

รับมือ Hacker ใช้เทคนิค brute-force เล่นงานเรา **Brute force Attacking from hackers**

ผู้ช่วยศาสตราจารย์ ดร.กิตติพงษ์ สุวรรณราช : เขียน

Asst. Prof. Dr. Kittipong Suwannaraj

ECA , MTCNA, MTCUME, MTCTCE, RHCT

kitti@psru.ac.th

หากเราพูดถึงการโจมตีของ Hacker แบบ Brute force Attacking นั้น ผู้ดูแลระบบที่มีประสบการณ์ก็มักจะทราบกันดีครับว่าเป็นการโจมตีในลักษณะใด แต่สำหรับผู้ดูแลระบบมือใหม่หรือผู้ที่ยังไม่มีประสบการณ์กับการโจมตีในลักษณะของ Brute force นั้น จะขออธิบายให้ฟังเพื่อเป็นความรู้เบื้องต้นก่อนที่จะอ่านวิธีแก้ไขต่อไปครับ

การโจมตีแบบ Brute force นั้นผู้โจมตี หรือที่เราเรียกว่า (Attacker) จะทำการส่งรหัสผ่าน (password) หรือเรียกว่า (passphrases) จำนวนมากเป็นหลายร้อย หรือหลายพันคำ ส่งเข้ามายัง Server ของเราโดยผ่านทาง Protocol ที่เป็นเป้าหมายของการบุกรุกเช่น Protocol SSH (ใช้ Port : 22 TCP) เป็นต้น เราเรียกการโจมตีนี้ว่า SSH Brute-force Attacking จะส่งเข้ามาจนสามารถค้นพบรหัสผ่านในการเข้าระบบของเราได้ ซึ่งปัจจุบันถือว่าเป็นช่องทางที่นิยมบุกรุกมากสำหรับ Linux Server เนื่องจากหากบุกรุกสำเร็จจะสามารถเข้าไปยังระบบได้ง่าย และทำลาย Server ได้หลายรูปแบบ เครื่องมือที่ Hacker นิยมใช้ในการโจมตีแบบ Brute force นั้นมีหลายตัวครับที่นิยมใช้ก็คือ Hydra โดยโปรแกรม Hydra นี้จะต้องกำหนด ip address เป้าหมายในการโจมตี และตามด้วยไฟล์ dictionary (เป็นไฟล์ที่เก็บรหัสผ่านที่คาดว่าจะถูกต้องมีเป็นหมื่นๆ บรรทัดในไฟล์นี้) หรือที่เราเรียกว่า Password Cracking World lists โปรแกรม Hydra จะลองไปเรื่อย ๆ จนกว่าจะถูกต้อง

```

juniour@hackaholic: ~/pass
juniour@hackaholic:~/pass$ ls
Bnum      dark0de.lst  dict.txt-   johnpass.lst-  num.txt.txt  password.lst-
airpass.lst  dic-0294.txt  final-wordlist.txt  mine.lst      pass1.lst    rockyou.txt
DB.DIC      dict.txt     johnpass.lst  NORM.DIC      password.lst
juniour@hackaholic:~/pass$ sudo hydra 127.0.0.1 ssh -l juniour -P dict.txt -s 22 -v
Hydra v7.5 (c)2013 by van Hauser/THC & David Mactejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2014-12-26 04:40:48
[DATA] 5 tasks, 1 server, 5 login tries (l:1/p:5), -1 try per task
[VERBOSE] Resolving addresses ... done
[ATTEMPT] target 127.0.0.1 - login 'juniour' - pass 'hello' - 1 of 5 [child 0]
[ATTEMPT] target 127.0.0.1 - login 'juniour' - pass 'hello1234' - 2 of 5 [child 1]
[ATTEMPT] target 127.0.0.1 - login 'juniour' - pass 'blabla' - 3 of 5 [child 2]
[ATTEMPT] target 127.0.0.1 - login 'juniour' - pass 'helloworld' - 4 of 5 [child 3]
[ATTEMPT] target 127.0.0.1 - login 'juniour' - pass 'alexbob' - 5 of 5 [child 4]
[22][ssh] host: 127.0.0.1 login: juniour password: helloworld
[STATUS] 1 of 1 target
Hydra (http://www.thc.org/thc-hydra) finished
juniour@hackaholic:~/pass$

```

รูปที่ 1. โปรแกรม HTC hydra ใช้ในการ Brute-force SSH protocol

รับมือ Hacker ใช้เทคนิค brute-force เล่นงานเรา **Brute force Attacking from hackers**


```

root@kali:~/WPA_cowpatty# grep password12345 rockyou.txt
password12345
password123456789
password123456
password1234567
password12345678
password1234567890
password12345678910
password1234567 -
password12345?
password123456
password1234567899
password123456.
newpassword12345
mypassword12345.
mypassword12345
bpassword12345b
root@kali:~/WPA_cowpatty#

```

รูปที่ 2. ตัวอย่างไฟล์ Password Cracking World lists

**ทำไม Hacker รู้ว่า SSH ใช้พอร์ตสื่อสารหมายเลข 22 ?**

การที่ Hacker รู้ว่า Server ของเรานั้นเปิดพอร์ตสื่อสารใดไว้บ้างนั้น ไม่ใช่เรื่องยากอะไร เพียงแค่ใช้เครื่องมือในการ Scan ports ตัวอย่างเช่น โปรแกรม nmap ทำการสแกนพอร์ตของ ip address ของ Server ก็สามารถบอกรายละเอียดได้ทันทีครับ และโดยส่วนใหญ่ Internet Service ต่าง ๆ ก็จะมีพอร์ตมาตรฐานของตัวเองที่ได้จองไว้เรียบร้อยแล้ว เช่น พอร์ต 20 และ 21 คือ ftp , พอร์ต 23 คือ telnet เป็นต้น หากเราอยากทราบว่าพอร์ตมาตรฐาน (UDP, TCP Standard port) มีพอร์ตหมายเลขใดบ้าง สามารถดูได้จาก [https://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers) โดยถ้าเราไล่ดูดี ๆ จะเห็นว่า Standard Port หรือ บางครั้งก็เรียกว่า Well-known ports จะอยู่ตั้งแต่หมายเลข 0-1023 นั้น หมายความว่า เราควรระวังการป้องกันตัวเองโดยการ เปลี่ยนพอร์ต หรือปิดพอร์ตที่ไม่มีการใช้งานครับ เพื่อความปลอดภัย และไม่เป็นการเปิดบ้านต้อนรับ Hacker มากเกินไป

**การป้องกันการ SSH Brute force** ที่นิยมใช้ในปัจจุบันมีอยู่หลายวิธีการด้วยกัน แล้วแต่ประสบการณ์ของผู้ดูแลระบบเครือข่ายแต่ละคน จะขอแนะนำวิธีการที่ได้ผลดีและจากประสบการณ์การทำงานด้านนี้

1. เปลี่ยนพอร์ตไปใช้พอร์ตที่สูงขึ้น แน่แน่นอนครับว่า Hacker รู้ว่าพอร์ต 22 คือเป้าหมายของการโจมตี Protocol SSH นั้นเราควรที่จะปิดพอร์ตนี้ เปลี่ยนไปใช้พอร์ตที่อยู่หมายเลขที่สูงกว่า 1023 ขึ้นไป เพื่อหลีกเลี่ยงการโดน Scan ports แนะนำให้ใช้ตั้งแต่ port number เป็นหมื่นขึ้นไป เพราะโดยปกติของการ Scan port นั้น Hacker จะเลือกที่จะ Scan พอร์ตมาตรฐานเป็นหลัก (0-1,023) เนื่องจากการ Scan แต่ละ ip address นั้น ใช้เวลาพอสมควรครับ อาจจะไม่โดนเราตรวจพบได้ว่าการ Scan port

รับมือ Hacker ใช้เทคนิค brute-force เล่นงานเรา **Brute force Attacking from hackers**

การเปลี่ยนพอร์ตของ SSH นั้นบน Linux Centos เราจะทำการแก้ไขดังนี้

```
# nano /etc/ssh/sshd_config
ค้นหาคำว่า Port 22 แล้วเปลี่ยนค่า 22 เป็นหมายเลขอื่นๆ เช่น 50683
# What ports, IPs and protocols we listen for
Port 50683
```

2. การติดตั้งโปรแกรมที่ชื่อว่า fail2ban บน Linux โปรแกรมนี้จะเป็นโปรแกรมที่คอยเฝ้าดู (Port Monitoring) ว่ามีการพยายามเข้ามาที่ Port หมายเลขใด แล้วรอกองรหัสผ่านผิดกี่ครั้ง (ถ้าครบตามจำนวนที่เราได้กำหนดไว้ fail2ban จะทำการ block ip

## Fail2Ban



address ของ Hacker ทันทีอัตโนมัติ) ทำให้ Hacker จะต้องเปลี่ยน ip address เข้ามาโจมตีใหม่ ซึ่งเป็นการเสียเวลาพอสมควร การติดตั้ง fail2ban นั้นสามารถอ่านรายละเอียดเพิ่มเติมได้จาก <https://www.digitalocean.com/community/tutorials/how-to-protect-ssh-with-fail2ban-on-centos-7>

3. ใช้การเชื่อมต่อเข้าบริการของ Server ของเราด้วย VPN (Virtual Private Network) ซึ่งก็จะทำให้เครื่อง Server ของเรามีความปลอดภัยมากยิ่งขึ้น

4. เขียน Firewall เพื่อระบุว่า ip address ที่จะสามารถใช้บริการ ssh เข้ามายัง Server ได้นั้นจะต้องมาจาก ip address ใดได้บ้าง วิธีการแบบนี้ก็ต้องมีการเขียน Firewall rule เพิ่มเติมที่อุปกรณ์ เพื่อเป็นการบอกให้รู้ว่าการเข้ามานั้นจะต้องมาจาก Host ต้นทางที่ไว้ใจได้เท่านั้น



## รับมือ Hacker ใช้เทคนิค brute-force เล่นงานเรา **Brute force Attacking from hackers**

แหล่งสืบค้นเพิ่มเติม :

1. <http://colorpack.net/host-articles/904-cms-web-tip/3388-brute-force-attack-password-attacks.html>
2. [https://en.wikipedia.org/wiki/Brute-force\\_attack](https://en.wikipedia.org/wiki/Brute-force_attack)
3. [https://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)

บริการบน: linux , FreeBSD , Unix services , Windows Server Services

Article number : 201601110419