TCP SYN 서비스 거부 공격으로부터 보호하기 위한 전략 정의

목차

요약

네트워크 장치를 대상으로 하는 인터넷 서비스 공급자(ISP)의 잠재적인 서비스 거부 공격이 있습니다.

- **TCP SYN 공격**:발신자는 완료할 수 없는 연결 볼륨을 전송합니다.그러면 연결 큐가 채워져 합법적인 TCP 사용자에 대한 서비스가 거부됩니다.

이 백서에서는 잠재적인 TCP SYN 공격 발생 방식에 대한 기술적 설명과 Cisco IOS 소프트웨어를 사용하여 이를 방어하는 방법을 제시합니다.

참고: Cisco IOS 11.3 소프트웨어에는 TCP 서비스 거부 공격을 능동적으로 방지하는 기능이 있습니다.이 기능은 TCP 가로채기 구성(서비스 거부 공격 방지) 문서에서 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.라이브 네트워크에서 작업하는 경우, 사용하기 전에 모든 명령의 잠재적인 영향을 이해해야 합니다.

표기 규칙

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

문제 설명

TCP SYN 공격

일반 TCP 연결이 시작되면 대상 호스트는 소스 호스트에서 SYN(동기화/시작) 패킷을 수신하고 SYN ACK(동기화 승인)를 다시 보냅니다. 그런 다음 대상 호스트가 SYN ACK의 ACK(승인)를 들어야 연결이 설정됩니다.이를 "TCP 3방향 핸드셰이크"라고 합니다.

SYN ACK에 대한 ACK를 기다리는 동안 목적지 호스트의 제한된 크기의 연결 대기열이 완료되기를 기다리는 연결을 추적합니다.일반적으로 이 대기열은 SYN ACK가 몇 밀리초 후에 도착할 예정이므로 빠르게 비워집니다.

TCP SYN 공격은 공격 소스 호스트가 임의의 소스 주소가 있는 TCP SYN 패킷을 피해자 호스트에 생성하도록 함으로써 이 설계를 악용합니다.피해자 대상 호스트는 SYN ACK를 임의의 소스 주소로 다시 전송하고 연결 대기열에 항목을 추가합니다.SYN ACK는 부정확하거나 존재하지 않는 호스트를 대상으로 하므로 "3방향 핸드셰이크"의 마지막 부분은 완료되지 않으며 타이머가 만료될 때까지 항목이 연결 대기열에 남아 있습니다(일반적으로 약 1분).랜덤 IP 주소에서 신속하게 거짓 TCP SYN 패킷을 생성함으로써 연결 대기열을 채우고 합법적인 사용자에게 TCP 서비스(예: 이메일, 파일 전송 또는 WWW)를 거부할 수 있습니다.

소스의 IP 주소가 위조되므로 공격의 발신자를 쉽게 추적할 수 없습니다.

문제의 외부 매니페스트션에는 전자 메일을 받을 수 없거나, WWW 또는 FTP 서비스에 대한 연결을 수락할 수 없거나, SYN_RCVD 상태의 호스트에서 많은 수의 TCP 연결이 포함됩니다.

네트워크 장치에 대한 공격으로부터 보호

방화벽 뒤에 있는 장치

TCP SYN 공격은 임의 소스 IP 주소에서 SYN 패킷이 유입되는 것이 특징입니다.인바운드 SYN 패킷을 중지하는 방화벽 뒤에 있는 모든 디바이스는 이미 이 공격 모드에서 보호되며 추가 조치가 필요하지 않습니다.방화벽의 예로는 Cisco PIX(Private Internet Exchange) 방화벽 또는 액세스 목록으로 구성된 Cisco 라우터가 있습니다.Cisco 라우터에서 액세스 목록을 설정하는 방법에 대한 예는 IP 네트워크에서 보안 강화 문서를 참조하십시오.

공개적으로 이용 가능한 서비스를 제공하는 장치(메일 서버, 공용 웹 서버)

액세스 목록을 사용하여 일부 IP 주소에 대한 인바운드 액세스를 명시적으로 제한할 수 있으므로 방화벽 뒤에 있는 디바이스에서 무작위 IP 주소를 사용하여 SYN 공격을 방지하는 것은 비교적 간단

합니다.그러나 인터넷을 접하는 공용 웹 서버 또는 메일 서버의 경우 어느 수신 IP 소스 주소가 친화적인지 불친절한지 확인할 방법이 없습니다.따라서 랜덤 IP 주소에서 오는 공격에 대해 명확한 방어가 이루어지지 않습니다.다음과 같은 몇 가지 옵션을 호스트에서 사용할 수 있습니다.

- 연결 큐(SYN ACK 큐)의 크기를 늘립니다.
- 3방향 핸드셰이크를 기다리는 시간 제한을 줄입니다.
- 공급업체 소프트웨어 패치를 사용하여 문제를 탐지하고 우회합니다(가능한 경우).

호스트 공급업체에 문의하여 TCP SYN ACK 공격을 해결하기 위한 특정 패치를 만들었는지 확인해야 합니다.

참고: 공격자는 IP 주소를 변경할 수 있으므로 서버에서 IP 주소를 필터링하는 것은 효율적이지 않으며 주소는 합법적인 호스트의 주소와 같을 수도 있고 같지 않을 수도 있습니다.

네트워크를 무의식 중에 공격으로부터 방지

이러한 서비스 거부 공격의 기본 메커니즘은 무작위 IP 주소에서 소싱된 트래픽을 생성하는 것이므로 인터넷을 대상으로 향하는 트래픽을 필터링하는 것이 좋습니다.기본 개념은 잘못된 소스 IP 주소가 있는 패킷을 인터넷에 입력할 때 버리는 것입니다.이렇게 하면 네트워크에 대한 서비스 거부 공격을 방지할 수 없지만 공격자가 공격자의 소스로 사용자의 위치를 제외하는 데 도움이 됩니다.또한 이러한 유형의 공격의 기반으로서 네트워크를 덜 매력적으로 만듭니다.

유효하지 않은 IP 주소의 전송 방지

네트워크를 인터넷에 연결하는 라우터에서 패킷을 필터링하면 유효한 소스 IP 주소가 있는 패킷만 네트워크를 떠나 인터넷에 액세스하도록 허용할 수 있습니다.

예를 들어, 네트워크가 네트워크 172.16.0.0으로 구성되고 라우터가 직렬 0/1 인터페이스를 사용하여 ISP에 연결되는 경우 다음과 같이 액세스 목록을 적용할 수 있습니다.

```
access-list 111 permit ip 172.16.0.0 0.0.255.255 any
access-list 111 deny ip any any log

interface serial 0/1
ip access-group 111 out
```

참고: 액세스 목록의 마지막 행은 인터넷에 잘못된 소스 주소가 포함된 트래픽이 있는지 여부를 결정합니다.이 회선을 사용하는 것은 중요하지만, 가능한 공격의 출처를 찾는 데 도움이 될 것입니다.

유효하지 않은 IP 주소의 수신 방지

엔드 네트워크에 서비스를 제공하는 ISP의 경우, 클라이언트에서 들어오는 패킷의 검증을 적극 권장합니다.이 작업은 경계 라우터에서 인바운드 패킷 필터를 사용하여 수행할 수 있습니다.

예를 들어, 클라이언트에 "serial 1/0"이라는 직렬 인터페이스를 통해 라우터에 연결된 다음 네트워크 번호가 있는 경우 다음 액세스 목록을 생성할 수 있습니다.

```
The network numbers are 192.168.0.0 to 192.168.15.0, and 172.18.0.0.

access-list 111 permit ip 192.168.0.0 0.0.15.255 any
access-list 111 permit ip 172.18.0.0 0.0.255.255 any
```

```
access-list 111 deny ip any any log

interface serial 1/0
ip access-group 111 in
```

참고: 액세스 목록의 마지막 행은 인터넷에 잘못된 소스 주소가 포함된 트래픽이 있는지 여부를 결정합니다.이 회선을 사용하는 것은 필수적이지 않지만 가능한 공격의 출처를 찾는 데 도움이 됩니다.

이 항목에서는 NANOG [North American Network Operator1s Group] 메일 목록에 대해 자세히 설명합니다.목록 아카이브는 다음 위치에 있습니다
.http://www.merit.edu/mail.archives/nanog/index.html

TCP SYN 서비스 거부 공격 및 IP 스푸핑에 대한 자세한 설명은 다음을 참조하십시오
.http://www.cert.org/advisories/CA-1996-21.html

http://www.cert.org/advisories/CA-1995-01.html

관련 정보

- Technical Support - Cisco Systems