: maximum authentication attempts
exceeded for nhdd from 192.168.88.145 port 37216 ssh2 [preauth]
Jun 17 23:09:42 localhost.localdomain sshd[23896]: Disconnecting authenticating user nhdd
192.168.88.145 port 37216: Too many authentication failures [preauth]
Jun 17 23:09:42 localhost.localdomain sshd[23896]: PAM 5 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:09:42 localhost.localdomain sshd[23896]: PAM service(sshd) ignoring max retries; 6
> 3
Jun 17 23:09:42 localhost.localdomain sshd[23897]: error: maximum authentication attempts
exceeded for nhdd from 192.168.88.145 port 37214 ssh2 [preauth]
Jun 17 23:09:42 localhost.localdomain sshd[23897]: Disconnecting authenticating user nhdd
192.168.88.145 port 37214: Too many authentication failures [preauth]
Jun 17 23:09:42 localhost.localdomain sshd[23897]: PAM 5 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:09:42 localhost.localdomain sshd[23897]: PAM service(sshd) ignoring max retries; 6
> 3
Jun 17 23:09:42 localhost.localdomain sshd[23898]: error: maximum authentication attempts
exceeded for nhdd from 192.168.88.145 port 37242 ssh2 [preauth]
Jun 17 23:09:42 localhost.localdomain sshd[23898]: Disconnecting authenticating user nhdd
192.168.88.145 port 37242: Too many authentication failures [preauth]
Jun 17 23:09:42 localhost.localdomain sshd[23898]: PAM 5 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:09:42 localhost.localdomain sshd[23898]: PAM service(sshd) ignoring max retries; 6
> 3
Jun 17 23:09:42 localhost.localdomain sshd[23900]: error: maximum authentication attempts
exceeded for nhdd from 192.168.88.145 port 37248 ssh2 [preauth]
Jun 17 23:09:42 localhost.localdomain sshd[23900]: Disconnecting authenticating user nhdd
192.168.88.145 port 37248: Too many authentication failures [preauth]
Jun 17 23:09:42 localhost.localdomain sshd[23900]: PAM 5 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:09:42 localhost.localdomain sshd[23900]: PAM service(sshd) ignoring max retries; 6
> 3
Jun 17 23:09:43 localhost.localdomain sshd[23928]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
```

```
Jun 17 23:09:43 localhost.localdomain sshd[23932]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:09:43 localhost.localdomain sshd[23931]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:09:43 localhost.localdomain sshd[23929]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:09:45 localhost.localdomain sshd[23928]: Failed password for nhdd from
192.168.88.145 port 47660 ssh2
Jun 17 23:09:45 localhost.localdomain sshd[23931]: Failed password for nhdd from
192.168.88.145 port 47676 ssh2
Jun 17 23:09:45 localhost.localdomain sshd[23932]: Failed password for nhdd from
192.168.88.145 port 47680 ssh2
Jun 17 23:09:45 localhost.localdomain sshd[23929]: Failed password for nhdd from
192.168.88.145 port 47668 ssh2
Jun 17 23:09:47 localhost.localdomain sshd[23931]: Failed password for nhdd from
192.168.88.145 port 47676 ssh2
Jun 17 23:09:47 localhost.localdomain sshd[23928]: Failed password for nhdd from
192.168.88.145 port 47660 ssh2
Jun 17 23:09:47 localhost.localdomain sshd[23932]: Failed password for nhdd from
192.168.88.145 port 47680 ssh2
Jun 17 23:09:47 localhost.localdomain sshd[23929]: Failed password for nhdd from
192.168.88.145 port 47668 ssh2
Jun 17 23:09:50 localhost.localdomain sshd[23928]: Failed password for nhdd from
192.168.88.145 port 47660 ssh2
Jun 17 23:09:50 localhost.localdomain sshd[23931]: Failed password for nhdd from
192.168.88.145 port 47676 ssh2
Jun 17 23:09:50 localhost.localdomain sshd[23929]: Failed password for nhdd from
192.168.88.145 port 47668 ssh2
Jun 17 23:09:50 localhost.localdomain sshd[23932]: Failed password for nhdd from
192.168.88.145 port 47680 ssh2
Jun 17 23:09:52 localhost.localdomain sshd[23929]: Failed password for nhdd from
192.168.88.145 port 47668 ssh2
Jun 17 23:09:52 localhost.localdomain sshd[23928]: Failed password for nhdd from
192.168.88.145 port 47660 ssh2
Jun 17 23:09:52 localhost.localdomain sshd[23931]: Failed password for nhdd from
192.168.88.145 port 47676 ssh2
Jun 17 23:09:52 localhost.localdomain sshd[23932]: Failed password for nhdd from
192.168.88.145 port 47680 ssh2
Jun 17 23:09:55 localhost.localdomain sshd[23929]: Failed password for nhdd from
192.168.88.145 port 47668 ssh2
Jun 17 23:09:55 localhost.localdomain sshd[23928]: Failed password for nhdd from
192.168.88.145 port 47660 ssh2
Jun 17 23:09:55 localhost.localdomain sshd[23931]: Failed password for nhdd from
192.168.88.145 port 47676 ssh2
Jun 17 23:09:55 localhost.localdomain sshd[23932]: Failed password for nhdd from
192.168.88.145 port 47680 ssh2
Jun 17 23:09:58 localhost.localdomain sshd[23928]: Failed password for nhdd from
192.168.88.145 port 47660 ssh2
```

```
Jun 17 23:09:58 localhost.localdomain sshd[23932]: Failed password for nhdd from
192.168.88.145 port 47680 ssh2
Jun 17 23:09:58 localhost.localdomain sshd[23931]: Failed password for nhdd from
192.168.88.145 port 47676 ssh2
Jun 17 23:09:58 localhost.localdomain sshd[23929]: Failed password for nhdd from
192.168.88.145 port 47668 ssh2
Jun 17 23:09:59 localhost.localdomain sshd[23928]: error: maximum authentication attempts
exceeded for nhdd from 192.168.88.145 port 47660 ssh2 [preauth]
Jun 17 23:09:59 localhost.localdomain sshd[23928]: Disconnecting authenticating user nhdd
192.168.88.145 port 47660: Too many authentication failures [preauth]
Jun 17 23:09:59 localhost.localdomain sshd[23928]: PAM 5 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:09:59 localhost.localdomain sshd[23928]: PAM service(sshd) ignoring max retries; 6
> 3
Jun 17 23:09:59 localhost.localdomain sshd[23929]: error: maximum authentication attempts
exceeded for nhdd from 192.168.88.145 port 47668 ssh2 [preauth]
Jun 17 23:09:59 localhost.localdomain sshd[23929]: Disconnecting authenticating user nhdd
192.168.88.145 port 47668: Too many authentication failures [preauth]
Jun 17 23:09:59 localhost.localdomain sshd[23929]: PAM 5 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:09:59 localhost.localdomain sshd[23929]: PAM service(sshd) ignoring max retries; 6
> 3
Jun 17 23:09:59 localhost.localdomain sshd[23931]: error: maximum authentication attempts
exceeded for nhdd from 192.168.88.145 port 47676 ssh2 [preauth]
Jun 17 23:09:59 localhost.localdomain sshd[23931]: Disconnecting authenticating user nhdd
192.168.88.145 port 47676: Too many authentication failures [preauth]
Jun 17 23:09:59 localhost.localdomain sshd[23931]: PAM 5 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:09:59 localhost.localdomain sshd[23931]: PAM service(sshd) ignoring max retries; 6
> 3
Jun 17 23:09:59 localhost.localdomain sshd[23932]: error: maximum authentication attempts
exceeded for nhdd from 192.168.88.145 port 47680 ssh2 [preauth]
Jun 17 23:09:59 localhost.localdomain sshd[23932]: Disconnecting authenticating user nhdd
192.168.88.145 port 47680: Too many authentication failures [preauth]
Jun 17 23:09:59 localhost.localdomain sshd[23932]: PAM 5 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:09:59 localhost.localdomain sshd[23932]: PAM service(sshd) ignoring max retries; 6
> 3
Jun 17 23:09:59 localhost.localdomain sshd[23960]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:09:59 localhost.localdomain sshd[23965]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:09:59 localhost.localdomain sshd[23961]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:09:59 localhost.localdomain sshd[23963]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:10:01 localhost.localdomain sshd[23960]: Failed password for nhdd from
192.168.88.145 port 34718 ssh2
```

```
Jun 17 23:10:01 localhost.localdomain sshd[23965]: Failed password for nhdd from
192.168.88.145 port 34742 ssh2
Jun 17 23:10:01 localhost.localdomain sshd[23961]: Failed password for nhdd from
192.168.88.145 port 34720 ssh2
Jun 17 23:10:01 localhost.localdomain sshd[23963]: Failed password for nhdd from
192.168.88.145 port 34736 ssh2
Jun 17 23:10:04 localhost.localdomain sshd[23960]: Failed password for nhdd from
192.168.88.145 port 34718 ssh2
Jun 17 23:10:04 localhost.localdomain sshd[23963]: Failed password for nhdd from
192.168.88.145 port 34736 ssh2
Jun 17 23:10:04 localhost.localdomain sshd[23961]: Failed password for nhdd from
192.168.88.145 port 34720 ssh2
Jun 17 23:10:04 localhost.localdomain sshd[23965]: Failed password for nhdd from
192.168.88.145 port 34742 ssh2
Jun 17 23:10:06 localhost.localdomain sshd[23960]: Failed password for nhdd from
192.168.88.145 port 34718 ssh2
Jun 17 23:10:06 localhost.localdomain sshd[23965]: Failed password for nhdd from
192.168.88.145 port 34742 ssh2
Jun 17 23:10:06 localhost.localdomain sshd[23961]: Failed password for nhdd from
192.168.88.145 port 34720 ssh2
Jun 17 23:10:06 localhost.localdomain sshd[23963]: Failed password for nhdd from
192.168.88.145 port 34736 ssh2
Jun 17 23:10:09 localhost.localdomain sshd[23960]: Failed password for nhdd from
192.168.88.145 port 34718 ssh2
Jun 17 23:10:09 localhost.localdomain sshd[23963]: Failed password for nhdd from
192.168.88.145 port 34736 ssh2
Jun 17 23:10:09 localhost.localdomain sshd[23961]: Failed password for nhdd from
192.168.88.145 port 34720 ssh2
Jun 17 23:10:09 localhost.localdomain sshd[23965]: Failed password for nhdd from
192.168.88.145 port 34742 ssh2
Jun 17 23:10:12 localhost.localdomain sshd[23960]: Failed password for nhdd from
192.168.88.145 port 34718 ssh2
Jun 17 23:10:12 localhost.localdomain sshd[23961]: Failed password for nhdd from
192.168.88.145 port 34720 ssh2
Jun 17 23:10:12 localhost.localdomain sshd[23963]: Failed password for nhdd from
192.168.88.145 port 34736 ssh2
Jun 17 23:10:12 localhost.localdomain sshd[23965]: Failed password for nhdd from
192.168.88.145 port 34742 ssh2
Jun 17 23:10:15 localhost.localdomain sshd[23960]: Failed password for nhdd from
192.168.88.145 port 34718 ssh2
Jun 17 23:10:15 localhost.localdomain sshd[23963]: Failed password for nhdd from
192.168.88.145 port 34736 ssh2
Jun 17 23:10:15 localhost.localdomain sshd[23961]: Failed password for nhdd from
192.168.88.145 port 34720 ssh2
Jun 17 23:10:15 localhost.localdomain sshd[23965]: Failed password for nhdd from
192.168.88.145 port 34742 ssh2
Jun 17 23:10:15 localhost.localdomain sshd[23960]: error: maximum authentication attempts
exceeded for nhdd from 192.168.88.145 port 34718 ssh2 [preauth]
```

```
Jun 17 23:10:15 localhost.localdomain sshd[23960]: Disconnecting authenticating user nhdd
192.168.88.145 port 34718: Too many authentication failures [preauth]
Jun 17 23:10:15 localhost.localdomain sshd[23960]: PAM 5 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:10:15 localhost.localdomain sshd[23960]: PAM service(sshd) ignoring max retries; 6
> 3
Jun 17 23:10:15 localhost.localdomain sshd[23961]: error: maximum authentication attempts
exceeded for nhdd from 192.168.88.145 port 34720 ssh2 [preauth]
Jun 17 23:10:15 localhost.localdomain sshd[23961]: Disconnecting authenticating user nhdd
192.168.88.145 port 34720: Too many authentication failures [preauth]
Jun 17 23:10:15 localhost.localdomain sshd[23961]: PAM 5 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:10:15 localhost.localdomain sshd[23961]: PAM service(sshd) ignoring max retries; 6
> 3
Jun 17 23:10:15 localhost.localdomain sshd[23963]: error: maximum authentication attempts
exceeded for nhdd from 192.168.88.145 port 34736 ssh2 [preauth]
Jun 17 23:10:15 localhost.localdomain sshd[23963]: Disconnecting authenticating user nhdd
192.168.88.145 port 34736: Too many authentication failures [preauth]
Jun 17 23:10:15 localhost.localdomain sshd[23963]: PAM 5 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:10:15 localhost.localdomain sshd[23963]: PAM service(sshd) ignoring max retries; 6
> 3
Jun 17 23:10:15 localhost.localdomain sshd[23965]: error: maximum authentication attempts
exceeded for nhdd from 192.168.88.145 port 34742 ssh2 [preauth]
Jun 17 23:10:15 localhost.localdomain sshd[23965]: Disconnecting authenticating user nhdd
192.168.88.145 port 34742: Too many authentication failures [preauth]
Jun 17 23:10:15 localhost.localdomain sshd[23965]: PAM 5 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:10:15 localhost.localdomain sshd[23965]: PAM service(sshd) ignoring max retries; 6
> 3
Jun 17 23:10:15 localhost.localdomain sshd[23994]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:10:15 localhost.localdomain sshd[23997]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:10:15 localhost.localdomain sshd[23993]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:10:15 localhost.localdomain sshd[23995]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:10:17 localhost.localdomain sshd[23994]: Failed password for nhdd from
192.168.88.145 port 37096 ssh2
Jun 17 23:10:17 localhost.localdomain sshd[23997]: Failed password for nhdd from
192.168.88.145 port 37122 ssh2
Jun 17 23:10:17 localhost.localdomain sshd[23993]: Failed password for nhdd from
192.168.88.145 port 37080 ssh2
Jun 17 23:10:17 localhost.localdomain sshd[23995]: Failed password for nhdd from
192.168.88.145 port 37106 ssh2
Jun 17 23:10:20 localhost.localdomain sshd[23994]: Failed password for nhdd from
192.168.88.145 port 37096 ssh2
```

```
Jun 17 23:10:20 localhost.localdomain sshd[23993]: Failed password for nhdd from
192.168.88.145 port 37080 ssh2
Jun 17 23:10:20 localhost.localdomain sshd[23995]: Failed password for nhdd from
192.168.88.145 port 37106 ssh2
Jun 17 23:10:20 localhost.localdomain sshd[23997]: Failed password for nhdd from
192.168.88.145 port 37122 ssh2
Jun 17 23:10:23 localhost.localdomain sshd[23994]: Failed password for nhdd from
192.168.88.145 port 37096 ssh2
Jun 17 23:10:23 localhost.localdomain sshd[23997]: Failed password for nhdd from
192.168.88.145 port 37122 ssh2
Jun 17 23:10:23 localhost.localdomain sshd[23995]: Failed password for nhdd from
192.168.88.145 port 37106 ssh2
Jun 17 23:10:23 localhost.localdomain sshd[23993]: Failed password for nhdd from
192.168.88.145 port 37080 ssh2
Jun 17 23:10:25 localhost.localdomain sshd[23995]: Failed password for nhdd from
192.168.88.145 port 37106 ssh2
Jun 17 23:10:25 localhost.localdomain sshd[23993]: Failed password for nhdd from
192.168.88.145 port 37080 ssh2
Jun 17 23:10:25 localhost.localdomain sshd[23994]: Failed password for nhdd from
192.168.88.145 port 37096 ssh2
Jun 17 23:10:25 localhost.localdomain sshd[23997]: Failed password for nhdd from
192.168.88.145 port 37122 ssh2
Jun 17 23:10:28 localhost.localdomain sshd[23994]: Failed password for nhdd from
192.168.88.145 port 37096 ssh2
Jun 17 23:10:28 localhost.localdomain sshd[23995]: Failed password for nhdd from
192.168.88.145 port 37106 ssh2
Jun 17 23:10:28 localhost.localdomain sshd[23997]: Failed password for nhdd from
192.168.88.145 port 37122 ssh2
Jun 17 23:10:28 localhost.localdomain sshd[23993]: Failed password for nhdd from
192.168.88.145 port 37080 ssh2
Jun 17 23:10:30 localhost.localdomain sudo[24059]: hoangdat : TTY=pts/2 ;
PWD=/home/hoangdat ; USER=root ; COMMAND=/bin/fail2ban-client status sshd
Jun 17 23:10:31 localhost.localdomain sshd[23994]: Failed password for nhdd from
192.168.88.145 port 37096 ssh2
Jun 17 23:10:31 localhost.localdomain sshd[23997]: Failed password for nhdd from
192.168.88.145 port 37122 ssh2
Jun 17 23:10:31 localhost.localdomain sshd[23995]: Failed password for nhdd from
192.168.88.145 port 37106 ssh2
Jun 17 23:10:31 localhost.localdomain sshd[23993]: Failed password for nhdd from
192.168.88.145 port 37080 ssh2
Jun 17 23:10:32 localhost.localdomain sshd[23994]: error: maximum authentication attempts
exceeded for nhdd from 192.168.88.145 port 37096 ssh2 [preauth]
Jun 17 23:10:32 localhost.localdomain sshd[23994]: Disconnecting authenticating user nhdd
192.168.88.145 port 37096: Too many authentication failures [preauth]
Jun 17 23:10:32 localhost.localdomain sshd[23994]: PAM 5 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:10:32 localhost.localdomain sshd[23994]: PAM service(sshd) ignoring max retries; 6
> 3
```

```
Jun 17 23:10:32 localhost.localdomain sshd[23995]: error: maximum authentication attempts
exceeded for nhdd from 192.168.88.145 port 37106 ssh2 [preauth]
Jun 17 23:10:32 localhost.localdomain sshd[23995]: Disconnecting authenticating user nhdd
192.168.88.145 port 37106: Too many authentication failures [preauth]
Jun 17 23:10:32 localhost.localdomain sshd[23995]: PAM 5 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:10:32 localhost.localdomain sshd[23995]: PAM service(sshd) ignoring max retries; 6
> 3
Jun 17 23:10:32 localhost.localdomain sshd[23997]: error: maximum authentication attempts
exceeded for nhdd from 192.168.88.145 port 37122 ssh2 [preauth]
Jun 17 23:10:32 localhost.localdomain sshd[23997]: Disconnecting authenticating user nhdd
192.168.88.145 port 37122: Too many authentication failures [preauth]
Jun 17 23:10:32 localhost.localdomain sshd[23997]: PAM 5 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:10:32 localhost.localdomain sshd[23997]: PAM service(sshd) ignoring max retries; 6
> 3
Jun 17 23:10:32 localhost.localdomain sshd[23993]: error: maximum authentication attempts
exceeded for nhdd from 192.168.88.145 port 37080 ssh2 [preauth]
Jun 17 23:10:32 localhost.localdomain sshd[23993]: Disconnecting authenticating user nhdd
192.168.88.145 port 37080: Too many authentication failures [preauth]
Jun 17 23:10:32 localhost.localdomain sshd[23993]: PAM 5 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:10:32 localhost.localdomain sshd[23993]: PAM service(sshd) ignoring max retries; 6
> 3
Jun 17 23:10:32 localhost.localdomain sshd[24073]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:10:32 localhost.localdomain sshd[24075]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:10:32 localhost.localdomain sshd[24077]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:10:32 localhost.localdomain sshd[24074]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:10:34 localhost.localdomain sshd[24073]: Failed password for nhdd from
192.168.88.145 port 53390 ssh2
Jun 17 23:10:34 localhost.localdomain sshd[24075]: Failed password for nhdd from
192.168.88.145 port 53408 ssh2
Jun 17 23:10:34 localhost.localdomain sshd[24077]: Failed password for nhdd from
192.168.88.145 port 53420 ssh2
Jun 17 23:10:34 localhost.localdomain sshd[24074]: Failed password for nhdd from
192.168.88.145 port 53394 ssh2
Jun 17 23:10:36 localhost.localdomain sshd[24073]: Failed password for nhdd from
192.168.88.145 port 53390 ssh2
Jun 17 23:10:36 localhost.localdomain sshd[24074]: Failed password for nhdd from
192.168.88.145 port 53394 ssh2
Jun 17 23:10:36 localhost.localdomain sshd[24075]: Failed password for nhdd from
192.168.88.145 port 53408 ssh2
Jun 17 23:10:36 localhost.localdomain sshd[24077]: Failed password for nhdd from
192.168.88.145 port 53420 ssh2
```

```
Jun 17 23:10:39 localhost.localdomain sshd[24073]: Failed password for nhdd from
192.168.88.145 port 53390 ssh2
Jun 17 23:10:39 localhost.localdomain sshd[24075]: Failed password for nhdd from
192.168.88.145 port 53408 ssh2
Jun 17 23:10:39 localhost.localdomain sshd[24077]: Failed password for nhdd from
192.168.88.145 port 53420 ssh2
Jun 17 23:10:39 localhost.localdomain sshd[24074]: Failed password for nhdd from
192.168.88.145 port 53394 ssh2
Jun 17 23:10:42 localhost.localdomain sshd[24073]: Failed password for nhdd from
192.168.88.145 port 53390 ssh2
Jun 17 23:10:42 localhost.localdomain sshd[24077]: Failed password for nhdd from
192.168.88.145 port 53420 ssh2
Jun 17 23:10:42 localhost.localdomain sshd[24075]: Failed password for nhdd from
192.168.88.145 port 53408 ssh2
Jun 17 23:10:42 localhost.localdomain sshd[24074]: Failed password for nhdd from
192.168.88.145 port 53394 ssh2
Jun 17 23:10:45 localhost.localdomain sshd[24073]: Failed password for nhdd from
192.168.88.145 port 53390 ssh2
Jun 17 23:10:45 localhost.localdomain sshd[24074]: Failed password for nhdd from
192.168.88.145 port 53394 ssh2
Jun 17 23:10:45 localhost.localdomain sshd[24075]: Failed password for nhdd from
192.168.88.145 port 53408 ssh2
Jun 17 23:10:45 localhost.localdomain sshd[24077]: Failed password for nhdd from
192.168.88.145 port 53420 ssh2
Jun 17 23:10:47 localhost.localdomain sshd[24073]: Failed password for nhdd from
192.168.88.145 port 53390 ssh2
Jun 17 23:10:47 localhost.localdomain sshd[24077]: Failed password for nhdd from
192.168.88.145 port 53420 ssh2
Jun 17 23:10:47 localhost.localdomain sshd[24075]: Failed password for nhdd from
192.168.88.145 port 53408 ssh2
Jun 17 23:10:47 localhost.localdomain sshd[24074]: Failed password for nhdd from
192.168.88.145 port 53394 ssh2
Jun 17 23:10:48 localhost.localdomain sshd[24073]: error: maximum authentication attempts
exceeded for nhdd from 192.168.88.145 port 53390 ssh2 [preauth]
Jun 17 23:10:48 localhost.localdomain sshd[24073]: Disconnecting authenticating user nhdd
192.168.88.145 port 53390: Too many authentication failures [preauth]
Jun 17 23:10:48 localhost.localdomain sshd[24073]: PAM 5 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:10:48 localhost.localdomain sshd[24073]: PAM service(sshd) ignoring max retries; 6
> 3
Jun 17 23:10:48 localhost.localdomain sshd[24075]: error: maximum authentication attempts
exceeded for nhdd from 192.168.88.145 port 53408 ssh2 [preauth]
Jun 17 23:10:48 localhost.localdomain sshd[24075]: Disconnecting authenticating user nhdd
192.168.88.145 port 53408: Too many authentication failures [preauth]
Jun 17 23:10:48 localhost.localdomain sshd[24075]: PAM 5 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:10:48 localhost.localdomain sshd[24075]: PAM service(sshd) ignoring max retries; 6
> 3
```

```
Jun 17 23:10:48 localhost.localdomain sshd[24077]: error: maximum authentication attempts exceeded for nhdd from 192.168.88.145 port 53420 ssh2 [preauth]
Jun 17 23:10:48 localhost.localdomain sshd[24074]: error: maximum authentication attempts exceeded for nhdd from 192.168.88.145 port 53394 ssh2 [preauth]
Jun 17 23:10:48 localhost.localdomain sshd[24077]: Disconnecting authenticating user nhdd 192.168.88.145 port 53420: Too many authentication failures [preauth]
Jun 17 23:10:48 localhost.localdomain sshd[24074]: Disconnecting authenticating user nhdd 192.168.88.145 port 53394: Too many authentication failures [preauth]
Jun 17 23:10:48 localhost.localdomain sshd[24074]: PAM 5 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:10:48 localhost.localdomain sshd[24074]: PAM service(sshd) ignoring max retries; 6 > 3
Jun 17 23:10:48 localhost.localdomain sshd[24077]: PAM 5 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:10:48 localhost.localdomain sshd[24077]: PAM service(sshd) ignoring max retries; 6 > 3
Jun 17 23:10:48 localhost.localdomain sshd[24110]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:10:48 localhost.localdomain sshd[24108]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:10:48 localhost.localdomain sshd[24109]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:10:48 localhost.localdomain sshd[24111]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:10:50 localhost.localdomain sshd[24110]: Failed password for nhdd from 192.168.88.145 port 48202 ssh2
Jun 17 23:10:50 localhost.localdomain sshd[24108]: Failed password for nhdd from 192.168.88.145 port 48184 ssh2
Jun 17 23:10:50 localhost.localdomain sshd[24111]: Failed password for nhdd from 192.168.88.145 port 48210 ssh2
Jun 17 23:10:50 localhost.localdomain sshd[24109]: Failed password for nhdd from 192.168.88.145 port 48198 ssh2
Jun 17 23:10:52 localhost.localdomain sshd[24108]: Failed password for nhdd from 192.168.88.145 port 48184 ssh2
Jun 17 23:10:53 localhost.localdomain sshd[24109]: Failed password for nhdd from 192.168.88.145 port 48198 ssh2
Jun 17 23:10:53 localhost.localdomain sshd[24110]: Failed password for nhdd from 192.168.88.145 port 48202 ssh2
Jun 17 23:10:53 localhost.localdomain sshd[24111]: Failed password for nhdd from 192.168.88.145 port 48210 ssh2
Jun 17 23:10:55 localhost.localdomain sshd[24110]: Failed password for nhdd from 192.168.88.145 port 48202 ssh2
Jun 17 23:10:56 localhost.localdomain sshd[24108]: Failed password for nhdd from 192.168.88.145 port 48184 ssh2
Jun 17 23:10:56 localhost.localdomain sshd[24111]: Failed password for nhdd from 192.168.88.145 port 48210 ssh2
Jun 17 23:10:56 localhost.localdomain sshd[24109]: Failed password for nhdd from 192.168.88.145 port 48198 ssh2
Jun 17 23:10:59 localhost.localdomain sshd[24108]: Failed password for nhdd from
192.168.88.145 port 48184 ssh2
Jun 17 23:10:59 localhost.localdomain sshd[24110]: Failed password for nhdd from
192.168.88.145 port 48202 ssh2
Jun 17 23:10:59 localhost.localdomain sshd[24109]: Failed password for nhdd from
192.168.88.145 port 48198 ssh2
Jun 17 23:10:59 localhost.localdomain sshd[24111]: Failed password for nhdd from
192.168.88.145 port 48210 ssh2
Jun 17 23:11:01 localhost.localdomain sshd[24108]: Failed password for nhdd from
192.168.88.145 port 48184 ssh2
Jun 17 23:11:01 localhost.localdomain sshd[24109]: Failed password for nhdd from
192.168.88.145 port 48198 ssh2
Jun 17 23:11:01 localhost.localdomain sshd[24110]: Failed password for nhdd from
192.168.88.145 port 48202 ssh2
Jun 17 23:11:01 localhost.localdomain sshd[24111]: Failed password for nhdd from
192.168.88.145 port 48210 ssh2
Jun 17 23:11:04 localhost.localdomain sshd[24108]: Failed password for nhdd from
192.168.88.145 port 48184 ssh2
Jun 17 23:11:04 localhost.localdomain sshd[24110]: Failed password for nhdd from
192.168.88.145 port 48202 ssh2
Jun 17 23:11:04 localhost.localdomain sshd[24109]: Failed password for nhdd from
192.168.88.145 port 48198 ssh2
Jun 17 23:11:04 localhost.localdomain sshd[24111]: Failed password for nhdd from
192.168.88.145 port 48210 ssh2
Jun 17 23:11:04 localhost.localdomain sshd[24108]: error: maximum authentication attempts
exceeded for nhdd from 192.168.88.145 port 48184 ssh2 [preauth]
Jun 17 23:11:04 localhost.localdomain sshd[24108]: Disconnecting authenticating user nhdd
192.168.88.145 port 48184: Too many authentication failures [preauth]
Jun 17 23:11:04 localhost.localdomain sshd[24108]: PAM 5 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:11:04 localhost.localdomain sshd[24108]: PAM service(sshd) ignoring max retries; 6
> 3
Jun 17 23:11:04 localhost.localdomain sshd[24110]: error: maximum authentication attempts
exceeded for nhdd from 192.168.88.145 port 48202 ssh2 [preauth]
Jun 17 23:11:04 localhost.localdomain sshd[24110]: Disconnecting authenticating user nhdd
192.168.88.145 port 48202: Too many authentication failures [preauth]
Jun 17 23:11:04 localhost.localdomain sshd[24110]: PAM 5 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:11:04 localhost.localdomain sshd[24110]: PAM service(sshd) ignoring max retries; 6
> 3
Jun 17 23:11:04 localhost.localdomain sshd[24111]: error: maximum authentication attempts
exceeded for nhdd from 192.168.88.145 port 48210 ssh2 [preauth]
Jun 17 23:11:04 localhost.localdomain sshd[24111]: Disconnecting authenticating user nhdd
192.168.88.145 port 48210: Too many authentication failures [preauth]
Jun 17 23:11:04 localhost.localdomain sshd[24111]: PAM 5 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:11:04 localhost.localdomain sshd[24111]: PAM service(sshd) ignoring max retries; 6
> 3
```

```
Jun 17 23:11:04 localhost.localdomain sshd[24109]: error: maximum authentication attempts
exceeded for nhdd from 192.168.88.145 port 48198 ssh2 [preauth]
Jun 17 23:11:04 localhost.localdomain sshd[24109]: Disconnecting authenticating user nhdd
192.168.88.145 port 48198: Too many authentication failures [preauth]
Jun 17 23:11:04 localhost.localdomain sshd[24109]: PAM 5 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:11:04 localhost.localdomain sshd[24109]: PAM service(sshd) ignoring max retries; 6
> 3
Jun 17 23:11:05 localhost.localdomain sshd[24145]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:11:05 localhost.localdomain sshd[24149]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:11:05 localhost.localdomain sshd[24148]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:11:05 localhost.localdomain sshd[24146]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:11:07 localhost.localdomain sshd[24145]: Failed password for nhdd from
192.168.88.145 port 47104 ssh2
Jun 17 23:11:07 localhost.localdomain sshd[24149]: Failed password for nhdd from
192.168.88.145 port 47128 ssh2
Jun 17 23:11:07 localhost.localdomain sshd[24148]: Failed password for nhdd from
192.168.88.145 port 47116 ssh2
Jun 17 23:11:07 localhost.localdomain sshd[24146]: Failed password for nhdd from
192.168.88.145 port 47108 ssh2
Jun 17 23:11:10 localhost.localdomain sshd[24145]: Failed password for nhdd from
192.168.88.145 port 47104 ssh2
Jun 17 23:11:10 localhost.localdomain sshd[24148]: Failed password for nhdd from
192.168.88.145 port 47116 ssh2
Jun 17 23:11:10 localhost.localdomain sshd[24146]: Failed password for nhdd from
192.168.88.145 port 47108 ssh2
Jun 17 23:11:10 localhost.localdomain sshd[24149]: Failed password for nhdd from
192.168.88.145 port 47128 ssh2
Jun 17 23:11:12 localhost.localdomain sshd[24145]: Failed password for nhdd from
192.168.88.145 port 47104 ssh2
Jun 17 23:11:12 localhost.localdomain sshd[24149]: Failed password for nhdd from
192.168.88.145 port 47128 ssh2
Jun 17 23:11:12 localhost.localdomain sshd[24146]: Failed password for nhdd from
192.168.88.145 port 47108 ssh2
Jun 17 23:11:12 localhost.localdomain sshd[24148]: Failed password for nhdd from
192.168.88.145 port 47116 ssh2
Jun 17 23:11:15 localhost.localdomain sshd[24145]: Failed password for nhdd from
192.168.88.145 port 47104 ssh2
Jun 17 23:11:15 localhost.localdomain sshd[24149]: Failed password for nhdd from
192.168.88.145 port 47128 ssh2
Jun 17 23:11:15 localhost.localdomain sshd[24146]: Failed password for nhdd from
192.168.88.145 port 47108 ssh2
Jun 17 23:11:15 localhost.localdomain sshd[24148]: Failed password for nhdd from
192.168.88.145 port 47116 ssh2
```

```
Jun 17 23:11:17 localhost.localdomain sshd[24145]: Failed password for nhdd from 192.168.88.145 port 47104 ssh2
Jun 17 23:11:17 localhost.localdomain sshd[24146]: Failed password for nhdd from 192.168.88.145 port 47108 ssh2
Jun 17 23:11:17 localhost.localdomain sshd[24148]: Failed password for nhdd from 192.168.88.145 port 47116 ssh2
Jun 17 23:11:17 localhost.localdomain sshd[24149]: Failed password for nhdd from 192.168.88.145 port 47128 ssh2
Jun 17 23:11:21 localhost.localdomain sshd[24145]: Failed password for nhdd from 192.168.88.145 port 47104 ssh2
Jun 17 23:11:21 localhost.localdomain sshd[24146]: Failed password for nhdd from 192.168.88.145 port 47108 ssh2
Jun 17 23:11:21 localhost.localdomain sshd[24148]: Failed password for nhdd from 192.168.88.145 port 47116 ssh2
Jun 17 23:11:21 localhost.localdomain sshd[24149]: Failed password for nhdd from 192.168.88.145 port 47128 ssh2
Jun 17 23:11:21 localhost.localdomain sshd[24145]: error: maximum authentication attempts exceeded for nhdd from 192.168.88.145 port 47104 ssh2 [preauth]
Jun 17 23:11:21 localhost.localdomain sshd[24145]: Disconnecting authenticating user nhdd 192.168.88.145 port 47104: Too many authentication failures [preauth]
Jun 17 23:11:21 localhost.localdomain sshd[24145]: PAM 5 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:11:21 localhost.localdomain sshd[24145]: PAM service(sshd) ignoring max retries; 6 > 3
Jun 17 23:11:21 localhost.localdomain sshd[24146]: error: maximum authentication attempts exceeded for nhdd from 192.168.88.145 port 47108 ssh2 [preauth]
Jun 17 23:11:21 localhost.localdomain sshd[24146]: Disconnecting authenticating user nhdd 192.168.88.145 port 47108: Too many authentication failures [preauth]
Jun 17 23:11:21 localhost.localdomain sshd[24146]: PAM 5 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:11:21 localhost.localdomain sshd[24146]: PAM service(sshd) ignoring max retries; 6 > 3
Jun 17 23:11:21 localhost.localdomain sshd[24148]: error: maximum authentication attempts exceeded for nhdd from 192.168.88.145 port 47116 ssh2 [preauth]
Jun 17 23:11:21 localhost.localdomain sshd[24148]: Disconnecting authenticating user nhdd 192.168.88.145 port 47116: Too many authentication failures [preauth]
Jun 17 23:11:21 localhost.localdomain sshd[24148]: PAM 5 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:11:21 localhost.localdomain sshd[24148]: PAM service(sshd) ignoring max retries; 6 > 3
Jun 17 23:11:21 localhost.localdomain sshd[24149]: error: maximum authentication attempts exceeded for nhdd from 192.168.88.145 port 47128 ssh2 [preauth]
Jun 17 23:11:21 localhost.localdomain sshd[24149]: Disconnecting authenticating user nhdd 192.168.88.145 port 47128: Too many authentication failures [preauth]
Jun 17 23:11:21 localhost.localdomain sshd[24149]: PAM 5 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:11:21 localhost.localdomain sshd[24149]: PAM service(sshd) ignoring max retries; 6 > 3
Jun 17 23:11:21 localhost.localdomain sshd[24182]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:11:21 localhost.localdomain sshd[24178]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:11:21 localhost.localdomain sshd[24179]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:11:21 localhost.localdomain sshd[24181]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:11:22 localhost.localdomain sshd[24182]: Failed password for nhdd from
192.168.88.145 port 60384 ssh2
Jun 17 23:11:22 localhost.localdomain sshd[24178]: Failed password for nhdd from
192.168.88.145 port 60364 ssh2
Jun 17 23:11:22 localhost.localdomain sshd[24179]: Failed password for nhdd from
192.168.88.145 port 60370 ssh2
Jun 17 23:11:22 localhost.localdomain sshd[24181]: Failed password for nhdd from
192.168.88.145 port 60378 ssh2
Jun 17 23:11:26 localhost.localdomain sshd[24178]: Failed password for nhdd from
192.168.88.145 port 60364 ssh2
Jun 17 23:11:26 localhost.localdomain sshd[24182]: Failed password for nhdd from
192.168.88.145 port 60384 ssh2
Jun 17 23:11:26 localhost.localdomain sshd[24179]: Failed password for nhdd from
192.168.88.145 port 60370 ssh2
Jun 17 23:11:26 localhost.localdomain sshd[24181]: Failed password for nhdd from
192.168.88.145 port 60378 ssh2
Jun 17 23:11:29 localhost.localdomain sshd[24178]: Failed password for nhdd from
192.168.88.145 port 60364 ssh2
Jun 17 23:11:29 localhost.localdomain sshd[24182]: Failed password for nhdd from
192.168.88.145 port 60384 ssh2
Jun 17 23:11:29 localhost.localdomain sshd[24179]: Failed password for nhdd from
192.168.88.145 port 60370 ssh2
Jun 17 23:11:29 localhost.localdomain sshd[24181]: Failed password for nhdd from
192.168.88.145 port 60378 ssh2
Jun 17 23:11:34 localhost.localdomain sshd[24178]: Failed password for nhdd from
192.168.88.145 port 60364 ssh2
Jun 17 23:11:34 localhost.localdomain sshd[24179]: Failed password for nhdd from
192.168.88.145 port 60370 ssh2
Jun 17 23:11:34 localhost.localdomain sshd[24181]: Failed password for nhdd from
192.168.88.145 port 60378 ssh2
Jun 17 23:11:34 localhost.localdomain sshd[24182]: Failed password for nhdd from
192.168.88.145 port 60384 ssh2
Jun 17 23:11:37 localhost.localdomain sshd[24178]: Failed password for nhdd from
192.168.88.145 port 60364 ssh2
Jun 17 23:11:37 localhost.localdomain sshd[24181]: Failed password for nhdd from
192.168.88.145 port 60378 ssh2
Jun 17 23:11:37 localhost.localdomain sshd[24179]: Failed password for nhdd from
192.168.88.145 port 60370 ssh2
Jun 17 23:11:37 localhost.localdomain sshd[24182]: Failed password for nhdd from
192.168.88.145 port 60384 ssh2
```

```
Jun 17 23:11:40 localhost.localdomain sshd[24178]: Failed password for nhdd from
192.168.88.145 port 60364 ssh2
Jun 17 23:11:40 localhost.localdomain sshd[24179]: Failed password for nhdd from
192.168.88.145 port 60370 ssh2
Jun 17 23:11:40 localhost.localdomain sshd[24178]: error: maximum authentication attempts
exceeded for nhdd from 192.168.88.145 port 60364 ssh2 [preauth]
Jun 17 23:11:40 localhost.localdomain sshd[24178]: Disconnecting authenticating user nhdd
192.168.88.145 port 60364: Too many authentication failures [preauth]
Jun 17 23:11:40 localhost.localdomain sshd[24178]: PAM 5 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:11:40 localhost.localdomain sshd[24178]: PAM service(sshd) ignoring max retries; 6
> 3
Jun 17 23:11:40 localhost.localdomain sshd[24179]: error: maximum authentication attempts
exceeded for nhdd from 192.168.88.145 port 60370 ssh2 [preauth]
Jun 17 23:11:40 localhost.localdomain sshd[24179]: Disconnecting authenticating user nhdd
192.168.88.145 port 60370: Too many authentication failures [preauth]
Jun 17 23:11:40 localhost.localdomain sshd[24179]: PAM 5 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:11:40 localhost.localdomain sshd[24179]: PAM service(sshd) ignoring max retries; 6
> 3
Jun 17 23:11:40 localhost.localdomain sshd[24181]: Failed password for nhdd from
192.168.88.145 port 60378 ssh2
Jun 17 23:11:40 localhost.localdomain sshd[24182]: Failed password for nhdd from
192.168.88.145 port 60384 ssh2
Jun 17 23:11:40 localhost.localdomain sshd[24182]: error: maximum authentication attempts
exceeded for nhdd from 192.168.88.145 port 60384 ssh2 [preauth]
Jun 17 23:11:40 localhost.localdomain sshd[24182]: Disconnecting authenticating user nhdd
192.168.88.145 port 60384: Too many authentication failures [preauth]
Jun 17 23:11:40 localhost.localdomain sshd[24182]: PAM 5 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:11:40 localhost.localdomain sshd[24182]: PAM service(sshd) ignoring max retries; 6
> 3
Jun 17 23:11:40 localhost.localdomain sshd[24181]: error: maximum authentication attempts
exceeded for nhdd from 192.168.88.145 port 60378 ssh2 [preauth]
Jun 17 23:11:40 localhost.localdomain sshd[24181]: Disconnecting authenticating user nhdd
192.168.88.145 port 60378: Too many authentication failures [preauth]
Jun 17 23:11:40 localhost.localdomain sshd[24181]: PAM 5 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:11:40 localhost.localdomain sshd[24181]: PAM service(sshd) ignoring max retries; 6
> 3
Jun 17 23:11:40 localhost.localdomain sshd[24214]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:11:40 localhost.localdomain sshd[24218]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:11:40 localhost.localdomain sshd[24215]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:11:40 localhost.localdomain sshd[24217]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
```

```
Jun 17 23:11:42 localhost.localdomain sshd[24214]: Failed password for nhdd from
192.168.88.145 port 56404 ssh2
Jun 17 23:11:42 localhost.localdomain sshd[24218]: Failed password for nhdd from
192.168.88.145 port 56444 ssh2
Jun 17 23:11:42 localhost.localdomain sshd[24215]: Failed password for nhdd from
192.168.88.145 port 56420 ssh2
Jun 17 23:11:42 localhost.localdomain sshd[24217]: Failed password for nhdd from
192.168.88.145 port 56436 ssh2
Jun 17 23:11:45 localhost.localdomain sshd[24214]: Failed password for nhdd from
192.168.88.145 port 56404 ssh2
Jun 17 23:11:45 localhost.localdomain sshd[24215]: Failed password for nhdd from
192.168.88.145 port 56420 ssh2
Jun 17 23:11:45 localhost.localdomain sshd[24217]: Failed password for nhdd from
192.168.88.145 port 56436 ssh2
Jun 17 23:11:45 localhost.localdomain sshd[24218]: Failed password for nhdd from
192.168.88.145 port 56444 ssh2
Jun 17 23:11:47 localhost.localdomain sshd[24214]: Failed password for nhdd from
192.168.88.145 port 56404 ssh2
Jun 17 23:11:47 localhost.localdomain sshd[24217]: Failed password for nhdd from
192.168.88.145 port 56436 ssh2
Jun 17 23:11:47 localhost.localdomain sshd[24215]: Failed password for nhdd from
192.168.88.145 port 56420 ssh2
Jun 17 23:11:47 localhost.localdomain sshd[24218]: Failed password for nhdd from
192.168.88.145 port 56444 ssh2
Jun 17 23:11:50 localhost.localdomain sshd[24214]: Failed password for nhdd from
192.168.88.145 port 56404 ssh2
Jun 17 23:11:50 localhost.localdomain sshd[24218]: Failed password for nhdd from
192.168.88.145 port 56444 ssh2
Jun 17 23:11:50 localhost.localdomain sshd[24215]: Failed password for nhdd from
192.168.88.145 port 56420 ssh2
Jun 17 23:11:50 localhost.localdomain sshd[24217]: Failed password for nhdd from
192.168.88.145 port 56436 ssh2
Jun 17 23:11:53 localhost.localdomain sshd[24214]: Failed password for nhdd from
192.168.88.145 port 56404 ssh2
Jun 17 23:11:53 localhost.localdomain sshd[24218]: Failed password for nhdd from
192.168.88.145 port 56444 ssh2
Jun 17 23:11:53 localhost.localdomain sshd[24215]: Failed password for nhdd from
192.168.88.145 port 56420 ssh2
Jun 17 23:11:53 localhost.localdomain sshd[24217]: Failed password for nhdd from
192.168.88.145 port 56436 ssh2
Jun 17 23:11:56 localhost.localdomain sshd[24214]: Failed password for nhdd from
192.168.88.145 port 56404 ssh2
Jun 17 23:11:56 localhost.localdomain sshd[24217]: Failed password for nhdd from
192.168.88.145 port 56436 ssh2
Jun 17 23:11:56 localhost.localdomain sshd[24215]: Failed password for nhdd from
192.168.88.145 port 56420 ssh2
Jun 17 23:11:56 localhost.localdomain sshd[24218]: Failed password for nhdd from
192.168.88.145 port 56444 ssh2
```

```
Jun 17 23:11:56 localhost.localdomain sshd[24214]: error: maximum authentication attempts
exceeded for nhdd from 192.168.88.145 port 56404 ssh2 [preauth]
Jun 17 23:11:56 localhost.localdomain sshd[24214]: Disconnecting authenticating user nhdd
192.168.88.145 port 56404: Too many authentication failures [preauth]
Jun 17 23:11:56 localhost.localdomain sshd[24214]: PAM 5 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:11:56 localhost.localdomain sshd[24214]: PAM service(sshd) ignoring max retries; 6
> 3
Jun 17 23:11:56 localhost.localdomain sshd[24215]: error: maximum authentication attempts
exceeded for nhdd from 192.168.88.145 port 56420 ssh2 [preauth]
Jun 17 23:11:56 localhost.localdomain sshd[24215]: Disconnecting authenticating user nhdd
192.168.88.145 port 56420: Too many authentication failures [preauth]
Jun 17 23:11:56 localhost.localdomain sshd[24215]: PAM 5 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:11:56 localhost.localdomain sshd[24215]: PAM service(sshd) ignoring max retries; 6
> 3
Jun 17 23:11:56 localhost.localdomain sshd[24217]: error: maximum authentication attempts
exceeded for nhdd from 192.168.88.145 port 56436 ssh2 [preauth]
Jun 17 23:11:56 localhost.localdomain sshd[24217]: Disconnecting authenticating user nhdd
192.168.88.145 port 56436: Too many authentication failures [preauth]
Jun 17 23:11:56 localhost.localdomain sshd[24217]: PAM 5 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:11:56 localhost.localdomain sshd[24217]: PAM service(sshd) ignoring max retries; 6
> 3
Jun 17 23:11:56 localhost.localdomain sshd[24218]: error: maximum authentication attempts
exceeded for nhdd from 192.168.88.145 port 56444 ssh2 [preauth]
Jun 17 23:11:56 localhost.localdomain sshd[24218]: Disconnecting authenticating user nhdd
192.168.88.145 port 56444: Too many authentication failures [preauth]
Jun 17 23:11:56 localhost.localdomain sshd[24218]: PAM 5 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:11:56 localhost.localdomain sshd[24218]: PAM service(sshd) ignoring max retries; 6
> 3
Jun 17 23:11:56 localhost.localdomain sshd[24248]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:11:56 localhost.localdomain sshd[24253]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:11:56 localhost.localdomain sshd[24250]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:11:56 localhost.localdomain sshd[24251]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:11:59 localhost.localdomain sshd[24248]: Failed password for nhdd from
192.168.88.145 port 56204 ssh2
Jun 17 23:11:59 localhost.localdomain sshd[24253]: Failed password for nhdd from
192.168.88.145 port 56240 ssh2
Jun 17 23:11:59 localhost.localdomain sshd[24250]: Failed password for nhdd from
192.168.88.145 port 56212 ssh2
Jun 17 23:11:59 localhost.localdomain sshd[24251]: Failed password for nhdd from
192.168.88.145 port 56226 ssh2
```

```
Jun 17 23:12:04 localhost.localdomain sshd[24248]: Failed password for nhdd from
192.168.88.145 port 56204 ssh2
Jun 17 23:12:04 localhost.localdomain sshd[24251]: Failed password for nhdd from
192.168.88.145 port 56226 ssh2
Jun 17 23:12:04 localhost.localdomain sshd[24250]: Failed password for nhdd from
192.168.88.145 port 56212 ssh2
Jun 17 23:12:04 localhost.localdomain sshd[24253]: Failed password for nhdd from
192.168.88.145 port 56240 ssh2
Jun 17 23:12:06 localhost.localdomain sshd[24248]: Failed password for nhdd from
192.168.88.145 port 56204 ssh2
Jun 17 23:12:06 localhost.localdomain sshd[24251]: Failed password for nhdd from
192.168.88.145 port 56226 ssh2
Jun 17 23:12:06 localhost.localdomain sshd[24250]: Failed password for nhdd from
192.168.88.145 port 56212 ssh2
Jun 17 23:12:06 localhost.localdomain sshd[24253]: Failed password for nhdd from
192.168.88.145 port 56240 ssh2
Jun 17 23:12:07 localhost.localdomain sshd[24248]: Accepted password for nhdd from
192.168.88.145 port 56204 ssh2
Jun 17 23:12:08 localhost.localdomain sshd[24248]: pam_unix(sshd:session): session opened
for user nhdd(uid=1005) by nhdd(uid=0)
Jun 17 23:12:08 localhost.localdomain sshd[24248]: pam_unix(sshd:session): session closed
for user nhdd
Jun 17 23:12:10 localhost.localdomain sshd[24251]: Failed password for nhdd from
192.168.88.145 port 56226 ssh2
Jun 17 23:12:10 localhost.localdomain sshd[24250]: Failed password for nhdd from
192.168.88.145 port 56212 ssh2
Jun 17 23:12:10 localhost.localdomain sshd[24253]: Failed password for nhdd from
192.168.88.145 port 56240 ssh2
Jun 17 23:12:10 localhost.localdomain sshd[24250]: Connection closed by authenticating user
nhdd 192.168.88.145 port 56212 [preauth]
Jun 17 23:12:10 localhost.localdomain sshd[24250]: PAM 3 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:12:10 localhost.localdomain sshd[24250]: PAM service(sshd) ignoring max retries; 4
> 3
Jun 17 23:12:10 localhost.localdomain sshd[24251]: Connection closed by authenticating user
nhdd 192.168.88.145 port 56226 [preauth]
Jun 17 23:12:10 localhost.localdomain sshd[24251]: PAM 3 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:12:10 localhost.localdomain sshd[24251]: PAM service(sshd) ignoring max retries; 4
> 3
Jun 17 23:12:10 localhost.localdomain sshd[24253]: Connection closed by authenticating user
nhdd 192.168.88.145 port 56240 [preauth]
Jun 17 23:12:10 localhost.localdomain sshd[24253]: PAM 3 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=nhdd
Jun 17 23:12:10 localhost.localdomain sshd[24253]: PAM service(sshd) ignoring max retries; 4
> 3
Jun 17 23:14:18 localhost.localdomain sudo[24386]: hoangdat : TTY=pts/2 ;
PWD=/home/hoangdat ; USER=root ; COMMAND=/bin/fail2ban-client status sshd
```

```
Jun 17 23:53:09 localhost.localdomain sudo[24624]: hoangdat : TTY=pts/1 ;
PWD=/home/hoangdat ; USER=root ; COMMAND=/bin/fail2ban-client status sshd
Jun 17 23:53:26 localhost.localdomain sudo[24642]: hoangdat : TTY=pts/1 ;
PWD=/home/hoangdat ; USER=root ; COMMAND=/bin/fail2ban-client status sshd
Jun 17 23:57:08 localhost.localdomain sudo[24722]: hoangdat : TTY=pts/1 ;
PWD=/home/hoangdat ; USER=root ; COMMAND=/bin/fail2ban-client status sshd
Jun 17 23:57:58 localhost.localdomain sshd[24742]: Received disconnect from 192.168.88.145
port 59194:11: Bye Bye [preauth]
Jun 17 23:57:58 localhost.localdomain sshd[24742]: Disconnected from authenticating user
hdat 192.168.88.145 port 59194 [preauth]
Jun 17 23:57:58 localhost.localdomain sshd[24747]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=hdat
Jun 17 23:57:58 localhost.localdomain sshd[24744]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=hdat
Jun 17 23:57:58 localhost.localdomain sshd[24745]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=hdat
Jun 17 23:57:58 localhost.localdomain sshd[24746]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=hdat
Jun 17 23:58:00 localhost.localdomain sshd[24747]: Failed password for hdat from
192.168.88.145 port 59228 ssh2
Jun 17 23:58:00 localhost.localdomain sshd[24744]: Failed password for hdat from
192.168.88.145 port 59216 ssh2
Jun 17 23:58:00 localhost.localdomain sshd[24745]: Failed password for hdat from
192.168.88.145 port 59202 ssh2
Jun 17 23:58:00 localhost.localdomain sshd[24746]: Failed password for hdat from
192.168.88.145 port 59244 ssh2
Jun 17 23:58:04 localhost.localdomain sshd[24744]: Failed password for hdat from
192.168.88.145 port 59216 ssh2
Jun 17 23:58:04 localhost.localdomain sshd[24747]: Failed password for hdat from
192.168.88.145 port 59228 ssh2
Jun 17 23:58:04 localhost.localdomain sshd[24746]: Failed password for hdat from
192.168.88.145 port 59244 ssh2
Jun 17 23:58:04 localhost.localdomain sshd[24745]: Failed password for hdat from
192.168.88.145 port 59202 ssh2
Jun 17 23:58:04 localhost.localdomain sshd[24744]: Accepted password for hdat from
192.168.88.145 port 59216 ssh2
Jun 17 23:58:05 localhost.localdomain sshd[24744]: pam_unix(sshd:session): session opened
for user hdat(uid=1002) by hdat(uid=0)
Jun 17 23:58:05 localhost.localdomain sshd[24744]: pam_unix(sshd:session): session closed
for user hdat
Jun 17 23:58:06 localhost.localdomain sshd[24747]: Failed password for hdat from
192.168.88.145 port 59228 ssh2
Jun 17 23:58:06 localhost.localdomain sshd[24745]: Failed password for hdat from
192.168.88.145 port 59202 ssh2
Jun 17 23:58:06 localhost.localdomain sshd[24746]: Failed password for hdat from
192.168.88.145 port 59244 ssh2
Jun 17 23:58:07 localhost.localdomain sshd[24747]: Connection closed by authenticating user
hdat 192.168.88.145 port 59228 [preauth]
```

```
Jun 17 23:58:07 localhost.localdomain sshd[24747]: PAM 2 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=hdat
Jun 17 23:58:07 localhost.localdomain sshd[24746]: Connection closed by authenticating user
hdat 192.168.88.145 port 59244 [preauth]
Jun 17 23:58:07 localhost.localdomain sshd[24746]: PAM 2 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=hdat
Jun 17 23:58:07 localhost.localdomain sshd[24745]: Connection closed by authenticating user
hdat 192.168.88.145 port 59202 [preauth]
Jun 17 23:58:07 localhost.localdomain sshd[24745]: PAM 2 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.88.145  user=hdat
Jun 18 00:01:23 localhost.localdomain sudo[24831]: hoangdat : TTY=pts/1 ;
PWD=/home/hoangdat ; USER=root ; COMMAND=/bin/fail2ban-client status sshd
Jun 18 00:06:33 localhost.localdomain sudo[24917]: hoangdat : TTY=pts/1 ;
PWD=/home/hoangdat ; USER=root ; COMMAND=/bin/fail2ban-client status sshd
```

6. Log của fail2ban

```
[hoangdat@localhost ~]$ sudo cat /var/log/fail2ban.log
2025-06-17 21:57:02,889 fail2ban.server         [20964]: INFO    -------------------------------------
-------------
2025-06-17 21:57:02,890 fail2ban.server         [20964]: INFO    Starting Fail2ban v1.1.0
2025-06-17 21:57:02,890 fail2ban.observer       [20964]: INFO    Observer start...
2025-06-17 21:57:02,902 fail2ban.database       [20964]: INFO    Connected to fail2ban
persistent database '/var/lib/fail2ban/fail2ban.sqlite3'
2025-06-17 21:57:02,905 fail2ban.database       [20964]: WARNING New database created.
Version '4'
2025-06-17 22:17:41,162 fail2ban.server         [20964]: INFO    Shutdown in progress...
2025-06-17 22:17:41,163 fail2ban.observer       [20964]: INFO    Observer stop ... try to end
queue 5 seconds
2025-06-17 22:17:41,183 fail2ban.observer       [20964]: INFO    Observer stopped, 0 events
remaining.
2025-06-17 22:17:41,224 fail2ban.server         [20964]: INFO    Stopping all jails
2025-06-17 22:17:41,225 fail2ban.database       [20964]: INFO    Connection to database
closed.
2025-06-17 22:17:41,226 fail2ban.server         [20964]: INFO    Exiting Fail2ban
2025-06-17 23:56:46,271 fail2ban.server         [24696]: INFO    -------------------------------------
-------------
2025-06-17 23:56:46,272 fail2ban.server         [24696]: INFO    Starting Fail2ban v1.1.0
2025-06-17 23:56:46,273 fail2ban.observer       [24696]: INFO    Observer start...
2025-06-17 23:56:46,291 fail2ban.database       [24696]: INFO    Connected to fail2ban
persistent database '/var/lib/fail2ban/fail2ban.sqlite3'
2025-06-17 23:56:46,313 fail2ban.jail           [24696]: INFO    Creating new jail 'sshd'
2025-06-17 23:56:46,357 fail2ban.jail           [24696]: INFO    Jail 'sshd' uses systemd {}
2025-06-17 23:56:46,359 fail2ban.jail           [24696]: INFO    Initiated 'systemd' backend
2025-06-17 23:56:46,361 fail2ban.filter         [24696]: INFO      maxLines: 1
2025-06-17 23:56:46,374 fail2ban.filtersystemd  [24696]: INFO    [sshd] Added journal match
for: '_SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session'
```

```
2025-06-17 23:56:46,374 fail2ban.filter         [24696]: INFO      maxRetry: 3
2025-06-17 23:56:46,374 fail2ban.filter         [24696]: INFO      findtime: 300
2025-06-17 23:56:46,374 fail2ban.actions        [24696]: INFO      banTime: 600
2025-06-17 23:56:46,375 fail2ban.filter         [24696]: INFO      encoding: UTF-8
2025-06-17 23:56:46,380 fail2ban.jail           [24696]: INFO    Jail 'sshd' started
2025-06-17 23:56:46,448 fail2ban.filtersystemd  [24696]: INFO    [sshd] Jail is in operation
now (process new journal entries)
2025-06-17 23:58:01,069 fail2ban.filter         [24696]: INFO    [sshd] Found 192.168.88.145 -
2025-06-17 23:58:00
2025-06-17 23:58:01,070 fail2ban.filter         [24696]: INFO    [sshd] Found 192.168.88.145 -
2025-06-17 23:58:00
2025-06-17 23:58:01,070 fail2ban.filter         [24696]: INFO    [sshd] Found 192.168.88.145 -
2025-06-17 23:58:00
2025-06-17 23:58:01,070 fail2ban.filter         [24696]: INFO    [sshd] Found 192.168.88.145 -
2025-06-17 23:58:00
2025-06-17 23:58:01,224 fail2ban.actions        [24696]: NOTICE  [sshd] Ban 192.168.88.145
2025-06-17 23:58:04,202 fail2ban.filter         [24696]: INFO    [sshd] Found 192.168.88.145 -
2025-06-17 23:58:04
2025-06-17 23:58:04,203 fail2ban.filter         [24696]: INFO    [sshd] Found 192.168.88.145 -
2025-06-17 23:58:04
2025-06-17 23:58:04,203 fail2ban.filter         [24696]: INFO    [sshd] Found 192.168.88.145 -
2025-06-17 23:58:04
2025-06-17 23:58:04,204 fail2ban.filter         [24696]: INFO    [sshd] Found 192.168.88.145 -
2025-06-17 23:58:04
2025-06-17 23:58:04,711 fail2ban.actions        [24696]: NOTICE  [sshd] 192.168.88.145
already banned
2025-06-17 23:58:06,996 fail2ban.filter         [24696]: INFO    [sshd] Found 192.168.88.145 -
2025-06-17 23:58:06
2025-06-17 23:58:06,997 fail2ban.filter         [24696]: INFO    [sshd] Found 192.168.88.145 -
2025-06-17 23:58:06
2025-06-17 23:58:06,997 fail2ban.filter         [24696]: INFO    [sshd] Found 192.168.88.145 -
2025-06-17 23:58:06
2025-06-17 23:58:07,316 fail2ban.actions        [24696]: NOTICE  [sshd] 192.168.88.145
already banned
2025-06-18 00:08:06,655 fail2ban.actions        [24696]: NOTICE  [sshd] Unban
192.168.88.145
```

- Khởi động dịch vụ Fail2Ban

2025-06-17 23:56:46,272 fail2ban.server: INFO Starting Fail2ban v1.1.0

→ Dịch vụ Fail2Ban bắt đầu chạy (phiên bản 1.1.0).

2025-06-17 23:56:46,313 fail2ban.jail: INFO Creating new jail 'sshd'

→ Jail tên sshd được tạo. Jail này sẽ giám sát các lần đăng nhập SSH thất bại.

- Thông số cấu hình Jail sshd

```
maxRetry: 3
findtime: 300
banTime: 600
```

- maxRetry = 3: Nếu 1 IP sai mật khẩu quá 3 lần…
- findtime = 300: … trong vòng 5 phút (300 giây)…
- banTime = 600: … thì sẽ bị chặn trong vòng 10 phút (600 giây).

- Phát hiện hành vi brute-force từ IP 192.168.88.145

```
2025-06-17 23:58:01,070 fail2ban.filter: INFO [sshd] Found 192.168.88.145
 …………
2025-06-17 23:58:01,224 fail2ban.actions: NOTICE [sshd] Ban 192.168.88.145
```

→ IP 192.168.88.145 đã vi phạm quá số lần đăng nhập sai cho phép, nên đã bị chặn bởi iptables.

```
2025-06-17 23:58:04,711 fail2ban.actions: NOTICE [sshd] 192.168.88.145 already banned
```

→ Fail2Ban phát hiện IP này tiếp tục brute-force, nhưng đã bị block nên không thể tiếp tục truy cập SSH.

- Hết thời gian ban (10 phút sau)

```
2025-06-18 00:08:06,655 fail2ban.actions: NOTICE [sshd] Unban 192.168.88.145
```

→ Hết thời gian block (600 giây), IP tự động được gỡ chặn (unban).