CHƠNG IV : CÁC KIỂU TẤN CÔNG VÀO FIREWALL VÀ CÁC BIỆN PHÁP PHÒNG CHỐNG

Suốt từ khi Cheswick và Bellovin viết cuốn anh hùng ca về cách xây dựng các bức tờng lửa và theo dõi một hắc cơ quỷ quyệt tên Berferd, ý tởng thiết đặt một hệ phục vụ web trên Internet mà không triển khai một bức tờng lửa đã đợc xem là tự sát. Cũng bằng nh tự sát nếu quyết định phó mặc các nhiệm vụ về bức tờng lửa vào tay các kỹ s mạng. Tuy giới này có thể tìm hiểu các quan hệ mật thiết về kỹ thuật của một bức tờng lửa, song lại không hòa chung nhịp thở với hệ bảo mật và tìm hiểu não trạng cũng nh các kỹ thuật của các tay hắc cơ quỷ quyệt. Kết quả là, các bức tờng lửa có thể bị chọc thủng do cấu hình sai, cho phép bọn tấn công nhảy bổ vào mạng và gây ra đại họa.

I. Phong cảnh bức tờng lửa

Hai kiểu bức tờng lửa đang thống lĩnh thị trờng hiện nay: hệ giám quản ứng dụng (application proxies) và các ngỏ thông lọc gói tin (packet filtering gateway). Tuy các hệ giám quản ứng dụng đợc xem là an ninh hơn các ngỏ thông lọc gói tin, song bản chất hạn hẹp và các hạn chế khả năng vận hành

của chúng đã giới hạn chúng vào luồng lu thông đi ra công ty thay vì luồng lu thông đi vào hệ phục vụ web của công ty. Trong khi đó, ta có thể gặp các ngỏ thông loc gói tin, hoặc các ngỏ thông lọc gói tin hữu trạng (stateful) phức hợp hơn, mặt khác, trong nhiều tổ chức lớn có các yêu cầu khả năng vận hành cao.

Nhiều ngời tin rằng hiện cha xuất hiện bứcc tờng lửa "hoàn hảo", nhng tơng lai đầy sán lạn. Một số hãng kinh doanh nh Network Associates Inc. (NAI), AXENT, Internet Dynamics, và Microsoft đã phát triển công nghệ cung cấp tính năng bảo mật của công nghệ giám quản với khả năng vận hành của công nghệ lọc gói tin (một dạng lai ghép giữa hai công nghệ). Nhng chúng vẫn cha già dặn.

Suốt từ khi bức tờng lửa đầu tiên đợc cài đặt, các bức tờng lửa đã bảo vệ vô số mạng tránh đợc những cặp mắt tò mò và bọn phá hoại nhng còn lâu chúng mới trở thành phơng thuốc trị bách bệnh bảo mật. Các chỗ yếu bảo mật đều đợc phát hiện hàng năm với hầu nh mọi kiểu bức tờng lửa trên thị trờng. Tệ hại hơn, hầu hết các bức tờng lửa thờng bị cấu hình sai, không bảo trì, và không giám sát, biến chúng trở thành một vật cản cửa điện tử (giữ cho các ngỏ thông luôn rộng mở).

Nến không phạm sai lầm, một bức tờng lửa đợc thiết kế, cấu hình, và bảo trì kỹ lỡng hầu nh kh ông thể đột nhập. Thực tế, hầu hết các kẻ tấn công có tay nghề cao đều biết điều này và sẽ đơn giản tránh vòng qua bức tờng lửa bằng cách khai thác các tuyến quan hệ ủy quản (trust relationships) và các chỗ yếu bảo mật nối kết lỏng lẻo nhất, hoặc tránh nó hoàn toàn bằng cách tấn công qna một tài khoản

quay số.

Điểm căn bản: hầu hết bọn tấn công dồn mọi nỗ lực để vòng qua một bức tờng lửa mạnh - mục tiêu ở đây là tạo một bức tờng lửa mạnh.

Với t cách là điều hành viên bức tờng lửa, ta biết rõ tầm quan trọng của việc tìm hiểu kẻ địch. Nắm đợc các bớc đầu tiên mà một bọn tấn công thực hiện để bỏ qua các bức tờng lửa sẽ giúp bạn rất nhiều trong việc phát hiện và phản ứng lại một cuộc tấn công. Chơng này sẽ hớng dẫn bạn qua các kỹ thuật thờng dùng hiện nay để phát hiện và điểm danh các bức tờng lửa, đồng thời mô tả vài cách mà bọn tấn công gắng bỏ qua chúng. Với từng kỹ thuật, ta sẽ tìm hiểu cách phát hiện và ngăn chặn các cuộc tấn công.

II. Định danh các bức tờng lửa

Hầu hết mọi bức tờng lửa đều mang một "mùi hơng" điện tử duy nhất. Nghĩa là, với một tiến trình quét cổng, lập cầu lửa, và nắm giữ biểu ngữ đơn giản, bọn tấn công có thể hiệu quả xác định kiểu, phiên bản, và các quy tắc của hầu hết mọi bức tờng lửa trên mạng. Tại sao việc định danh này lại quan trọng? Bởi vì một khi đã ánh xạ đợc các bức tờng lửa, chúng có thể bắt đầu tìm hiểu các điểm yếu và gắng khai thác chúng.

1. Quét trực tiếp : Kỹ thuật Noisy

Cách dễ nhất để tìm kiếm các bức tờng lửa đó là quét các cổng ngầm định cụ thể. Một số bức t-ờng lửa trên thị trờng sẽ tự định danh duy nhất bằng các đợt quét cổng đơn giản bạn chỉ cần biết nội dung tìm kiếm.

Ví dụ, Firewall-1 của Check point lắng chờ trên các cổng TCP 256, 257, 258, và Proxy Server của Microsoft thờng lắng chờ trên các cổng TCP 1080 và 1745. Với sự hiểu biết này, quá trình tìm kiếm các kiểu bức tờng lửa này chẳng có gì khó với một bộ quét cổng nh nmap:

```
nmap -n -vv -P0 -p256,1080,1745 192.168.50.1 - 60.254
```

Dùng khóa chuyển -PO để vô hiệu hóa tính năng ping ICMP trớc khi quét. Điều này quan trọng bởi hầu hết bức tờng lửa không đáp ứng các yêu cầu dội ICMP.

Cả bọn tấn công nhút nhát lẫn hung bạo đều tiến hành quét rộng rãi mạng của bạn theo cách này, tìm kiếm các bức tờng lửa này và tìm kiếm mọi khe hở trong két sắt vành đai của bạn. Nhng bọn tấn công nguy hiểm hơn sẽ lùng sục

vành đai của bạn càng lén lút càng tốt. Có nhiều kỹ thuật mà bọn tấn công có thể sử dụng để hạ sập radar của bạn, bao gồm ngẫu nhiên hóa các ping, các cổng đích, các địa chỉ đích, và các cổng nguồn; dùng các hệ chủ cò mồi; và thực hiện các đợt quét nguồn có phân phối.

Nếu cho rằng hệ thống phát hiện xâm nhập (IDS) của bạn nh RealSecure của Internet Security Systems

hoặc SessionWall-3 của Abirnet sẽ phát hiện bọn tấn công nguy hiểm này, bạn nên suy nghĩ lại. Hầu hết các IDS đều ngầm định cấu hình để chỉ nghe các đợt quét cổng ngu đần và ồn ào nhất. Trừ phi bạn sử dụng IDS nhanh nhạy và tinh chỉnh các ký danh phát hiện, hầu hết các cuộc tấn công sẽ hoàn toàn làm ngơ. Bạn có thể tạo một đợt quét ngẫu nhiên hóa nh vậy bằng cách dùng các ký mã Perl cung cấp trên chuyên khu web www.osborne.com/ <http://www.osborne.com/> hacking .

Các biện pháp phòng chống

Bạn cần phong tỏa các kiểu quét này tại các bộ định tuyến biên hoặc dùng một kiểu công cụ phát hiện đột nhập nào đó miễn phí hoặc thơng mại. Mặc dù thế, các đợt quét cổng đơn lẻ sẽ không đợc thu nhặt theo ngầm định trong hầu hết các IDS do đó bạn phải tinh chỉnh độ nhạy cảm của nó trớc khi có thể dựa vào tính năng phát hiện.

Phát Hiện

Để chính xác phát hiện các đợt quét cổng bằng tính năng ngẫu nhiên hóa và các hệ chủ cò mồi, bạn cần tinh chỉnh từng lý danh phát hiện quét cổng. Tham khảo tài liệu hớng dẫn sử dụng của hãng kinh doanh IDS để biết thêm chi tiết.

Nêu muốn dùng RealSecure 3.0 để phát hiện tiến trình quét trên đây, bạn ắt phải nâng cao độ nhạy cảm của nó theo các đợt quét cổng đơn lẻ bàng cách sửa đổi các tham số của ký danh quét cổng. Bạn nên thay đổi các nội dung dới đây để tạo độ nhạy cảm cho quét này:

1. Lựa và tùy biến (Customize) Network Engine Policy.
2. Tìm "Port Scan" và lựa tùy chọn Options.
3. Thay đổi ports thành 5 cổng.
4. Thay đổi Delta thành 60 giây.

Nếu đang dùng Firewall-l với UNIX, bạn có thể dùng trình tiện ích của Lance Spitzner để phát hiện các đợt quét cổng Firewall-1 www.enteract.com/~lspitz/intrusion.html <http://www.enteract.com/~lspitz/intrusion.html>. Ký mã alert.sh của ông sẽ cấu hình Check point để phát hiện và giám sát các đợt quét cổng và chạy một User Defined Alert khi đợc ứng tác.

Phòng Chống

Để ngăn cản các đợt quét cổng bức tờng lửa từ Internet, bạn cần phong tỏa các cổng này trên các bộ định tuyến đứng trớc các bức tờng lửa. Nếu các thiết bị này do ISP quản lý, bạn cần liên hệ với họ để tiến hành phong tỏa. Nếu tự bạn quản lý chúng, bạn có thể dùng các Cisco ACL dới đây để phong tỏa rõ rệt các đợt quét đã nêu trên đây:

```
access - list 101 deny tcp any any eq 256 log ! Block Firewall-l scans
access - list 101 deny tcp any any eq 257 log ! Block Firewall-l scans
access - list 101 deny tcp any any eq 258 log ! Block Firewall-l scans
access - list 101 deny tcp any any eq 1080 log ! Block Socks scans
access - list 101 deny tcp any any eq 1745 log ! Block Winsock scans
```

Ghi chú : Nếu phong tỏa các cổng của Check Point (256-258) tại các bộ dịnh tuyến biên, bạn sẽ không thể quản lửa bừc tường lửa từ lnternet.

Ngoài ra, tất cả các bộ định tuyến phải có một quy tắc dọn dẹp (nếu không khớc từ các gói tìn theo ngầm định), sẽ có cùng hiệu ứng nh khi chỉ định các tác vụ khớc từ:

```
access - list 101 deny ip any any log ! Deny and log any packet that got through our ACLs above
```

2. Rà Tuyến Đờng

Một cách thinh lặng và tinh tế hơn để tìm các bức tờng lửa trên một mạng đó là dùng traceroute . Bạn có thể dùng traceroute của UNIX hoặc tracert.exe của NT để tìm từng chặng dọc trên trên đờng truyền đến đích và tiến hành suy diễn. Traceroute của Linux có tùy chọn -I, thực hiện rà đờng bằng cách gửi các gói tin ICMP, trái với kỹ thuật gói tin UDP ngầm định.

[sm@atsunami sm] $ traceroute - I www.yourcompany.com

traceroute to www.yourcompany.com (172.17.100.2) , 30 hops max, 140 byte packets

1 attack-gw (192.168.50.21) 5.801 ms 5.105 ms 5.445 ms

2 gw1.smallisp.net (192.168.51.l)

3 gw2.smallisp.net (192.168.52.2)

.....

13 hssi.bigisp.net (10.55.201.2)

14 seriall.bigisp.net (10.55.202.l)

15 www.yourcompany.com (172.29.11.2)

Có cơ may chặng đứng ngay trớc đích (10.55.202.1) là bức tờng lửa, nhng ta cha biết chắc. Cần phải đào sâu thêm một chút.

Ví dụ trên đây là tuyệt vời nếu các bộ định tuyến giữa bạn và các hệ phục vụ đích đáp ứng các gói tin có TTL hết hạn. Nhng một số bộ định tuyến và bức tờng lửa đợc xác lập để không trả về các gói tin ICMP có TTL hết hạn (từ các

gói tin ICMP lẫn UDP). Trong trờng hợp này, sự suy diễn ít khoa học hơn. Tất cả những gì bạn có thể thực hiện đó là chạy traceroute và xem chặng nào đáp ứng cuối cùng, và suy ra đây là một bức tờng lửa hoặc chí ít là bộ định tuyến đầu tiên trong đờng truyền bắt đầu phong tỏa tính năng tracerouting. Ví dụ, ở đây ICMP đang bị phong tỏa đến đích của nó, và không có đáp ứng nào từ các bộ định tuyến vợt quá client - gw.smallisp.net :

```
1   stoneface (192.168.10.33) 12.640 ms 8.367 ms
2   gw1.localisp.net (172.31.10.1) 214.582 ms 197.992 ms
3   gw2.localisp.net (172.31.10.2) 206.627 ms 38.931 ms
4   dsl.localisp.net (172.31.12.254) 47.167 ms 52.640 ms
.....
14 ATM6.LAX2.BIGISP.NET (10.50.2.1) 250.030 ms 391.716 ms
15 ATM7.SDG.BIGISP.NET (10.50.2.5) 234.668 ms 384.525 ms
16 client-gw.smallisp.net (10.50.3.250) 244.065 ms ! X * *
17 * * *
18 * * *
```

Các Biện Pháp Phòng Chống

Việc chỉnh sửa sự rò rỉ thông tin traceroute đó là hạn chế tối đa các bức tờng lửa và bộ định tuyến đáp ứng các gói tin có TTL hết hạn. Tuy nhiên, điều này không phải lúc nào cũng nằm dới sự kiểm soát của bạn vì nhiều bộ định tuyến

có thể nằm dới s điều khiển cúa ISP.

Phát Hiện

Để phát hiện các traceroute chuẩn trên biên, bạn cần giám sát các gói tin UDP và ICMP có giá trị TTL là 1. Để thực hiện điều này với RealSecure 3.0, bạn bảo đảm đánh dấu TRACE_ROUTE decode name trong Security Events của Network Engine Policy.

Phòng chống

Để ngăn cản các traceroute chạy trên biên, bạn có thể cấu hình các bộ định tuyến không đáp ứng các th ông điệp TTL EXPIRED khi nó nhận một gói tin có TTL là 0 hoặc 1. ACL dới đây sẽ làm việc với các bộ định tuyến Cisco:
access - list 101 deny ip any any 11 0 ! ttl-exceeded
Hoặc theo lý tởng, bạn nên phong tỏa toàn bộ luồng lu thông UDP không cần thiết tại các bộ định tuyến biên.

3. Nắm Giữ Biểu Ngữ

Kỹ thuật quét tìm các cổng bức tờng lừa là hữu ích trong việc định vị các bức tờng lửa, nhng hầu hết các bức tờng lửa không lắng chờ trên các cổng ngầm định nh Check point và Microsoft, do đó việc phát hiện phải đợc suy diễn. Nhiều bức tờng lứa phổ dụng sẽ công bố sự hiện diện của chúng bằng cách đơn giản nối với chúng. Ví dụ , nhiều bức tờng lửa giám quản sẽ công bố chức năng cúa chúng với t cách một bức tờng lửa, và một số sẽ quảng cáo kiểu và phiên bản của chúng. Ví dụ, khi ta nối với một máy đợc tin là một bức tờng lửa bằng netcat trên cổng 21 (FTP), ta sẽ thấy một số thông tin thú vị :

```
C:\TEMP>nc -v -n 192.168.51.129  2 l
[UNKNOWN] [ 192.168.5l.129 ] 2 l ( ? ) open
220 Secure Gateway FTP server ready .
```

Biểu ngữ "Secure Gateway server FTP ready" là một dấu hiệu lộ tẩy của một hộp Eagle Raptor cũ. Việc nối thêm với cổng 23 (telnet) sẽ xác nhận tên bức tờng lửa là "Eagle."

```
C:\TEMP>nc -v -n 192.168.51.129  23
[UNKNOWN] [ 192.168.5l.129 ] 23 ( ? ) open
Eagle Secure Gateway . Hostname :
```

Và cuối cùng. nếu vẫn cha bị thuyết phục hệ chủ của bạn là một bức tờng lửa. bạn có thể netcat với cổng 25 (SMTP), và nó sê báo cho ban biết nó là gì:

```
C:\TEMP>nc -v -n 192.168.51.129 25
```

[UNKNOWN] [192.168.5l.129] 25 (?) open
421 fw3.acme.com Sorry, the firewall does not provide mail service to you.

Nh đã thấy trong các ví dụ trên đây, thông tin biểu ngữ có thể cung cấp các thông tin quý giá cho bọn tấn công trong khi định danh các bức tờng lửa. Dùng thông tin này, chúng có thể khai thác các chỗ yếu phổ biến hoặc các cấu hình sai chung.

Biện Pháp Phòng Chống

Để chỉnh sửa chỗ yếu rò rỉ thông tin này, bạn giới hạn thông tin biểu ngữ quảng cáo. Một biểuu ngữ tốt có thể kèm theo một mục cảnh giác mang tính pháp lý và tất cả mọi nỗ lực giao kết sẽ đợc ghi sổ. Các chi tiết thay đổi cụ thể của các biểu ngữ ngầm định sẽ tùy thuộc nhiều vào bức tờng lửa cụ thể, do đó bạn cần liên hệ hãng kinh doanh bức tờng lửa.

Phòng Chống

Để ngăn cản bọn tấn công giành đợc quá nhiều thông tin về các bức tờng lửa từ các biểu ngữ quảng cáo, bạn có thể thay đổi các tập tin cấu hình biểu ngữ. Các khuyến nghị cụ thể thờng tùy thuộc vào hã ng kinh doanh bức tờng lửa.

Trên các bức tờng lửa Eagle Raptor, bạn có thể thay đổi các biểu ngữ ftp và telnet bằng cách sửa đổi các tập tin thông báo trong ngày: tập tin ftp.motd và telnet.motd.

4. Kỹ Thuật Phát Hiện Bức Tờng Lửa Cao Cấp

Nếu tiến trình quét cổng tìm các bức tờng lửa trực tiếp, dò theo đờng truyền, và nắm giữ biểu ngữ kh ông mang lại hiệu quả, bọn tấn công sẽ áp dụng kỹ thuật điểm danh bức tờng lửa theo cấp kế tiếp. Có thể suy diễn các bức tờng lửa và các quy tắc ACL của chúng bằng cách dò tìm các đích và lu ý các lộ trình phải theo (hoặc không theo) để đến đó.

Suy Diễn Đơn Giản với nmap

Nmap là một công cụ tuyệt vời để phát hiện thông tin bức tờng lửa và chúng tôi liên tục dùng nó. Khi nmap quét một hệ chủ, nó không chỉ báo cho bạn biết các cổng nào đang mở hoặc đóng, mà còn cho biết các cổng nào đang bị phong tỏa. Lợng (hoặc thiếu) thông tin nhận đợc từ một đợt quét cổng có thể cho biết khá nhiều về cấu hình của bức tờng lửa.
Một cổng đã lọc trong nmap biểu hiện cho một trong ba nội dung sau:

- Không nhận gói tin SYN/ACK nào.

- Không nhận gói tin RST/ACK nào.
- Đã nhận một thông báo ICMP type 3 (Destination Unreachable) có một mã 13 (Communication Administratively Prohibited - [RFC1812]).

Nmap gom chung cả ba điều kiện này và báo cáo nó dới dạng một cổng "đã lọc." Ví dụ, khi quét www.mycompany.com <http://www.mycompany.com>, ta nhận hai gói tin ICMP cho biết bức tờng lửa đã phong tỏa các cổng 23 và 111 từ hệ thống cụ thể của chúng ta.

```
[ root@bldg_043 /opt ] # nmap -p20, 21, 23,  53, 80, 111 - P0 -vv
www.mycompany.com
Starting nmap V. 2.08 by Fyodor ( fyodor@dhp.com <mailto:fyodor@dhp.com>, www.insecure.org/nmap/ )
Initiating TCP connect ( ) scan agains t ( 172.32.12.4 )
Adding TCP port 53 (state Open)
Adding TCP port 111 ( state Firewalled )
Adding TCP port 80 ( state Open)
Adding TCP port 23 ( state Firewalled) .
Interesting ports on ( 172.17.12.4 ) :
port            State           Protocol            Service
23              filtered        tcp                 telnet
```

53	open	tcp	domain
80	open	tcp	http
111	filtered	tcp	sunrpc

Trạng thái "Firewalled", trong kết xuất trên đây, là kết quả của việc nhận một ICMP type 3, mã 13 (Admin Prohibited Filter), nh đã gặp trong kết xuất tcpdump:

23 : 14 : 01.229743 10.55.2.1 > 172.29.11.207 : icmp : host 172.32.12.4
nreachable - admin prohibited filter
23 : 14 : 01.97 9743 10.55.2.l > 172.29.11.207 : icmp : host 172.32.12.4
nreachable - admin prohibited filter

Làm sao để nmap kết hợp các gói tin này với các gói tin ban đầu, nhất là khi chúng chỉ là một vài trong biển cả các gói tin đang ríu rít trên mạng? Vâng, gói tin ICMP đợc gửi trở lại cho máy quét sẽ chứa đựng tất cả các dữ liệu cần
thiết để tìm hiểu nội dung đang xảy ra. Cổng đang bị phong tỏa là phần một byte trong phần đầu ICMP tại byte 0x41 (1 byte), và bức tờng lửa lọc gửi thông điệp sẽ nằm trong phần IP của gói tin tại byte 0x1b (4 byte).

Cuối cùng, một cổng “cha lọc” nmap chỉ xuất hiện khi bạn quét một số cổng và nhận trở lại một gói tin RST/ACK. Trong trạng thái "unfiltered", đợt quét của chúng ta hoặc đang đi qua bức tờng lửa và hệ đích của chúng ta đang báo cho biết nó không lắng chờ trên cổng đó, hoặc bức tờng lửa đang đáp ứng

đích và đánh lừa địa chỉ IP của nó với cờ RST/ACK đợc ấn định. Ví dụ, đợt quét một hệ thống cục bộ cho ta hai cổng cha lọc khi nó nhận hai gói tin RST/ACK từ cùng hệ chủ. Sự kiện này cũng có thể xảy ra với một số bức tờng lửa nh Check point (với quy tắc REJECT) khi nó đáp ứng đích đang gửi trả một gói tin RST/ACK và đánh lừa địa chỉ IP nguồn của đích. .

[root@bldg_043 sniffers] # nmap - sS -p1 -300 172.18.20.55

Starting nmap V . 2.08 by Fyodor (fyodor@dhp.com <mailto:fyodor@dhp.com>, www.insecure.org/nmap/)

Interesting ports on (172.18.20.55) :

(Not showing ports in state : filtered)

Port	State	Protocol	Service
7	unfiltered	tcp	echo
53	unfilteres	tcp	domain
256	open	tcp	rap
257	open	tcp	set
258	open	tcp	yak-chat

Nmap run completed - 1 IP address (1 host up) scanned in 15 seconds

Đợt rà gói tin tcpdump kết hợp nêu các gói tin RST/ACK đã nhận.

21 :26 :22.742482 172.18.20.55.258 > 172.29.11.207.39667 : S

415920470 : 1415920470 (0) ack 3963453111 win 9112 <mss 536> (DF)

(ttl 254, id 50438)

21 :26 :23.282482 172.18.20.55.53 > 172.29.11.207.39667 :

R 0 : 0 (0) ack 3963453111 win 0 (DF) (ttl 44, id 50439)

21 :2 6: 24.362482 172.18.20.55.257 > 172.29.111.207.39667 : S

1416174328 : 1416174328 (0) ack 396345311 win X112

<mss 5 3 6 >

(DF) (ttl 254, id 504 0)

21: 26: 26.282482 172.18.20.55.7 > 17.2.29.11.207.39667 :

R 0 : 0 (0) ack 3963453111 win 0 (DF) (ttl 44, id 50441)

Các Biện Pháp Phòng Chống

Phòng Chống

Để ngăn cản bọn tấn công điểm danh các ACL bộ định tuyến và bức tòng lửa thông qua kỹ thuật "admin prohibited filter", bạn có thể vô hiệu hóa khả năng đáp ứng với gói tin ICMP type 13 của bộ định tuyến. Trên Cisco, bạn có thể thực hiện điều này bàng cách phong tỏa thiết bị đáp ứng các thông điệp IP không thể đụng đến

```
no ip unreachables
```

5. Định Danh Cổng

Một số bức tòng lửa có một dấu ấn duy nhất xuất hiện dới dạng một sêri con số phân biệt với các bức t-òng lửa khác. Ví dụ, Check Point sẽ hiển thì một sêri các con số khi bạn nối với cổng quản lý SNMP của chúng, TCP 257. Tuy sự hiện diện đơn thuần của các cổng 256-259 trên một hệ thống thòng cũng đủ là một dấu chỉ báo về sự hiện diện của Firewall-1 của Check Point song trắc nghiệm sau đây sẽ xác nhận nó :

```
[ root@bldg_043 # nc -v -n 192.168.51.1  257
( UNKNOWN) [ 192.168.51.1] 257 ( ? ) open
30000003
```

```
[ root@bldg_043 # nc -v -n 172.29.11.19l  257
(UNKNOWN ) [ 172.29.11.191] 257 ( ? ) open
31000000
```

Các Biện Pháp Phòng Chống

Phát Hiện

Để phát hiện tuyến nối của một kẻ tấn công với các cổng của bạn. bạn bố sung một sự kiện tuyến nối trong RealSecure. Theo các bớc sau:

1. Hiệu chỉnh nội quy
2. Lựa tab Connection Events.
3. Lựa nut Add Connection, và điền một mục cho Check Point.
4. Lựa đích kéo xuống và lựa nút Add.
5. Điền dịch vụ và cổng, nhắp OK.
6. Lựa cổng mới, và nhắp lại OK.
7. Giờ đây lựa OK và áp dụng lại nội quy cho động cơ.

Phòng Chống

Để ngăn cản các tuyến nối với cổng TCP 257, bạn phong tỏa chúng tại các bộ định tuyến thợng nguồn. Một Cisco ACL đơn giản nh dới đây có thể khớc từ rõ rệt một nỗ lực của bọn tấn công:

```
access -list 101 deny tcp any any eq 257 log ! Block Firewall- l scans
```

III. Quét qua các bức tờng lửa

Đừng lo, đoạn này không có ý cung cấp cho bọn nhóc ký mã một số kỹ thuật ma thuật để vô hiệu hóa các bức tờng lửa. Thay vì thế, ta sẽ tìm hiểu một số kỹ thuật để nhảy múa quanh các bức tờng lửa và thu thập một số thông tin quan trọng về các lộ trình khác nhau xuyên qua và vòng quanh chúng.

1. hping

hping (www.Genocide2600.com/-tattooman/scanners/hping066.tgz), của Salvatore Sanfilippo, làm việc bằng cách gửi các gói tin TCP đến một cổng đích và báo cáo các gói tin mà nó nhận trở lại. hping trả về nhiều đáp ứng khác nhau tùy theo vô số điều kiện. Mỗi gói tin từng phần và toàn thể có thể cung cấp một bức tranh khá rõ về các kiểu kiểm soát truy cập của bức tờng lửa. Ví dụ, khi dùng hping ta có thể phát hlện các gói tin mở, bị phong tỏa, thả, và loại bỏ.

Trong ví dụ sau đây, hping báo cáo cổng 80 đang mở và sẵn sàng nhận một tuyến nối. Ta biết điều này bởi nó đã nhận một gói tin với cờ SA đợc ấn định (một gói tin SYN/ACK).

```
[ root@bldg_043 / opt ] # hping www.yourcompany.com -c2 - S
-p80 -n HPING www.yourcomapany.com ( eth0 172.30.1.2 0 ) : S
set, 40 data bytes 60 bytes from 172.30.1.20 : flags=SA
seq=0 ttl=242 id= 65121 win= 64240 time=144.4 ms
```

Giờ đây ta biết có một cổng mở thông đến đích, nhng cha biết nơi của bức tờng lửa. Trong ví dụ kế tiếp, hping báo cáo nhận một ICMP unreachable type 13 từ 192.168.70.2. Một ICMP type 13 là một gói tin lọc bị ICMP admin ngăn cấm, thờng đợc gửi từ một bộ định tuyến lọc gói tin.

```
[root@bldg_043 /opt ] # hping www.yourcompany.com -c2 -S
-p23 -n HPING www.yourcompany.com ( eth0 172.30.1.20 ) : S
set, 40 data bytes ICMP Unreachable type 13 f rom
192.168.70.2
```

Giờ đây nó đợc xác nhận, 192.168.70.2 ắt hẳn là bức tờng lửa, và ta biết nó đang rõ rệt phong tỏa cổng 23 đến đích của chúng ta. Nói cách khác, nếu hệ thống là một bộ định tuyến Cisco nó ắt có một dòng nh dới đây trong tập tin config:

```
access -list 101 deny tcp any any 23 ! telnet
```

Trong ví dụ kế tiếp, ta nhận đợc một gói tin RST/ACK trả lại báo hiệu một trong hai viêc: (1) gói tin

lọt qua bức tờng lửa và hệ chủ không lắng chờ cổng có , hoặc (2) bức tờng lửa thải bỏ gói tin (nh trờng hợp của quy tắc reject của Check Point).

```
[ root@bldg_043 /opt ] # hping 192.168.50.3 -c2 -S -p22 -n
HPING 192.168.50.3 ( eth0 192.168.50.3 ) : S set, 40 data
bytes 60 bytes from 192.168.50.3 : flags=RA seq= 0 ttl= 59
id= 0 win= 0 time=0.3 ms
```

Do đã nhận gói tin ICMP type 13 trên đây, nên ta có thể suy ra bức tờng lửa (192.168.70.2) đang cho phép gói tin đi qua bức tờng lửa, nhng hệ chủ không lắng chờ trên cổng đó.

Nếu bức tờng lửa mà bạn đang quét qua là Check point, hping sẽ báo cáo địa chỉ IP nguồn của đích, nhng gói tin thực sự đang đợc gửi từ NIC bên ngoài của bức tờng lửa Check Point. Điểm rắc rối về Check Point đó là nó sẽ đáp ứng các hệ thống bên trong của nó , gửi một đáp ứng và lừa bịp địa chỉ của đích. Tuy nhiên, khi bọn tấn công đụng một trong các điều kiện này trên Internet, chúng không hề biết sự khác biệt bởi địa chỉ MAC sẽ không bao giờ chạm máy của chúng.

Cuối cùng, khi một bức tờng lửa đang phong toả các gói tin đến một cổng, bạn thờng không nhận đợc gì trở lại.

```
[ root@bldg_04 3 /opt ] # hping 192.168.50.3 -c2 -S -p2 2 -n
HPING 192.168.50.3 ( eth0 192.168.50.3 ) : S set, 40 data
```

Kỹ thuật hping này có thể có hai ý nghĩa: (1) gói tin không thể đạt đến đích và đã bị mất trên đ-

ờng truyền, hoặc (2) có nhiều khả năng hơn, một thiết bị (ắt là bức tờng lửa của chúng ta 192.168.70.2) đã bỏ gói tin trên sàn dới dạng một phần các quy tắc ACL của nó.

Biện Pháp Phòng Chống

Phòng Chống

Ngăn ngừa một cuộc tấn công hping không phải là dễ . Tốt nhất, ta chỉ việc phong tỏa các thông điệp ICMP type 13 (nh mô tả trong đoạn phòng chống tiến trình quét nmap trên đây).

2. Cầu Lửa

Firewalk (http://www.packetfactory.net/firewalk/) là một công cụ nhỏ tiện dụng, nh một bộ quét cổng, đợc dùng để phát hiện các cổng mở đàng sau một bức tờng lửa. Đợc viết bởi Mike Schiffnlan, còn gọi là Route và Dave Goldsmith, trình tiện ích này sẽ quét một hệ chủ xuôi dòng từ một bức tờng lửa và báo cáo trở lại các quy tắc đợc phép đến hệ chủ đó mà không phải thực tế chạm đến hệ đích.

Firewalk làm việc bằng cách kiến tạo các gói tin với một IP TTL đợc tính toán để kết thúc một chãng vợt quá bức tờng lửa. Về lý thuyết, nếu gói tin đợc bức tờng lửa cho phép, nó sẽ đợc phép đi qua và sẽ kết thúc nh dự kiến, suy ra một thông điệp "ICMP TTL expired in transit." Mặt khác, nếu gói tin

bị ACL của bức tờng lửa phong tỏa, nó sẽ bị thả, và hoặc không có đáp ứng nào sẽ đợc gửi, hoặc một gói tin lọc bị ICMP type 13 admin ngăn cấm sẽ đợc gửi.

```
[ root@exposed / root ] # firewalk -pTCP -S135 -140  10.22.3.1
192.168.1.1
Ramping up hopcounts to binding host . . .
probe : 1 TTL : 1 port 33434 : expired from [exposed.acme.com]
probe : 2 TTL : 2 port 33434 : expired from [rtr.isp.net]
probe : 3 TTL : 3 port 33434 : Bound scan at 3 hops [rtr.isp.net]
port open
port 136 : open
port 137 : open
port 138 : open
port 139 : *
port 140 : open
```

Sự cố duy nhất mà chúng tôi gặp khi dùng Firewalk đó là nó có thể ít hơn dự đoán, vì một số bức tờng lửa sẽ phát hiện gói tin hết hạn trớc khi kiểm tra các ACL của nó và cứ thế gửi trả một gói tin ICMP TTL EXPIRED. Kết quả là, Firewalk mặc nhận tất cả các cổng đều mở.

Biện Pháp Phòng Chống

Phòng Chống

Bạn có thể phong tỏa các gói tin ICMP TTL EXPIRED tại cấp giao diện bên ngoài, nhng điều này có thể tác động tiêu cực đến khả năng vận hành của nó, vì các hệ khách hợp pháp đang nối sẽ kh ông bao giờ biết điều gì đã xảy ra với tuyến nối của chúng.

IV. Lọc gói tin

Các bức tờng lửa lọc gói tin nh Firewall-1 của Check Point, Cisco PIX, và IOS của Cisco (vâng, Cisco IOS có thể đợc xác lập dới dạng một bức tờng lửa) tùy thuộc vào các ACL (danh sách kiểm soát truy cập) hoặc các quy tắc để xác định xem luồng lu thông có đợc cấp quyền để truyền vào/ra mạng bên trong. Đa phần, các ACL này đợc sắp đặt kỹ và khó khắc phục. Nhng thông thờng, bạn tình cờ gặp một bức tờng lửa có các ACL tự do, cho phép vài gói tin đi qua ở tình trạng mở. .

Các ACL Tự Do

Các danh sách kiểm soát truy cập (ACL) tự do thờng gặp trên các bức tờng lửa nhiều hơn ta t-

ởng. Hãy xét trờng hợp ở đó có thể một tổ chức phải cho phép ISP thực hiện các đợt chuyển giao miền. Một ACL tự do nh "Cho phép tất cả mọi hoạt động từ cổng nguồn 53" có thể đợc sử dụng thay vì “cho phép hoạt động từ hệ phục vụ DNS của ISP với cổng nguồn 53 và cổng đích 53." Nguy cơ tồn tại các cấu hình sai này có thể gây tàn phá thực sự, cho phép một hắc cơ quét nguyên cả mạng từ bên ngoài. Hầu hết các cuộc tấn công này đều bắt đầu bằng một kẻ tấn công tiến hành quét một hệ chủ đằng sau bức tờng lửa và đánh lừa nguồn của nó dới dạng cổng 53 (DNS).

Biện Pháp Phòng Chống

Phòng Chống

Bảo đảm các quy tắc bức tờng lửa giới hạn ai có thể nối ở đâu. Ví dụ, nếu ISP yêu cầu khả năng chuyển giao miền, thì bạn phải rõ ràng về các quy tắc của mình. Hãy yêu cầu một địa chỉ IP nguồn và mã hóa cứng địa chỉ IP đích (hệ phục vụ DNS bên trong của bạn) theo quy tắc mà bạn nghĩ ra.

Nếu đang dùng một bức tờng lửa Checkpoint, bạn có thể dùng quy tắc sau đây để hạn chế một cổng nguồn 53 (DNS) chỉ đến DNS của ISP. Ví dụ, nếu DNS của ISP là 192.168.66.2 và DNS bên trong của bạn là 172.30.140.1, bạn có thể dùng quy tắc dới đây:

Nguồn gốc	Đích	Dịch vụ	Hành động	Dấu vết

192.168.66.2	172.30. 140.1	domain-tcp	Accept	Short

V. Phân Luồng ICMP và UDP

Phân lạch (tunneling) ICMP là khả năng đóng khung dữ liệu thực trong một phần đầu ICMP. Nhiều bộ định tuyến và bức tờng lửa cho phép ICMP ECHO, ICMP ECHO REPLY, và các gói tin UDP mù quáng đi qua, và nh vậy sẽ dễ bị tổn thơng trớc kiểu tấn công này. Cũng nh chỗ yếu Checkpoint DNS, cuộc tấn công phân lạch ICMP và UDP dựa trên một hệ thống đã bị xâm phạm đằng sau bức t-ờng lửa.

Jeremy Rauch và Mike D. Shiffman áp dụng khái niệm phân lạch vào thực tế và đã tạo các công cụ để khai thác nó : loki và lokid (hệ khách và hệ phục vụ) -xem <http://www.phrack.com/search.phtml?view&article=p49-6> . Nếu chạy công cụ hệ phục vụ lokid trên một hệ thống đằng sau bức tờng lửaa cho phép ICMP ECHO và ECHO REPLY, bạn cho phép bọn tấn công chạy công cụ hệ khách (loki), đóng khung mọi lệnh gửi đi trong các gói tin ICMP ECHO đến hệ phục vụ (lokid). Công cụ lokid sẽ tháo các lệnh, chạy các lệnh cục bộ , và đóng khung kết xuất của các lệnh trong các gói tin ICMP ECHO REPLY trả lại cho bọn tấn công. Dùng kỹ thuật này, bọn tấn công có thể hoàn toàn bỏ qua bức tờng lửa.

Phòng Chống

Để ngăn cản kiểu tấn công này, bạn vô hiệu hóa khả năng truy cập ICMP thông qua bức tờng lửa hoặc cung cấp khả năng truy cập kiểm soát chi tiết trên luồng lu thông ICMP. Ví dụ, Cisco ACL dới đây sẽ vô hiệu hóa toàn bộ luồng lu thông ICMP phía ngoài mạng con 172.29.10.0 (DMZ) vì các mục tiêu điều hành:

```
access - list 101 permit  icmp any 172.29.10.0
        0.255.255.255  8 ! echo
access - list 101 permit  icmp any 172.29.10.0
        0.255.255.255  0 !
echo- reply
access - list 102 deny ip any any log ! deny and log
        all else
```

Cảnh giác: nếu ISP theo dõi thời gian hoạt động của hệ thống bạn đằng sau bức tờng lửa của bạn với các ping ICMP (hoàn toàn không nên!), thì các ACL này sẽ phá vỡ chức năng trọng yếu của chúng. Hãy liên hệ với ISP để khám phá xem họ có dùng các ping ICMP để kiểm chứng trên các hệ thống của

bạn hay không.

Tóm Tắt

Trong thực tế một bức tờng lửa đợc cấu hình kỹ có thể vô cùng khó vợt qua. Nhng dùng các c ông cụ thu thập thông tin nh traceroute, hping, và nmap, bọn tấn công có thể phát hiện (hoặc chí ít suy ra) các lộ trình truy cập thông qua bộ định tuyến và bức tờng lửa cũng nh kiểu bức tờng lửa mà bạn đang dùng. Nhiều chỗ yếu hiện hành là do cấu hình sai trong bức tờng lửa hoặc thiếu sự giám sát eấp điều hành, nhng dẫu thế nào, kết quả có thể dẫn đến một cuộc tấn công đại họa nếu đợc khai thác.
Một số điểm yếu cụ thể tồn tại trong các hệ giám quản lẫn các bức tờng lửa lọc gói tin, bao gồm các kiểu đăng nhập web, telnet, và localhost không thẩm định quyền. Đa phần, có thể áp dụng các biện pháp phòng chống cụ thể để ngăn
cấm khai thác chỗ yếu này, và trong vài trờng hợp chỉ có thể dúng kỹ thuật phát hiện.
Nhiều ngời tin rằng tơng lại tất yếu của các bức tờng lửa sẽ là một dạng lai ghép giữa ứng dụng giám quản và công nghệ lọc gói tin hữu trạng [stateful] sẽ cung cấp vài kỹ thuật để hạn chế khả năng cấu hình sai. Các tính năng phản ứng cũng sẽ là một phần của bức tờng lửa thế hệ kế tiếp. NAI đã thực thi một dạng nh vậy với kiến trúc Active Security. Nhờ đó, ngay khi phát hiện cuộc xâm phạm, các thay đổi đã đợc thiết kế sẵn sẽ tự động khởi phát và áp dụng cho bức tờng lửa bị ảnh hởng. Ví dụ, nếu một IDS có thể phát hiện tiến trình phân lạch ICMP, sản phẩm có thể hớng bức tờng lửa đóng các yêu cầu ICMP ECHO vào trong bức tờng lửa. Bối cảnh nh vậy luôn là cơ hội cho một cuộc tấn công khớc từ

dịch vụ; đó là lý do tại sao luôn cần có mặt các nhân viên bảo mật kinh nghiệm.