Firewall Security Testing

(infosecinstitute)

번역 문서

원본 : http://resources.infosecinstitute.com/firewall-security-testing/

번역자 정진환 (쇼우)
조혜정(scv4424)
편집자 조정원 (니키)

- 보안프로젝트 (www.boanproject.com) -

목 차

1. 시작하기전에

방화벽 테스트와 IDS(침입탐지 시스템) 규칙은 침투 테스트 또는 보안감사의 정규 부분입니다. 그러나 다른 환경에 관련된 고유의 복잡성 때문에 자동스캐너는 이 지역에서 많은 사용을 제공할 수 없습니다. 몇몇 무료와 오픈 소스 도구는 일반적인 평가에 도움이 될 수 있는 테스트 방화벽과 IDS 규칙 기술 패킷을 돕기 위해 존재합니다.

일반적인 작업 TCP/IP 의 지식은 도구의 사용뿐만 아니라 휴대용 테스트를 위한 Linux 또는 OS X 에서 휴대용 컴퓨터에 권장접근을 하기 위해 필요합니다. 방화벽과 규칙의 일반적인 평가를 획득한 후, 규칙에 대한 정정을 적절하게 업데이트할 수 있습니다.

오늘, 기본적으로 주요 공급업체에서 현대의 방화벽은 엄격한 규칙 세트가 일반적으로 상당히 안전합니다. 공급업체는 이전 년도 보다 더 많은 보안을 의식하고 있고 이제 다행히도 환경과 인터넷의 보안의식을 더 많이 반영하고 있습니다. 다양한 테스트는 여전히 장소에서 규칙이 반드시 요구되고 조직되기 때문에 그들은 테스트나 배열에서 향상 지역에 위치시켜야 합니다.

각각의 TCP 또는 UDP 패킷은 라우팅에 관해서 헤더 정보의 네 가지 기본 부분으로 구성되어 있습니다. :
* 소스 포트 : 소스 IP | 대상 포트 : 대상 IP

방화벽 규칙은 종종 그들이 패킷 헤더에 이러한 소스/대상 징후를 기반으로 두어 패킷과 경로를 검사하도록 설치합니다. 이것의 문제는 소스 IP 또는 포트가 빈곤한 규칙의 자리에 있다면 방화벽을 우회하려고 시도하기 위해 변경될 수 있습니다.

방화벽 규칙은 대부분의 경우 이러한 보안 문제의 다수를 피하기 위해 나중에 ACCEPT 수락 규칙 뒤에 첫 번째 규칙 DENY 를 처리하도록 환경을 설정해야 합니다.

2. tcpdump 에서 보조 노드

방화벽 테스트는 일반적으로 두 가지 구성요소가 포합됩니다.: 활성 프로세스 또는 응용프로그램은 이벤트의 패킷 캡쳐 아래로 요청하며 또한 별도의 독립적인 응용프로그램 기록을 전했습니다.

아래의 예제가 포함되어 있는, 그것은 상호작용과 요청 대상 방화벽에서 결과를 기록하기 위해 별도의 창에서 tcpdump 또는 wireshark 를 실행하는 것을 권합니다.

```
1 $ sudo tcpdump -i eth0
```

tcpdump 방침을 실행하면 I [인터페이스]는 당신의 터미널 창에서 간단한 출력을 제공할 것입니다. 그것이 파일에 자세히 써 데이터를 가지고 하는 것이 더 바람직하다면, 뾰족한 w 를 사용합니다.

```
1 $ sudo tcpdump -i eth0 -w myfile.cap
```

3. namp

nmap 은 열린 포트에 관해 몇 가지 초기 방화벽 평가를 얻을 뿐만 아니라 빠른 검사를 필요로 몇 가지 일반적인 방화벽 검사를 수행하기 위해서만 유용하지 않습니다.

특히, 현대의 방화벽은 패킷을 산산이 부수거나 트래픽이 방화벽을 통과하도록 대체 소스포트를 사용하여 호스트에 의해 던져지면 안됩니다.

```
$ sudo nmap [target]
```

옵션이 없이 자연스럽게 nmap 을 실행하면 오직 TCP 스캔을 수행할 것입니다.

ICMP 응답은 nmap 의 ICMP 호스트 발견 단계를 건너 뛰기 위해 막혔다면 -Pn 을 사용하세요.

```
$ sudo nmap example.com
Starting Nmap 5.51 ( http://nmap.org ) at 2012-04-24 18:22 EDT
Nmap scan report for example.com (192.168.1.14)
Host is up (0.12s latency).
Not shown: 990 filtered ports
PORT    STATE SERVICE
25/tcp   open  smtp
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
443/tcp  open  https
465/tcp  open  smtps
587/tcp  open  submission
993/tcp  open  imaps
995/tcp  open  pop3s
5432/tcp open  postgresql
```

SYN 스캔

```
$ sudo nmap -sS [target]
```

TCP SYN 스캔은 -sS 사용을 수행합니다. 이것은 일반적으로 포트스캐너를 차단하는 방화벽에 도움이 됩니다.

SYN 스캔은 오직 절반 개방 연결로 알려진 것을 만드는 초기 TCP SYN 패킷을 보냅니다.

그것은 종종 이 방법은 리소스의 로드 줄이기 또는 네트워크 스트레스를 일으키는 것으로 인식되고 있습니다.

ACK 스캔

```
$ sudo nmap -sA [target]
```

TCP ACK 스캔은 또한 유용할 수 있습니다. 만약 방화벽에서 허용한다면, 포트가 필터링이나 필터가 없는 경우 ACK 스캔을 다시 보고 할 수 있습니다.

일반적으로, 가장 현대적인 방화벽들은 ACK 요청을 필터링 합니다.

아래는 테스트의 이 종류를 필터 하도록 제대로 환경이 설정된 방화벽으로부터 출력은 다음과 같습니다.:

```
$ sudo nmap -sA example.com
Starting Nmap 5.51 ( http://nmap.org ) at 2012-04-24 18:19 EDT
Nmap scan report for example.com (192.168.1.12)
Host is up (0.11s latency).
rDNS record for 192.168.1.12: example.com
All 1000 scanned ports on example.com (192.168.1.12) are filtered
```

방화벽을 위한 비교는 ACK 스캔으로부터 테스트는 필터링 되지 않습니다.:

```
$ sudo nmap -sA example.com

Starting Nmap 5.51 ( http://nmap.org ) at 2012-04-24 18:21 EDT
Nmap scan report for example.com (192.168.1.12)
Host is up (0.10s latency).
rDNS record for 192.168.1.12: example.com
Not shown: 996 filtered ports
PORT    STATE    SERVICE
22/tcp  unfiltered ssh
25/tcp  unfiltered smtp
80/tcp  unfiltered http
443/tcp unfiltered https
```

UDP 스캔

```
$ sudo nmap -sU [target]
```

UDP 스캔을 수행하려면, -sU 를 사용하세요.
이것은 방화벽의 현재 개방된 UDP 포트 점검을 위한 TCP 스캔이 추가로 수행되어야 합니다.

UDP 포트에 대한 스캔을 하는 것은 TCP 에 대한 스캔, 앞뒤로의 부족으로 인해 핸드셰이크 응답이 UDP 패킷을 보낼 때 보다 더 문제가 있습니다.

UDP 스캔을 시도할 때 많은 잘못된 반응이 발생할 수도 있으니 주의하세요.

추가 nmap 팁

```
$ sudo nmap -f [target]
```

일반적인 포트 평가는 nmap 으로 달성되면, 다른 빠른 검사의 몇 개는 방화벽 규칙을 테스트하기 위해 수행할 수 있습니다.

-f 조각 패킷

nmap 에서 압정 f 는 Linux 나 BSD 호스에서 가능합니다. 이 옵션은 방화벽을 우회하는데 사용됩니다.; 그래도, 다시, 대부분의 현대적인 방화벽 공급업자들은 이러한 유형의 요청을 차단합니다.

방화벽에 대한 테스트는 일반적인 트래픽보다 이 트래픽을 다르게 처리하지 않습니다.
-g 는 소스 포트로 명시합니다.

언급했듯이, 각 패킷은 소스 IP 와 목적지 IP 와 함께 소스포트와 마찬가지로 목적지포트를 가지고 있습니다. 그것은 방화벽 규칙을 특정 소스 포트에 따라 트래픽을 허용하도록 환경을 설치 하였다면 테스트하는 빠른 nmap 테스트와 소스포트를 변경할 수 있습니다.

포트 53 또는 20 은 종종 테스트 소스포트로 사용됩니다.

많은 시간 이것은 트래픽이 특정소스/목적지 콤보와 방화벽을 통과하도록 허용했다면 대상포트 지정의 조합에 사용되었습니다.:

```
$ sudo nmap -g53 -p22 [target]
```

다음은 방화벽에서 필터링된 포트 22 TCP 호스트의 예입니다.

트래픽이 방화벽을 우회하도록 허용하는 20 소스포트를 사용하여 다음과 같이 설명할 수 있습니다.:

```
$ sudo nmap -sS -p22 -g20 192.168.1.16
Starting Nmap 5.51 ( http://nmap.org ) at 2012-04-24 18:12 EDT
Nmap scan report for 192.168.1.16
Host is up (0.057s latency).
PORT    STATE    SERVICE
22/tcp filtered ssh
```

반면에, 전형적인 포트 스캔은 지정된 포트가 보이게 게재되지 않습니다.:

```
$ sudo nmap 192.168.1.16
Starting Nmap 5.51 ( http://nmap.org ) at 2012-04-24 18:14 EDT
Nmap scan report for 192.168.1.16
Host is up (0.060s latency).
Not shown: 998 filtered ports
PORT    STATE  SERVICE
80/tcp  closed http
443/tcp closed https
```

4. hping

hping 은 ping 유틸리티를 ICMP 패킷을 작동시키는 반복적인 방식으로 TCP, UDP 또는 ICMP 패킷 많이 만드는 툴입니다.

hping 은 특정포트 또는 패킷이 대상 방화벽 측면에서 필터링이 되고 있는지 또는 특정 트래픽 유형이 모두 조작되고 있는지 검사하는데 유용합니다.

hping 과 명령의 예입니다.:

```
$ sudo hping3 192.168.1.202 -p 22 -c 4 -V -S
```

sudo hping3 [목적지 호스트] [포트] [전송하는 패킷 수] [자세한 정보표시] [SYN 에 대한 -S]
이 위의 예제는 호스트 포트 22 에 4 개의 TCP SYN 패킷을 보내고 있습니다. 이것은 hping 명령 두 번째 터미널을 열고 동시에 세션을 기록하는 tcpdump 를 실행하는 동안 도움이 됩니다.

필터링 되는 포트 22 트래픽의 예는 다음과 비슷합니다.:

```
$ sudo hping3 example.com -p 22 -c 4 -V -S
Password:
using en1, addr: 172.16.1.101, MTU: 1500
HPING example.com (en1 192.168.1.12): S set, 40 headers + 0 data bytes

--- example.com hping statistic ---
4 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

포트 22 SYN 패킷들을 허용하는 반면에 다음과 비슷하게 나타납니다.

```
$ sudo hping3 example.com -p 22 -c 4 -V -S
using en1, addr: 172.16.1.101, MTU: 1500
HPING example.com (en1 192.168.1.14): S set, 40 headers + 0 data bytes
len=44 ip=192.168.1.14 ttl=51 DF id=0 tos=0 iplen=44
sport=22 flags=SA seq=0 win=14600 rtt=94.4 ms
seq=2025389860 ack=1382964684 sum=d336 urp=0

len=44 ip=192.168.1.14 ttl=51 DF id=0 tos=0 iplen=44
sport=22 flags=SA seq=1 win=14600 rtt=114.5 ms
seq=2231940279 ack=1895298182 sum=abbf urp=0

len=44 ip=192.168.1.14 ttl=51 DF id=0 tos=0 iplen=44
sport=22 flags=SA seq=2 win=14600 rtt=97.0 ms
seq=1994283418 ack=1525068590 sum=5b80 urp=0

len=44 ip=192.168.1.14 ttl=51 DF id=0 tos=0 iplen=44
sport=22 flags=SA seq=3 win=14600 rtt=95.3 ms
seq=96473888 ack=1204458524 sum=216a urp=0

--- example.com hping statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 94.4/100.3/114.5 ms
```

5. tcpreply

tcpreply 는 많은 방화벽 공급업체에 의해 자신의 방화벽 하드웨어를 테스트하는데 사용하는 도구입니다.

topreply 는 특성 대상에 대해 이전에 기록된 패킷캡처 (.pcap 형식)를 재생하여 작동합니다. 특정 캡처는 tcprewrite 로 수정하고 주어진 네트워크 트래픽 시나리오를 위해 특정 하드웨어 또는 TCP/IP 스택을 테스트하는데 도움이 되는 재생을 할 수 있습니다.

tcpreplay 는 단순히 재생 테스트를 위한 수정한 캡처를 사용할 뿐만 아니라, 그것은 장치에 대해서도 캡처한 트래픽의 특정 속도를 테스트하는 데 사용됩니다.

지정된 특정 패킷 캡처를 통해 재생하려면 다음 명령어를 사용하세요.:

```
$ sudo tcpreplay --intf1=eth0 file.cap
```

재생속도는 mpbs 에 지정할 수 있습니다, 예를 들어:

```
$ sudo tcpreplay --mbps=100.0 --intf1=eth0 file.cap
```

tcpreplay 의 대응은 tcprewrite 이다. tcprewrite 는 다음 tcpreplay 를 통해 재생될 수 있는 기존 캡처파일을 수정하는데 사용됩니다.

패킷 캡처 파일을 편집하기 위해 사용되는 구문입니다.;

```
$ tcprewrite [options] --infile=input.cap --outfile=output.cap
```

다양한 옵션은 tcp/udp 포트를 다시 쓰기, 소스/목적지주소 다시 쓰기, MTU 를 변경, 소스/목적지 MAC 주소 변경, 뿐만 아니라 이더넷 체크섬 수정이 포함됩니다.

추가정보는 프로젝트 페이지 위키에서 찾아볼 수 있습니다.

(http://tcpreplay.synfin.net/wiki/tcprewrite)

6. Legacy tools

관심이 있을 것 같은 다른 도구는 TCP/IP 스택의 안정성 테스트를 할 수 있는 isic 입니다.: http://isic.sourceforge.net/. Tomahawk 는 네트워크 하드웨어의 네트워크 처리량을 테스트 하기 위해 유용합니다.

http://tomahawk.sourceforge.net/. Fragroute 는 TCP/IP 를 닦고 다른 고급 테스트 http://www.monkey.org/~dugsong/fragroute/ 를 하는 것에 대한 대상호스트의 목적을 다시 쓰는데 유용합니다.

또 다른 오래된 유틸리티는 패킷 스니퍼와 함께 패킷 생성기를 통합하는 ftester (http://dev.inversepath.com/ftester/README)입니다.
비록 그것들의 툴은 오래 되었음에도 불구하고 그들은 여전히 바뀌지 않은 채로 남은 TCP/IP 의 기본개념을 오늘날에도 여전히 유지합니다.

7. 결론

IDS 설정과 함께 방화벽은 모든 규모의 네트워크에서 매우 일반적입니다. IDS 를 사용하는 것은 선택사항이지만 그 IDS 는 일반적으로 악의적인 시도에 대한 감시 트래픽 뿐만 아니라 DoS 또는 속도-제한 방지를 제공하는 많은 관리자를 위한 안락의 수준을 제공합니다.

많은 네트워크 관리자와 보안 관리자는 종종 별도의 감사 또는 테스트와 공급업체에서 하드웨어 설치를 합니다. 새로운 배포 또는 방화벽 규칙에 대한 변경과 함께 방화벽이나 IDS 의 전체 감사는 보안이 가이드에서뿐만 아니라 상업적인 도구로 도구를 사용하는지 확인하기 위해 수행되어야 합니다.

방화벽은 네트워크에 접속의 첫 번째 요점과 잠재적인 해커에 의해 찔리거나 24×7 테스트 하는 장치를 고려하여야 합니다. 적절한 구성과 규칙을 장소에 보장하는 것은 전체 네트워크의 보안을 위해 대단히 중요합니다.

관련 검색어

- tcp source port pass firewall
- firewall security test

- infosec security testing examples
- test firewall security
- hping firewall penetration test
- udp source port pass firewall
- replay packets pass thru sslstrip
- auditing firewall with nmap
- pfsec ₩₩
- nmap test firewall

저자에 관하여

"John Maher"는 웹 응용프로그램 해킹, 리눅스 보안 또한 네트워크 보안의 경험이 있는 인포섹 연구소에 대한 보안 연구원입니다. 리눅스 관리자와 오픈 소스 옹호자로서 Maher 는 고등교육과 보안과제의 다양성에 직면하는 엔터프라이즈 네트워크와 민간부문에서 근무하고 있습니다.

8. 끝맺음

http://resources.infosecinstitute.com/ 사이트에서는 다양한 해킹 공격 시연 문서 및 방어들이 정기적으로 배포되고 있습니다. 입문자들 대상으로 설명한 문서들이 많아서 연구 목적으로 번역을 시작하였습니다. 앞으로도 좋은 컨텐츠에 대해서는 정기적으로 번역을 해서 배포하도록 하겠습니다. 번역에 참여해주신 멤버들에게 감사합니다.