Cisco 라우터를 사용한 패킷 플러드 특성 및 추적

목차

소개

DoS(서비스 거부) 공격은 인터넷에서 흔히 발생합니다.이러한 공격에 대응할 때 사용하는 첫 번째 단계는 정확히 어떤 종류의 공격인지 파악하는 것입니다.일반적으로 사용되는 대부분의 DoS 공격은 고대역폭 패킷 플러드 또는 기타 반복적인 패킷 스트림을 기반으로 합니다.

많은 DoS 공격 스트림의 패킷은 Cisco IOS® 소프트웨어 액세스 목록 항목과 일치시킬 때 격리될 수 있습니다.이는 공격을 필터링하는 데 유용합니다.또한 알 수 없는 공격의 특성을 지정할 때, 그리고 "스푸핑된" 패킷을 추적할 때 실제 소스로 다시 스트림할 때도 유용합니다.

디버그 로깅 및 IP 어카운팅과 같은 Cisco 라우터 기능은 유사한 용도로 사용될 수 있습니다. 특히 신규 또는 비정상적인 공격에서도 마찬가지입니다.그러나 최신 버전의 Cisco IOS 소프트웨어에서는 액세스 목록 및 액세스 목록 로깅이 일반적인 공격의 특성을 파악하고 추적할 때 사용되는 기본 기능입니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

가장 일반적인 DoS 공격

다양한 DoS 공격이 가능합니다.소프트웨어 버그를 사용하여 상대적으로 트래픽이 적은 시스템을 종료하는 공격을 무시해도, 네트워크를 통해 전송할 수 있는 모든 IP 패킷을 사용하여 플러딩 DoS 공격을 실행할 수 있다는 사실은 그대로 유지됩니다.공격을 받을 때는 항상 일반적인 카테고리에 속하지 않는 것이 보이는 것일 가능성을 고려해야 합니다.

그러나 이러한 주의 사항에 따라 많은 공격이 비슷하다는 점을 기억하면 좋습니다.공격자는 특히 효과적이고, 특히 추적하기가 어렵거나, 툴을 사용할 수 있기 때문에 일반적인 익스플로잇을 선택합니다.많은 DoS 공격자들은 자체 툴을 개발하고 인터넷에 있는 프로그램을 사용할 수 있는 기술이나 동기가 부족합니다.이 도구들은 유행에 뒤떨어지는 경향이 있다.

1999년 7월, 이 글을 쓸 당시 대부분의 고객 Cisco 지원 요청은 "smurf" 공격입니다.이 공격에는 두 명의 피해자가 있습니다."궁극적인 목표"와 "리플렉터"입니다. 공격자는 리플렉터 서브넷의 브로드캐스트 주소로 ICMP 에코 요청("ping")의 자극적인 스트림을 전송합니다.이러한 패킷의 소스 주소는 최종 대상의 주소로 위조됩니다.공격자가 전송하는 각 패킷에 대해 리플렉터 서브넷의 많은 호스트가 응답합니다.이는 최종 목표를 초과 달성하고 두 피해자 모두의 대역폭을 낭비합니다.

"fraggle"이라고 하는 유사한 공격은 동일한 방식으로 지정 브로드캐스트를 사용하지만 ICMP(Internet Control Message Protocol) 에코 요청 대신 UDP 에코 요청을 사용합니다.Fraggle은 보통 스머프보다 더 작은 증폭 요인을 얻으며 훨씬 덜 인기 있습니다.

보통 네트워크 링크가 오버로드되기 때문에 스머프 공격이 발생합니다.이러한 공격 및 방어 조치에 대한 전체 설명은 Denial of Service Attacks Information 페이지에 있습니다 .

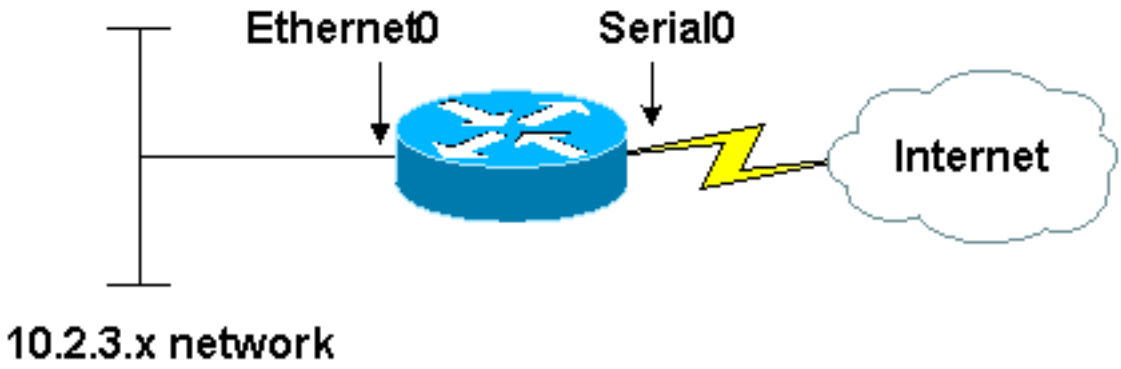
또 다른 일반적인 공격은 SYN 플러드이며, 대상 시스템에 TCP 연결 요청이 플러딩됩니다.연결 요청 패킷의 소스 주소 및 소스 TCP 포트는 임의로 지정됩니다.목표는 완료되지 않은 많은 연결에 대해 대상 호스트가 상태 정보를 유지하도록 하는 것입니다.

SYN 플러드 공격은 일반적으로 대상 호스트(HTTP 또는 SMTP 서버 자주)가 매우 느리거나 충돌 또는 중단되기 때문에 발생합니다.또한 대상 호스트에서 반환되는 트래픽이 라우터에서 문제를 일으킬 수도 있습니다.이는 이 반환 트래픽이 원래 패킷의 임의 소스 주소로 이동하고, "실제" IP 트래픽의 지역 속성이 없으며, 경로 캐시를 오버플로할 수 있기 때문입니다.Cisco 라우터에서 이 문제는 메모리가 부족한 라우터에서 발생하는 경우가 많습니다.

Cisco에 보고된 대부분의 DoS 공격은 함께 스머프와 SYN 플러드 공격을 통해 이루어지며 이를 신속하게 파악하는 것이 매우 중요합니다.Cisco 액세스 목록을 사용할 경우 공격(ping flood와 같은 일부 "보조 계층" 공격 모두 쉽게 인식됩니다.

A DoS 특성 평가 액세스 목록

두 개의 인터페이스가 있는 라우터를 보여줍니다.이더넷 0은 비즈니스 또는 소규모 ISP에서 내부 LAN에 연결됩니다.직렬 0은 업스트림 ISP를 통해 인터넷 연결을 제공합니다.직렬 0의 입력 패킷 속도는 전체 링크 대역폭에서 "페깅됨"이며, LAN의 호스트는 느리게 실행, 충돌, 중단 또는 DoS 공격의 다른 징후를 표시합니다.라우터가 연결되는 소규모 사이트에는 네트워크 분석기가 없으며, 추적 항목이 사용 가능하더라도 분석기 추적을 읽는 경험이 거의 없거나 전혀 없습니다.



이제 다음 출력에 표시된 대로 액세스 목록을 적용한다고 가정합니다.

```
access-list 169 permit icmp any any echo
access-list 169 permit icmp any any echo-reply
access-list 169 permit udp any any eq echo
access-list 169 permit udp any eq echo any
access-list 169 permit tcp any any established
access-list 169 permit tcp any any
access-list 169 permit ip any any

interface serial 0
ip access-group 169 in
```

이 목록은 트래픽을 전혀 필터링하지 않습니다.모든 항목은 허용됩니다.그러나 유용한 방법으로 패킷을 분류하므로 이 목록을 사용하여 세 가지 공격 유형을 모두 미정으로 진단할 수 있습니다 .smurf, SYN 플러드 및 fraggle.

스머프 얼티밋 타겟

show access-list 명령을 실행하면 다음과 유사한 출력이 표시됩니다.

```
Extended IP access list 169
    permit icmp any any echo (2 matches)
    permit icmp any any echo-reply (21374 matches)
    permit udp any any eq echo
    permit udp any eq echo any
    permit tcp any any established (150 matches)
    permit tcp any any (15 matches)
    permit ip any any (45 matches)
```

시리얼 인터페이스에 도착하는 대부분의 트래픽은 ICMP 에코 응답 패킷으로 구성됩니다.이것은 아마도 스머프 공격의 시그니처일 것입니다. 우리의 사이트는 리플렉터가 아니라 궁극적인 목표입니다.다음 출력에 표시된 대로 액세스 목록을 수정할 때 공격에 대한 자세한 정보를 수집할 수 있습니다.

```
interface serial 0
no ip access-group 169 in

no access-list 169
access-list 169 permit icmp any any echo
access-list 169 permit icmp any any echo-reply log-input
access-list 169 permit udp any any eq echo
access-list 169 permit udp any eq echo any
access-list 169 permit tcp any any established
access-list 169 permit tcp any any
access-list 169 permit ip any any

interface serial 0
ip access-group 169 in
```

여기서 변경하면 **log-input** 키워드가 의심스러운 트래픽과 일치하는 액세스 목록 항목에 추가됩니다.(11.2 이전 버전의 Cisco IOS Software 릴리스에는 이 키워드가 없습니다.대신 "**log**" 키워드를 사용합니다.) 그러면 라우터가 목록 항목과 일치하는 패킷에 대한 정보를 로깅합니다.**logging buffered**가 구성된 경우 **show log** 명령으로 표시되는 메시지를 볼 수 있습니다(속도 제한 때문에 메시지가 누적되는 데 다소 걸릴 수 있음). 메시지는 다음 출력과 유사합니다.

```
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.142
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.113
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.72
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.154
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.15
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.142
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.47
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.35
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.113
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.59
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.82
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.56
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.84
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.47
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.35
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.15
```

```
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.33
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
```

에코 응답 패킷의 소스 주소는 주소 접두사 192.168.212.0/24, 192.168.45.0/24 및 172.16.132.0/24에서 클러스터링됩니다. (192.168.x.x 및 172.16.x.x 네트워크의 개인 주소는 인터넷에 포함되지 않습니다.실습 그림입니다.) 이는 스머프 공격의 매우 특징이며, 소스 주소는 스머프 리플렉터의 주소입니다.적절한 인터넷 "whois" 데이터베이스에서 이러한 주소 블록의 소유자를 조회하면 이러한 네트워크의 관리자를 찾아 공격 처리에 대한 도움을 요청할 수 있습니다.

이 시점에서는 스머프 사건에서 이러한 반사 벡터가 공격자가 아니라 동료 희생자라는 것을 기억하는 것이 중요합니다.공격자가 DoS 플러드에서 IP 패킷에 자신의 소스 주소를 사용하는 경우는 극히 드물며, 진행 중인 스머프 공격에서는 이러한 소스 주소를 사용하는 것은 불가능합니다.플러드 패킷의 모든 주소는 완전히 위조된 것으로 가정하거나, 어떤 종류의 피해자의 주소로 간주해야 합니다.스머프 공격의 궁극적인 목표를 위한 가장 생산적인 방법은 리플렉터에 연락하여 공격 종료를 위해 네트워크를 재구성하도록 요청하거나, 자극적인 스트림을 추적하는데 도움을 요청하는 것입니다.

스머프 공격의 최종 표적에 대한 피해는 보통 인터넷에서 들어오는 링크를 오버로드하여 발생하므로, 반사판에 연결하는 것 외에는 응답이 없는 경우가 많습니다.패킷이 타겟의 제어 하에 있는 시스템에 도착할 때까지 대부분의 피해가 이미 완료되었습니다.

하나의 임시 방편적인 측정은 업스트림 네트워크 공급자에게 모든 ICMP 에코 응답 또는 특정 리플렉터의 모든 ICMP 에코 응답을 필터링하도록 요청하는 것입니다.이러한 종류의 필터는 영구적으로 그대로 두는 것이 좋습니다.임시 필터의 경우에도 모든 ICMP 패킷이 아니라 에코 응답만 필터링해야 합니다.또 다른 가능성은 업스트림 공급자가 QoS(Quality of Service) 및 속도 제한 기능을 사용하여 에코 응답에 사용할 수 있는 대역폭을 제한하는 것입니다.적절한 대역폭 제한은 무한정 그대로 유지할 수 있습니다.이 두 접근 방식은 모두 필요한 용량을 가진 업스트림 공급자의 장비에 따라 다르며, 경우에 따라 해당 용량을 사용할 수 없습니다.

스머프 리플렉터

수신 트래픽이 에코 응답 대신 에코 요청으로 구성된 경우(즉, 첫 번째 액세스 목록 항목이 두 번째 액세스 목록 항목이 예상한 것보다 더 많은 일치 항목을 계산한 경우), 네트워크가 리플렉터로 사용되고 있던 스머프 공격 또는 단순한 ping 플러드일 수 있습니다.어느 경우든 공격이 성공하면 직렬 회선의 발신 측면은 물론 수신 측도 압도될 것입니다.사실, 증폭 요인 때문에, 당신은 들어오는 쪽보다 나가는 쪽이 훨씬 더 과부하가 있을 것으로 예상합니다.

스머프 공격을 단순한 ping 플러드와 구별하는 방법은 여러 가지가 있습니다.

- 보통 ping 플러드는 거의 항상 유니캐스트를 사용하는 반면, Smurf 자극 패킷은 유니캐스트 주소가 아니라 직접 브로드캐스트 주소로 전송됩니다.적절한 액세스 목록 항목에서 **log-input** 키워드를 사용하는 주소를 볼 수 있습니다.
- 스머프 리플렉터로 사용되는 경우 시스템의 이더넷 측에 **show interface** 디스플레이의 출력 브로드캐스트가 지나치게 많으며, 일반적으로 **show ip 트래픽** 표시에서 전송되는 브로드캐스트 수가 지나치게 많습니다.표준 ping 플러드는 백그라운드 브로드캐스트 트래픽을 증가시키지 않습니다.
- 스머프 리플렉터로 사용되는 경우 인터넷에서 들어오는 트래픽보다 인터넷을 향해 나가는 트래픽이 더 많습니다.일반적으로 직렬 인터페이스의 입력 패킷보다 더 많은 출력 패킷이 있습니다.자극 스트림이 입력 인터페이스를 완전히 채우더라도 응답 스트림이 자극 스트림보다 크고 패킷 삭제가 계산됩니다.

스머프 리플렉터는 스머프 공격의 최종 목표보다 더 많은 옵션을 가지고 있다.리플렉터가 공격을

종료하도록 선택하는 경우 **no ip directed-broadcast**(또는 그와 동등한 non-IOS 명령)를 적절하게 사용합니다.이러한 명령은 활성 공격이 없는 경우에도 모든 컨피그레이션에 속합니다.Cisco 장비가 스머프 공격에 사용되지 않도록 방지하는 방법에 대한 자세한 내용은 Cisco 라우터의 보안 향상 을 참조하십시오.일반적인 스머프 공격에 대한 일반적인 정보와 타사 장비 보호에 대한 자세한 내용은 서비스 거부 공격 정보 페이지를 참조하십시오 .

스머프 리플렉터는 공격자에게 가장 가까운 한 단계이며, 따라서 공격을 추적하기에 더 나은 위치에 있습니다.공격을 추적하도록 선택하는 경우 관련 ISP와 함께 작업해야 합니다.추적을 완료했을 때 조치를 취하려면 적절한 법 집행 기관과 함께 작업해야 합니다.공격을 추적하려는 경우 가능한 한 빨리 법 집행을 수행하는 것이 좋습니다.플러딩 공격 추적에 대한 기술 정보는 추적 섹션을 참조하십시오.

조각

fraggle 공격은 ICMP 에코 요청 대신 UDP 에코 요청이 자극적인 스트림에 사용된다는 점을 제외하면 스머프 공격과 유사합니다.액세스 목록의 세 번째 및 네 번째 행은 단편적인 공격을 식별합니다 .UDP 에코가 ICMP 에코보다 대부분의 네트워크에서 덜 중요한 서비스라는 점을 제외하면 피해자에 대한 적절한 응답이 동일합니다.따라서 부정적인 결과를 줄이면서 완전히 비활성화할 수 있습니다.

SYN 플러드

액세스 목록의 다섯 번째와 여섯 번째 줄은 다음과 같습니다.

```
access-list 169 permit tcp any any established
access-list 169 permit tcp any any
```

이러한 선 중 첫 번째 항목은 ACK 비트 세트와 모든 TCP 패킷과 일치합니다.우리의 목적을 위해, 이것이 의미하는 것은 TCP SYN이 아닌 모든 패킷과 일치한다는 것입니다.두 번째 행은 TCP SYN인 패킷만 매칭합니다.SYN 플러드는 이러한 목록 항목의 카운터에서 쉽게 식별됩니다.일반 트래픽에서 비 SYN TCP 패킷은 SYN보다 적어도 2배 이상 많으며, 대개 4~5배 정도 많습니다.SYN 플러드에서는 일반적으로 SYN이 비 SYN TCP 패킷보다 여러 번 많습니다.

이 시그니처를 생성하는 유일한 비공격 조건은 정품 연결 요청의 대량 오버로드입니다.일반적으로 이러한 오버로드는 예기치 않게 발생하지 않으며 실제 SYN 플러드만큼 많은 SYN 패킷을 포함하지 않습니다.또한 SYN 플러드에는 소스 주소가 완전히 잘못된 패킷이 포함되어 있는 경우가 많습니다 .**log-input** 키워드를 사용하여 연결 요청이 해당 주소에서 오는지 확인할 수 있습니다.

SYN 플러드와 다소 비슷한 "프로세스 테이블 공격"이라고 불리는 공격이 있습니다.프로세스 테이블 공격에서는 TCP 연결이 완료되고, 이후 프로토콜 트래픽 없이 시간 초과가 허용되는 반면, SYN 플러드에서는 초기 연결 요청만 전송됩니다.프로세스 테이블 공격은 TCP 초기 핸드셰이크를 완료해야 하므로 일반적으로 공격자가 액세스할 수 있는 실제 시스템의 IP 주소를 사용하여 시작해야 합니다(일반적으로 도난 액세스). 따라서 프로세스 테이블 공격은 패킷 로깅을 사용하여 SYN 플러드와 쉽게 구별됩니다.프로세스 테이블 공격의 모든 SYN은 하나 또는 몇 개의 주소 또는 하나 또는 몇 개의 서브넷에서 옵니다.

SYN 홍수 피해자들에 대한 대응 옵션은 매우 제한적입니다.공격 중인 시스템은 일반적으로 중요한 서비스이며, 시스템에 대한 액세스를 차단하면 공격자가 원하는 것이 됩니다.Cisco를 비롯한 많은 라우터 및 방화벽 제품에는 SYN 플러드의 영향을 줄이는 데 사용할 수 있는 기능이 있습니다.그러나 이러한 기능의 효율성은 환경에 따라 달라집니다.자세한 내용은 Cisco IOS Firewall Feature Set 설명서, Cisco IOS TCP Intercept 기능 설명서 및 Cisco 라우터의 보안 개선 설명서를 참조하십시오 .

SYN 플러드는 추적할 수 있지만, 추적 프로세스에서는 공격자에서 피해자로 연결되는 경로를 따라 각 ISP의 지원이 필요합니다.SYN 플러드를 추적하려고 할 경우, 조기에 법률 집행 기관에 문의하고 자체 업스트림 서비스 공급자와 협력하십시오.Cisco 장비 사용을 추적하는 방법에 대한 자세한 내용은 이 문서의 추적 섹션을 참조하십시오.

기타 공격

공격을 받고 있다고 믿고 IP 소스 및 목적지 주소, 프로토콜 번호, 포트 번호를 사용하여 공격의 특성을 지정할 수 있는 경우 액세스 목록을 사용하여 가설을 테스트할 수 있습니다.의심스러운 트래픽과 일치하는 액세스 목록 항목을 생성하고, 적절한 인터페이스에 적용하고, 매치 카운터를 관찰하거나 트래픽을 로깅합니다.

로깅 및 카운터 경고

액세스 목록 항목의 카운터는 해당 항목과 일치하는 모든 항목을 계산합니다.두 인터페이스에 액세스 목록을 적용할 경우 표시되는 카운트는 집계 카운트입니다.

액세스 목록 로깅에는 항목과 일치하는 모든 패킷이 표시되지 않습니다.CPU 오버로드를 방지하기 위해 로깅 속도가 제한됩니다.로깅에 표시되는 것은 적절한 대표 샘플이지만 완전한 패킷 추적은 아닙니다.보이지 않는 패킷이 있습니다.

일부 소프트웨어 버전에서는 액세스 목록 로깅이 특정 스위칭 모드에서만 작동합니다.액세스 목록 엔트리가 많은 일치 항목을 계산하지만 로깅은 없는 경우 경로 캐시를 지워 패킷이 프로세스 스위칭되도록 합니다.많은 인터페이스가 있는 로드가 많은 라우터에서 이 작업을 수행할 경우 주의하십시오.캐시를 재구축하는 동안 많은 트래픽이 삭제될 수 있습니다.가능하면 Cisco Express Forwarding을 사용하십시오.

액세스 목록 및 로깅은 성능에 영향을 미치지만 큰 것은 아닙니다.약 80% 이상의 CPU 로드에서 실행되는 라우터 또는 매우 고속 인터페이스에 액세스 목록을 적용할 때 주의해야 합니다.

추적

DoS 패킷의 소스 주소는 거의 항상 공격자 자체와 아무런 관련이 없는 값으로 설정됩니다.따라서 공격자를 식별하는 데 유용하지 않습니다.공격의 소스를 확인할 수 있는 유일한 안정적인 방법은 네트워크를 통해 백홉별로 공격을 추적하는 것입니다.이 프로세스에는 라우터를 재구성하고 로그 정보를 검토하는 작업이 포함됩니다.공격자에서 피해자에 이르는 경로를 따라 모든 네트워크 운영자의 협조가 필요합니다.이러한 협력을 확보하려면 일반적으로 법 집행 기관의 개입이 필요하며, 이들은 공격자에 대해 조치를 취할 경우 관여해야 합니다.

DoS 플러드의 추적 프로세스는 비교적 간단합니다.플러드 트래픽을 전달하는 것으로 알려진 라우터("A")에서 시작하여 A가 트래픽을 수신하는 라우터("B")를 식별합니다.그런 다음 B에 로그인하여 B가 트래픽을 수신하는 라우터(이름이 "C"임)를 찾습니다.최종 소스가 발견될 때까지 계속됩니다.

이 방법에는 다음과 같은 몇 가지 복잡한 문제가 있습니다.

- "최종 출처"는 공격자에 의해 감염되었지만 실제로 다른 피해자가 소유하고 운영하는 컴퓨터입니다.이 경우 DoS 플러드를 추적하는 것이 첫 단계입니다.
- 공격자는 추적될 수 있음을 알고 있으며, 대개 제한된 시간 동안만 공격을 계속합니다.실제로 홍수를 추적할 시간이 충분하지 않을 수도 있습니다.
- 공격은 여러 소스에서 발생할 수 있습니다. 특히 공격자가 상대적으로 정교한 경우 더욱 그렇습

니다.가능한 한 많은 출처를 알아내는 것이 중요하다.
- 통신 문제로 추적 프로세스가 느려졌습니다.관련된 네트워크 운영자 중 한 명 이상이 적절한 기술을 갖춘 인력을 보유하고 있지 않은 경우가 많습니다.
- 법적 및 정치적 우려 때문에 공격자가 발견되더라도 공격자에 대해 조치를 취하기가 어려울 수 있습니다.

DoS 공격을 추적하려는 대부분의 노력이 실패합니다.이로 인해 많은 네트워크 운영자들은 압박을 받지 않는 한 공격을 추적하려고 시도조차 하지 않습니다.다른 많은 이들은 "심각한" 공격만 추적하며, "심각한" 공격에 대한 정의는 서로 다릅니다. 일부는 법 집행과 관련된 경우에만 추적을 지원합니다.

"log-input"으로 추적

Cisco 라우터를 통과하는 공격을 추적하도록 선택할 경우, 가장 효과적인 방법은 공격 트래픽과 일치하는 액세스 목록 항목을 구성하고, **log-input** 키워드를 추가하고, 공격 스트림이 최종 타겟으로 전송되는 인터페이스에 액세스 목록 아웃바운드를 적용하는 것입니다.액세스 목록에 의해 생성되는 로그 항목은 트래픽이 도달하는 라우터 인터페이스를 식별하고, 인터페이스가 멀티포인트 연결인 경우 수신되는 디바이스의 레이어 2 주소를 지정합니다.그런 다음 레이어 2 주소를 사용하여 체인의 다음 라우터를 식별할 수 있습니다. 예를 들어 **show ip arp *mac-address* 명령을 사용합니다**.

SYN 플러드

SYN 플러드를 추적하려면 다음과 유사한 액세스 목록을 만들 수 있습니다.

```
access-list 169 permit tcp any any established
access-list 169 permit tcp any host victim-host log-input
access-list 169 permit ip any any
```

이 로그는 합법적인 SYN을 포함하여 대상 호스트로 향하는 모든 SYN 패킷을 로깅합니다.공격자를 향한 실제 경로를 식별하려면 로그 항목을 자세히 검토합니다.일반적으로 플러드의 소스는 가장 많은 수의 일치하는 패킷이 도착하는 소스입니다.소스 IP 주소 자체는 아무것도 아닙니다.소스 인터페이스와 소스 MAC 주소를 찾고 있습니다.플러드 패킷에 잘못된 소스 주소가 있을 수 있으므로 플러드 패킷과 합법적인 패킷을 구분할 수 있는 경우도 있습니다.소스 주소가 유효하지 않은 패킷은 플러드에 속할 가능성이 높습니다.

SYN 플러드에는 상대적으로 드문 일이지만, 이 홍수는 여러 소스에서 발생할 수 있습니다.

스머프 자극제

스머프 경기 스트림을 추적하려면 다음과 같은 액세스 목록을 사용합니다.

```
access-list 169 permit icmp any any echo log-input
access-list 169 permit ip any any
```

첫 번째 항목은 리플렉터 주소로 향하는 패킷으로 자신을 제한하지 않습니다.그 이유는 대부분의 스머프 공격이 여러 리플렉터 네트워크를 사용하기 때문입니다.최종 대상과 연락하지 않을 경우 리플렉터 주소를 모두 알지 못할 수 있습니다.추적이 공격의 소스에 가까워지면 에코 요청이 더 많은 목적지로 이동하는 것을 볼 수 있습니다.이것은 좋은 징조이다.

그러나 많은 ICMP 트래픽을 처리하는 경우, 이렇게 하면 너무 많은 로깅 정보를 생성하여 쉽게 읽을 수 있습니다.이러한 경우 목적지 주소를 사용한다고 알려진 리플렉터 중 하나로 제한할 수 있습니다.또 다른 유용한 전술은 255.255.255.0의 넷마스크가 인터넷에서 매우 흔하다는 사실을 악용하

는 항목을 사용하는 것입니다.공격자가 스머프 리플렉터를 찾는 방식 때문에, 스머프 공격에 실제로 사용되는 리플렉터 주소는 그 마스크와 훨씬 더 일치합니다..0 또는 .255로 끝나는 호스트 주소는 인터넷에서 매우 흔합니다.따라서 다음과 같은 출력으로 스머프 자극에 대해 상대적으로 구체적인 인식기를 만들 수 있습니다.

```
access-list 169 permit icmp any host known-reflector echo log-input access-list 169 permit icmp any 0.0.0.255 255.255.255.0 echo log-input access-list 169 permit icmp any 0.0.0.0 255.255.255.0 echo log-input access-list 169 permit ip any any
```

이 목록을 사용하면 로그에서 많은 "노이즈" 패킷을 제거할 수 있지만, 공격자에게 더 가까이 다가가면 추가 자극의 흐름을 인식할 수 있습니다.

"log-input"이 없는 추적

log-input 키워드는 Cisco IOS Software Releases 11.2 이상 및 서비스 공급자 시장을 위해 특별히 만들어진 특정 11.1 기반 소프트웨어에 있습니다.오래된 소프트웨어는 이 키워드를 지원하지 않습니다.이전 소프트웨어가 포함된 라우터를 사용하는 경우 다음과 같은 세 가지 실행 가능한 옵션이 있습니다.

- 로깅하지 않고 의심스러운 트래픽과 일치하는 항목이 있는 액세스 목록을 생성합니다.각 인터페이스의 *입력* 쪽에 목록을 차례로 적용하고 카운터를 확인합니다.일치 속도가 높은 인터페이스를 찾습니다.이 방법은 성능 오버헤드가 매우 작으며 소스 인터페이스를 식별하는 데 유용합니다.가장 큰 단점은 링크 레이어 소스 주소를 제공하지 않으므로 포인트 투 포인트 회선에 주로 유용합니다.
- **log-input**과 반대로 **log** 키워드로 액세스 목록 항목**을** 생성합니다. 다시 한 번, 각 인터페이스의 수신 측에 목록을 차례로 적용합니다.이 방법은 여전히 소스 MAC 주소를 제공하지는 않지만 IP 데이터를 보는 데 유용할 수 있습니다.예를 들어, 패킷 스트림이 실제로 공격의 일부인지 확인합니다.성능에 미치는 영향은 이전 소프트웨어보다 보통~높음, 최신 소프트웨어가 더 잘 작동합니다.
- **debug ip packet detail** 명령을 사용하여 패킷에 대한 정보를 수집합니다.이 방법은 MAC 주소를 제공하지만 성능에 심각한 영향을 미칠 수 있습니다.이 방법을 잘못 사용하여 라우터를 사용할 수 없게 만드는 것은 쉽습니다.이 방법을 사용하는 경우, 라우터가 공격 트래픽을 빠른, 자동 또는 최적 모드로 전환하는지 확인합니다.액세스 목록을 사용하여 필요한 정보만 디버깅할 수 있습니다.디버깅 정보를 로컬 로그 버퍼에 로깅하지만 텔넷 세션 및 콘솔에 대한 디버그 정보 로깅을 해제합니다.가능한 경우, 필요에 따라 전원을 껐다가 켜서 라우터에 물리적으로 가까이 있는 사람을 준비합니다.debug **ip packet** 명령은 고속 스위치드 패킷에 대한 정보를 표시하지 않습니다.정보를 캡처하려면 **clear ip cache** 명령을 실행해야 합니다.각 **clear** 명령은 디버그 출력의 패킷을 한두 개 제공합니다.

관련 정보

- Kerberos
- 기술 지원 및 문서 – Cisco Systems