เขียน firewall Rules 1 rule = 194 rules ป้องกันการบุกรุกจากต่างประเทศ

ผู้ช่วยศาสตราจารย์ ดร.กิตติพงษ์ สุวรรณราช : เขียน

Asst. Prof. Dr. Kittipong Suwannaraj

ECA , MTCNA, MTCUME, MTCTCE, RHCT

kitti@psru.ac.th

วันนี้ขอนำเสนอบทความเกี่ยวกับการการเขียน Firewall Rules ด้วย iptables บนระบบปฏิบัติการ CentOS เพื่อใช้สำหรับปิดกั้นการบุกรุกเครือข่าย เครื่องแม่ข่ายระบบโทรศัพท์ Elastix หรือ Asterisk ที่ทำงานบน Linux ตระกูล CentOS ครับ ซึ่งปัจจุบันนี้เราจะเป็นได้ว่าการบุกรุกเครื่องแม่ข่ายที่ให้บริการ Voice over IP : VoIP มีจำนวนเยอะมากขึ้นทุกขณะ เนื่องจากเป้าหมายของการบุกรุกเครือข่าย VoIP นั้น หากเราป้องกันไม่ดีก็จะเป็นช่องทางที่จะทำให้ Hacker จะเอาเครื่องแม่ข่ายของเราเป็นไป Gateway ในการโทรออกไปยังต่างประเทศ ซึ่งก็จะทำให้ค่าใช้จ่ายนั้นเกิดขึ้นกับองค์กรเป็นจำนวนมาก แต่อย่างไรก็ดีครับ ปัญหาที่ได้กล่าวมานั้นมีทางแก้ไขได้หลายวิธี วันนี้ผมจะแนะนำวิธีการหนึ่งซึ่งเป็นวิธีการที่ใช้งานได้ผลเป็นอย่างดี หลังจากที่ได้มีการทดสอบกับเครือข่าย เครื่องแม่ข่ายขององค์กรตัวเองแล้วไม่ต่ำกว่า 1 ปี ก็สามารถปิดกั้นการบุกรุกเครือข่ายจากบรรดา Hacker ต่างประเทศได้เป็นอย่างดี

กรณีศึกษานี้ เราจะใช้ในกรณีที่เราต้องการปิดกั้นการลงทะเบียน หรือ register ของเครื่องลูกข่ายโทรศัพท์จากประเทศต่าง ๆ ทุกประเทศ (ปัจจุบันมีประเทศต่าง ๆ ที่อยู่ทั่วโลกทั้งหมด 195 ประเทศ รวมประเทศไทยของเราด้วย ปัจจุบันประเทศไทยของเรามีประชากรมากเป็นอันดับที่ 20 จาก 195 ประเทศทั่วโลก) ซึ่งถ้าเราต้องการที่จะปิดกั้นประเทศต่าง ๆ จากทั่วโลก เราก็อาจจะต้องเขียน Firewall Rules เท่ากับจำนวนประเทศทั้งหมด-1 คือ 194 ชุดคำสั่ง บรรดา Hacker ที่บุกรุกระบบโทรศัพท์เข้ามาในเครือข่ายของเรานั้น ต้องบอกว่าก็มาจากหลากหลายประเทศเช่นกันครับ เราปิดกั้นประเทศหนึ่ง เขาก็หา IP address ในประเทศอื่นมาบุกรุกเรา แต่มันก็ไม่ใช่เรื่องง่ายที่จะหา IP address ชุดใหม่มาบุกรุกเราได้ง่าย ๆ เรามาดูครับว่า เราจะใช้เทคนิคอะไรในการปิดกั้นการโจมตีในลักษณะนี้ได้บ้าง

เทคนิคที่จะนำเสนอในวันนี้ การปิดกั้น IP address จากต่างประเทศ ตามประเทศที่เราต้องการ เราจะใช้เทคนิคที่เรียกว่า GeoIP หรือ Geolocation IP address ซึ่งเราสามารถระบุได้เลยว่าเราจะปิดกั้นการเข้าถึงเครือข่ายของเรา หรือเครื่องแม่ข่ายของเราได้จากประเทศต้นทาง เช่น ทำการ Block ip address ของประเทศจีนทั้งหมด หรือประเทศใด ๆ ก็ได้ตามที่เราต้องการ ซึ่งอาจจะเป็นต้นทางที่ Hacker ใช้ในการบุกรุกเครือข่ายของเราเป็นต้น เรามาเรียนรู้วิธีการติดตั้งการใช้เทคนิค GeoIP กันเลยครับ

เขียน firewall Rules 1 rule = 194 rules ป้องกันการบุกรุกจากต่างประเทศ

วิธีการติดตั้ง GeoIP

ในการติดตั้ง GeoIP นี้ ขอแนะนำบนระบบปฏิบัติการ CentOS ซึ่งหากท่านใช้ระบบปฏิบัติการอื่นๆ ก็สามารถประยุกต์ตามวิธีการตามนี้ได้

```
# yum install gcc gcc-c++ make automake iptables-devel wget nano unzip zip xz
# yum install perl-Text-CSV_XS
# mkdir -p /opt/src
# cd /opt/src
# yum install iptables*
# uname –r
# base_url=http://sourceforge.net/projects/xtables-addons/files/Xtables-addons
# wget -t 3 -T 30 -qO- $base_url/xtables-addons-2.10.tar.xz | tar xJv
# cd xtables-addons-*
# ./configuremake && make install
# depmod
# cd geoip/
# ./xt_geoip_dl
# ./xt_geoip_build GeoIPCountryWhois.csv
# mkdir -p /usr/share/xt_geoip/
# cp -r {BE,LE} /usr/share/xt_geoip/
(เสร็จกระบวนการติดตั้ง GeoIP)
```

การทดสอบ GeoIP จากประเทศสหรัฐอเมริกา

```
# iptables -I INPUT -m geoip --src-cc US
# iptables -D INPUT -m geoip --src-cc US
```

หากเราสามารถรัน 2 บรรทัดด้านบนผ่านแสดงว่า iptables นั้นรับรู้ IP address class ทั้งหมดของประเทศสหรัฐอเมริกาเรียบร้อยแล้ว หากทดสอบไม่ผ่านก็จะมี Error แจ้งให้ทราบ

เขียน firewall Rules 1 rule = 194 rules ป้องกันการบุกรุกจากต่างประเทศ

ตัวอย่างที่ 1 การปิดกั้นบริการ SSH ที่ Port Number : 21 ที่มาจากประเทศสหรัฐอเมริกาทั้งหมด

```
# iptables -A INPUT -p tcp --dport 21 -m geoip --src-cc US -j DROP
# iptables -A INPUT -p tcp --dport 21 -j ACCEPT
```

ตัวอย่างที่ 2 การปิดกั้นบริการ SSH ที่ Port Number : 21 ที่มาจากประเทศญี่ปุ่นทั้งหมด

```
# iptables -A INPUT -p tcp --dport 21 -m geoip --src-cc JP -j DROP
# iptables -A INPUT -p tcp --dport 21 -j ACCEPT
```

ตัวอย่างที่ 3 การปิดกั้นบริการ SIP Port Number : 5060 ที่มาจากประเทศญี่ปุ่นทั้งหมด

```
iptables -A INPUT -p udp --dport 5060 -m geoip --src-cc JP -j DROP
iptables -A INPUT -p udp --dport 5060 -j ACCEPT
```

จากตัวอย่างที่ยกมาให้ดูทั้งสามตัวอย่างนั้น เราจะเห็นว่า GeoIP นั้นสามารถทำการปิดกั้นบริการต่าง ๆ ที่เราระบุไว้ โดยทำการปิดกั้นเฉพาะ IP address ของประเทศที่เราระบุไว้เช่น US หมายถึง สหรัฐอเมริกา JP หมายถึง ญี่ปุ่น เป็นต้น ถ้าเราปิดกั้นแบบตรงไปตรงมาลักษณะนี้ เราก็จะเหนื่อยมาก เพราะจะต้องปิดกั้น Service ต่าง ๆ ตามประเทศที่เราสนใจต้นทางที่บุกรุกมา แต่ถ้าเราคิดใหม่ แบบนี้โดยจะเป็นการมอบแบบตรงข้ามของ IP firewall rules ตัวอย่างเช่น

ตัวอย่างที่ 4 การอนุญาตเฉพาะ IP class ในประเทศไทยสามารถใช้บริการผ่าน https (443) ได้

```
# iptables -A INPUT -p tcp --dport 443 -m geoip --src-cc TH -j ACCEPT
# iptables -A INPUT -p tcp --dport 443 -j DROP
```

จากตัวอย่างที่ 4 จะเห็นได้ว่า เรามองอีกมุมหนึ่งคือ ไม่ได้มองที่ประเทศต้นทางเป็นหลัก เรามองที่ว่า เราจะอนุญาตเฉพาะ IP address ของประเทศไทยเท่านั้น ที่เหลือ Drop ทิ้งให้หมด เราก็จะไม่ต้องเหนื่อยในการเขียน IP firewall rules กับประเทศต่างๆ ทั้ง 194 ประเทศ ซึ่งวิธีการนี้เราก็สามารถนำไปประยุกต์การป้องกันกับบริการอื่นๆ ได้อีกมากมายครับ ขอบคุณครับ

แหล่งสืบค้นข้อมูล :

http://www.worldometers.info/geography/how-many-countries-are-there-in-the-world/

Article number : 201609111600