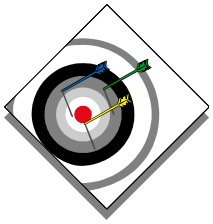

포/커/스

네트워크-기반 침입방지 시스템 성능 평가 기술 동향

전용희* 김기영** 장종수***

최근 들어 침입방지 시스템(IPS)이 차세대 보안 솔루션으로 자리를 굳히고 있다. 국내외의 보안 업체들이 IPS 를 발표하고 있는 가운데, 국내에서도 IPS 에 대한 평가인증제가 4 월부터 실시되고 있다. 본 고에서는 국내 IPS 의 공통평가기준과는 별도로, 국외에서 IPS 시험을 위한 국제 표준이 되기 위한 노력을 하고 있는 NSS 의 IPS 시험 방법론에 따른 성능 평가 항목과 성능 평가 방안을 중심으로 네트워크 기반 IPS 의 성능 평가 기술 동향에 대하여 기술한다. ▧

목 차

* ETRI 보안게이트웨이연구팀/초빙연구원
** ETRI 보안게이트웨이연구팀/팀장
*** ETRI 네트워크보안그룹/그룹장

Ⅰ. 서 론

침입방지 능력과 빠른 대응 속도를 위하여 네트워크 기반 침입방지 시스템(Network-based Intrusion Prevention System: NIPS)은 네트워크 라인상에 위치한 제품이어야 하며, 세션 기반 탐지를 지원할 수 있는 시스템이어야 한다. 그리고 시그니처, 프로토콜 비정상 행위 탐지와 같은 다양한 종류의 방식을 통하여 악의적인 세션을 차단하는 것도 필수적이다[1].

NIPS 는 공격 탐지에 기초하여 트래픽의 통과 여부에 대하여 결정을 내릴 수 있는 인라인 장치이다. 원하지 않는 트래픽을 차단할 수 있는 능력이 침입탐지 시스템(Intrusion Detection System: IDS)과의 주요한 차이점이다. NIPS 는 인라인 솔루션이기 때문에 성능, 네트워크 재설계, 가용성과 같은 다른 네트워크 사항들을 고려해야 한다.

IPS 는 무엇보다도 신뢰성이 또한 중요하다. 신뢰성은 지속적인 운영과 업무에의 적합성으로 주도되며 설계된 기능을 수행해야 한다. 궁극적으로, IPS 는 모든 적절한 트래픽은 자유로이 통과할 수 있도록 하는 반면에, 악성이나 부적절한 트래픽은 일관성 있게 차단해야 한다. 이것은 IPS 가 다음과 같은 품질을 지녀야 함을 의미한다[2].

- 고가용성: 시스템 과부하로 인하여 붕괴되지 않아야 하며, 지독한 네트워크 환경을 견디도록 구축되어야 한다.
- 고성능: 트래픽에 대하여 아무런 영향을 주지 않고 모든 패킷을 평가할 수 있어야 하며, 높은 처리율과 낮은 네트워크 지연 성능을 제공해야 한다.
- 관리성과 확장성: 효율적인 관리와 네트워크상의 트래픽을 지원할 수 있는 능력을 지녀야 한다.

본 고에서는 NSS 의 IPS 그룹 시험 결과 보고서의 내용을 중심으로 IPS 의 성능 평가 방안에 대하여 기술하고자 한다[3].

II. IPS 의 요구사항

수동적인 모드로 동작되는 IDS 에서는 없는 여러 가지 문제점이 IPS 구현에서 발생한다. 이 문제는 IPS 장치가 인라인으로 동작하도록 설계되어 단일 실패점이 될 수 있는 가능성이 있기 때문이다. 네트워크 IPS 는 네트워크 교환기와 상당히 유사하게 수행되어야 한다. 따라서 설치 전 요구사항으로 엄격한 네트워크 성능과 신뢰성 요구사항을 만족하여야 한다. 패킷 탈락(packet dropping)도 또한 문제가 된다. 만일 IPS 가 네트워크 에지에서 사용된다면, 성능 저하를 방지하기 위하여 네트워크상의 트래픽에 대한 특성화도 정확해야 한다. 평균 대역폭, 첨두율, 프로토콜의 식별, 평균 패킷 크기 및 매초마다 설정되는 신규 연결 레벨 등이 IPS 엔진에 나쁜 영향을 줄 수 있는 주요한 매개변수이다.

오탐지(false positive) 문제도 여전히 중요하다. 오탐지의 결과는 수동적인 IDS 장치에서 보다 인라인 IPS 어플라이언스에서는 훨씬 더 심각한 결과를 초래할 수 있다. 모든 기가급 IPS 장치가 가지는 다른 가능한 문제는 생성하는 경보 데이터의 양이다. 예를 들어, 비교적 낮은 경보율인 초당 10 개인 경우라도, 매시간 36,000 개의 경보가 발생되면, 매일 864,000 개의 경보가 발생되는 셈이다. 따라서 경보의 수를 절대적으로 최소로 유지하기 위하여 시그니처 셋을 정확하게 조율하는 능력이 필수적이다. 일단 경보가 발생하면 효과적으로 처리하는 것이 또한 필수적이다. 상세한 익스플로잇 정보와 패킷 콘텐츠와 데이터 스트림을 조사할 수 있는 능력을 포함

하여 향상된 경보 처리와 포렌식 평가 능력이 진정한 IPS 제품을 만들 수 있다. 효과적인 방지를 위한 IPS 의 요구사항으로 인라인 운용, 신뢰성과 가용성, 탄력성, 낮은 지연, 고성능, 확실한 탐지 정확성, 정교한 입상성 및 제어, 향상된 경보 취급 및 포렌식 평가능력과 같은 것이 있다[3].

III. IPS 성능 평가 방안

IPS 제품을 평가하기 위하여, NSS 시험 모음(test suite)은 성능과 신뢰성, 보안 정확성, 유용성 세 가지 주요 영역을 포함하고 있다[3]. 어떤 IPS 라도 신뢰성이 있어야 하며, 합법적인 트래픽을 차단하지 않아야 하며, 또한 네트워크 성능에 부당한 영향을 미치지 않아야 한다.

1. 부하 인가 시 탐지 및 차단 성능

이 그룹의 시험은 신규 TCP 연결이 빠르게 생성될 때에도, IPS 가 합법적인 트래픽에 나쁜 영향을 주지 않는다는 것을 검증한다. 이 시험에서는 또한 센서가 제조사에 의하여 지원된다고 주장되는 최대 대역폭까지 백그라운드 트래픽의 증가되는 부하에 대하여 익스플로잇을 탐지하고 차단할 수 있는지 검증한다.

센서가 기준선 공격을 탐지할 수 있는지를 보증하기 위하여 백그라운드 트래픽 없이 먼저 고정된 수의 익스플로잇이 개시된다. 일단 그것이 확립되면, 센서가 공격을 놓치는 점을 결정하기 위하여, 여러 가지 형태의 백그라운드 트래픽이 증가되면서 발생된다. 모든 시험이 장치 정격 용량의 1/4, 1/2, 3/4, 최대 용량까지의 백그라운드 트래픽으로 반복된다. 시험은 UDP, HTTP 및 혼합 프로토콜 트래픽으로 수행되며, 초당 1.48 백만 패킷까지, 초당 20,000 연결까지의 패킷율을 포함한다.

2. 지연 및 사용자 응답 시간

지연은 처리율에 대하여 상한 경계를 부과할 수 있고 대화형 애플리케이션에 또한 영향을 주고, 사용자 응답 시간에 영향을 미친다. 따라서 NIPS 에 의하여 도입되는 지연의 영향을 이해하고 최대 수용 가능한 지연을 결정하는 것이 중요하다. IPS 장치의 지연은 패킷 크기, 프로토콜의 복잡성, 공격 트래픽의 존재 혹은 그것을 통과하는 정상 트래픽의 구성에 따라서 상당히 다르다.

NIPS 의 지연은 설치되는 네트워크의 상황에서 평가되어야 한다. 교환기와 같이 코어망 장치는 대부분 다른 특성보다는 패킷 손실 및 지연과 같은 성능에 기반하여 선택된다. NIPS 가 인라인으로 동작된다면, 교환기와 유사하게 평가되는 것이 당연하다. 이 때문에, NSS 그룹 시험

방법은 애플리케이션 지연을 측정하는 이외에, 패킷 지연을 결정하기 위하여 교환기를 시험할 때 보통 채용하는 것과 매우 유사한 시험 기술을 사용한다[3].

UDP 패킷의 양방향 네트워크 지연은 세 가지 시험 조건으로 ① 부하없이, ②500Mbps 의 HTTP 트래픽(혹은 장치 정격 용량이 1Gbps 보다 작은 경우 정격 용량의 50% 부하), ③ 장치가 과도한 SYN 플러드 공격을 당할 때 측정된다.

3. 안정성 및 신뢰성

이 시험은 여러 가지 극도의 상태에서 IPS 장치의 안정성을 검증한다. 장기간 안정성이 인라인 IPS 장치에게는 매우 중요하다. 이 시험의 첫 부분에서는, 센서의 외부 인터페이스가 상당한 시간에 걸쳐서 지속적인 공격 스트림에 노출된다. 이 시험은 차단 및 경보 취급 메커니즘의 유효성에 대한 지표를 제공하기 위한 것이다. 지속적인 익스플로잇 스트림이 합법적인 세션에 혼합되어 추가적인 백그라운드 트래픽 없이 8 시간 동안 장치 처리율의 최대 90%율로 센서를 통하여 전송된다. 이 시험 기간 동안 장치는 운용적이며 안정 상태를 유지하여야 하며, 인식 가능한 익스플로잇을 100% 차단하고, 각각에 대하여 경보를 발생하고, 합법적인 트래픽 모두를 통과시켜야 한다.

시험의 두 번째 부분에서는, 시험중인 장치의 프로토콜 스택을 8 시간 동안 ISIC 시험 도구로부터 발생되는 비정상 트래픽에 노출함으로써 스트레스를 준다. 합격을 위하여 장치는 운용적이며 익스플로잇을 탐지하고 차단할 수 있어야 한다. 관리 인터페이스에 대한 시험도 수행되어야 한다.

4. 보안 유효성

가. 탐지 정확성 및 폭

이 그룹의 시험은 NIPS 가 합법적인 트래픽을 차단하지 않는지(정확성) 그리고 넓은 범위의 통상적인 익스플로잇을 탐지하고 차단할 수 있는지(폭)를 검증한다.

나. 회피 기법에 대한 저항

이 시험은 IPS 가 통상적인 회피(evasion) 기법에 대하여 기본적인 익스플로잇을 탐지하고 차단할 수 있는지를 검증하기 위함이다. 시험은 네 가지로 이루어져 있다.

- 기준선(baseline): 어떠한 회피 기법도 적용하지 않고, IPS 가 정상 상태에서 여러 가지의 통상적인 기본 공격을 탐지하고 차단할 수 있는지를 확립하기 위함이다.

- 패킷 단편화 및 스트림 분할: 19 개의 회피 기법을 사용하여 fragroute 를 통과시켜 기준선 HTTP 공격이 반복된다.
- URL Obfuscation: Whisker 웹 서버 취약성 스캐너에 의하여 만들어진 아홉 가지의 URL obfuscation 기법을 적용하여 기준선 HTTP 공격이 반복된다.
- 기타 회피 기술: 다음과 같은 7 가지의 프로토콜 혹은 익스플로잇 특정 회피 기술에 대하여 일정한 기준선 공격이 반복된다. 기본 포트 변경, FTP 명령 라인에 스페이스 삽입, FTP 데이터 스트림에 비문자 Telnet 옵코드 삽입, RPC 레코드 fragging.

다. 스테이트풀 운용

이 시험의 목적은 IPS 가 상태를 잃어버리거나 상태를 부정확하게 추론하지 않고, 다양한 트래픽 부하에서 장치를 통하여 설정된 스테이트풀 세션을 감시할 수 있는지를 결정하기 위한 것이다. TCP 세션 상태를 유지하지 않는 IPS 는 관리 콘솔을 오탐지 경보로 범람시킬 수 있다. 먼저 유효한 익스플로잇의 캡처 파일로부터 취해진 많은 패킷들을 타깃 서버와 유효한 세션을 먼저 확립하지 않고 전송한다. 이 시험에서 합격하기 위해서는 어떤 실제 익스플로잇에 대하여도 경보가 발생되지 않아야 한다. 그러나, 각 패킷은 “깨어진” 혹은 “불완전한” 세션을 나타내기 때문에 가능한 차단되어야 한다.

두 번째 시험에서는 센서가 증가하는 수의 개방 연결에서 상태를 유지할 수 있고, 상태 테이블이 다 찼을 때 합법적인 트래픽을 차단하지 않으면서 새로운 익스플로잇을 지속적으로 탐지하고 차단할 수 있는지를 시험한다.

라. 유용성

이것은 제품의 특성 및 유용성(usability)을 정성적으로 평가하는 것이다. 평가 범위는 설치, 구성, 정책 편집, 경보 취급, 보고 및 평가를 포함한다. 이 평가는 제품의 특성, IPS 설치 및 관리 콘솔과의 일상 운용이 얼마나 쉬운가를 보여준다.

IV. IPS 성능 평가

1. 시험 환경

NSS 성능 시험에 사용된 시험 환경은 다음과 같다[3].

- 네트워크: 100/1,000Mbit 이더넷

- 교환기: Allied Telesyn AT-9816GB, AT-9812T
- 모든 IPS 장비는 어플라이언스로 제공(소프트웨어인 경우, 하드웨어 플랫폼에 미리 설치)
- IPS 는 시험동안 perimeter 장치로 배치됨
- 목표 서버넷을 보호하는 방화벽은 없음
- 익스플로잇을 생성하는 기계와 같은 트래픽 생성 장비는 외부 네트워크에 연결
- 익스플로잇에 대한 목적 호스트는 내부 네트워크에 연결
- IPS 장비는 외부 네트워크의 에지에 있는 게이트웨이 교환기와 내부 네트워크의 에지에 있는 교환기 사이에 연결

2. 시험 항목

가. 탐지 엔진

센서가 오탐지에 견디면서, 광범위한 통상적인 익스플로잇을 정확하게 탐지하고 차단할 수 있는 능력을 검정하는 것이다. 이 절에서의 모든 시험은 백그라운드 네트워크 부하없이 수행된다. 최근 시그니처를 포함하여 모든 이용 가능한 공격 시그니처가 센서에 설치된다.

(1) 공격 인식

이 시험은 센서가 얼마나 정확하게 광범위한 통상적인 익스플로잇, 포트 스캔 및 서비스 거부(Denial of Service: DoS) 공격 시도를 탐지하고 차단하는가를 보여주기 위한 것이다. 모든 익스플로잇은 네트워크상에 부하없이, IP 단편화 없이 수행된다. 시험에 사용된 공격 suite 는 100 개 이상으로 다음 영역을 포함한다. 백도어, DNS, DoS, 미탐지(변경된 익스플로잇), 핑거, FTP, HTTP, ICMP, reconnaissance, RPC, SSH, Telnet, 데이터베이스, 메일 가능한 한 공격은 그들의 할당된 CVE(Common Vulnerabilities and Exposures) 참조에 의하여 식별되어야 한다. 같은 공격에 대하여 복수개의 비슷하거나 동일한 경보를 생성하면, 익스플로잇에 대한 대응이 너무 “noisy”라고 간주된다. 그리고 장치가 공격 패킷만 차단하는지 혹은 전체 “의심스러운” TCP 세션을 모두 차단하는지를 주시한다.

시험은 아래와 같은 평가를 위하여 두 번 반복된다:

- 공격 인식 평가(Attack Recognition Rating: ARR): 이 시험에서는 어떤 공격이 탐지되고 얼마나 정확하게 탐지되는지를 결정하기 위하여 센서상의 차단은 불능(disable)으로 만든다. 이는 단지 모니터 모드이다.

- 공격 차단 평가(Attack Block Rating: ABR): 이 시험에서는 어떤 공격이 탐지되거나 무슨 경보가 발생되느냐에 관계없이 어떤 공격이 성공적으로 차단되는지를 결정하기 위하여 차단을 가능하게 하고 수행된다.

기본(default) 구성 모드로는 다음과 같이 두 가지가 있다.

- 공격 인식 평가-탐지(ARR-Detect Only: ARRD): 탐지된 익스플로잇의 수/전체 익스플로잇의 수의 백분율(%)로 표시된다.
- 공격 인식 평가-차단(ARR-Block: ARRB): 차단된 익스플로잇의 수/전체 익스플로잇의 수의 백분율(%)로 표시된다.

초기 시험 후에 빠진 공격의 CVE 참조 목록이 주어지며, 각 벤더는 48 시간 안에 갱신된 시그니처 셋을 만들어서 배포해야 한다. 그리고 나서 동일하게 두 번째 시험이 수행되고 “고객(custom)” ARRD/ARRB 가 결정된다. 이것은 새로운 혹은 갱신된 시그니처를 위한 요구사항에 얼마나 효과적으로 벤더가 대응하는가를 보여준다. 기본 및 고객 ARRD/ARRB 결과가 보고된다.

(2) 오탐지에 대한 저항

이 시험의 목적은 IPS 장비에 특별히 중요한 것으로, 센서가 오탐지 경보를 얼마나 일으키는가를 보여주기 위한 것이다. 이를 위하여 의심스러운 내용을 가진 많은 정상 트래픽의 트레이스 파일을 사용한다. IPS 는 경보를 발생하지 않고 트래픽을 차단하지 않으면 모든 시험에서 통과된다. 이 시험에서 사용된 어떤 익스플로잇도 진정한 위협이 아니기 때문에 경보를 발생하면 실패한 것으로 간주된다.

나. IPS Evasion

이 부분의 목적은 센서가 여러 가지의 통상적인 회피(evasion) 기술에 대하여 기본적인 익스플로잇을 탐지하고 차단할 수 있는지를 검정하기 위함이다.

(1) 기준선 공격 재생

이 시험의 목적은 어떠한 회피 기술도 적용하지 않고, 센서가 정상 상태에서 여러 가지의 통상적인 기본 공격을 탐지하고 차단할 수 있는지를 확립하기 위함이다.

(2) 패킷 단편화 및 스트림 분할

여러 가지의 IP 단편화(fragmentation)와 TCP 분할(segmentation)을 포함하여, 다양한 회피 기술을 사용하여 기준선 HTTP 공격이 반복된다. 각 회피 기술에 대하여 다음과 같이 조사된다.

- 시도된 공격이 성공적으로 차단되었는지
- 시도된 공격이 탐지되고 어떤 형태로든 경보가 발생되었는지
- 익스플로잇이 원래 익스플로잇과 관련하여 정확한 경보를 제공하기 위하여 성공적으로 디코드 되었는지

(3) URL obfuscation

Whisker 웹 서버 취약성 스캐너에 의하여 만들어진 다음과 같은 다양한 URL obfuscation 기술을 적용하여 기준선 HTTP 공격이 반복된다. URL 인코딩, 디렉토리 삽입, 조기 URL 종료, 긴 URL, 허위 매개변수, TAB 분리, case sensitivity, 윈도 back 경계자, 세션 splicing. 각 회피 기술에 대하여 위와 동일하게 조사된다.

(4) 기타 회피 기술

다음과 같은 다양한 프로토콜 혹은 익스플로잇 특정 회피 기술에 대하여 일정한 기준선 공격이 반복된다. 기본 포트 변경, FTP 명령 라인에 스페이스 삽입, FTP 데이터 스트림에 비문자 Telnet 옵코드 삽입, 다형태 변화(ADMmutate), 프로토콜 및 RPC PROC 번호 변경, RPC 레코드 fragging. 각 회피 기술에 대하여 패킷 단편화와 스트림 분할에서처럼 조사된다.

다. 스테이트풀 운용

IPS 센서가 상태를 상실하거나 상태를 부정확하게 추론하지 않고 다양한 트래픽 부하에서 장치를 통하여 설립된 스테이트풀 세션을 감시할 수 있는지를 결정하기 위한 것이다.

(1) Stateless 공격 재생(Mid-Flows)

이 시험은 Stick 과 Snot 과 같은 상태가 없는(stateless) 공격 플러딩 도구에 센서가 저항적인지를 결정한다. Stick 과 Snot 은 유효한 소스와 목적지 주소 및 어떤 범위의 프로토콜을 사용하여 보호되는 서브넷에 대하여 타깃 서버에 연결을 설정하지 않고 많은 수의 거짓 경보를 생성하기 위하여 사용된다. 이 시험에서 타깃 서버와 유효한 세션을 먼저 설정하지 않고, 유효한 익스플로잇의 캡처 파일로부터 취해진 많은 수의 패킷을 전송한다. 그리고 센서가 유효한 연결이 만들어졌다는 것을 추론하지 못하도록 세션 해제(session tear down)와 응답 패킷을 또한 제거한다. 이 시험에서 통과되기 위하여, 어떤 실제 익스플로잇에 대하여도 경보가 발행되지 않아야 한다. 그러나 각 패킷은 “broken” 혹은 “불완전한” 세션을 나타내기 때문에 가능하면 차단되어야 한다.

(2) 동시 개방 연결(기본 세팅)

이 시험은 상태 테이블이 포화된 때, 새로운 익스플로잇을 탐지하고 차단하는 것을 계속하면

서, 센서가 증가하는 수의 개방 연결 전역에서 상태를 유지할 수 있는가를 결정하기 위함이다. 또한 이 시험은 상태 테이블이 포화된 후 센서가 합법적인 트래픽을 차단할 수 있는가를 결정하기 위하여 시도한다.

합법적인 HTTP 세션이 열리고 두-패킷 익스플로잇의 처음 패킷이 전송된다. 그리고 나서 IPS 센서의 외부 인터페이스상의 Spirent Avalanche 가 IPS 센서의 내부 인터페이스상의 Spirent Reflector 와 10,000 에서 1,000,000 까지의 다양한 수의 TCP 세션을 연다. 그리고 초기 HTTP 세션이 익스플로잇의 후반부와 함께 종료되고 세션이 닫힌다. 만약 IPS 가 설정된 처음 세션에 대한 상태를 아직 유지하고 있다면 그 익스플로잇은 기록된다. 만약 상태 테이블이 소진된다면 그 익스플로잇 스트링은 non-stateful 공격으로 간주되고 무시된다.

두개의 익스플로잇의 반쪽 모두 경보를 발생시키는 것이 요구된다. IPS 는 두 번째 패킷이 전송된 후 경보 생성이 실패하거나, 혹은 자기 스스로 익스플로잇의 각 반에서 경보를 생성하면 이 시험에 실패하는 것이 된다. 각 스텝에서 장치가 합법적인 트래픽을 차단하지 않는다는 것을 확인하면서 모든 연결이 일단 개방되면, IPS 엔진이 새롭게 개시된 익스플로잇을 여전히 탐지하고 차단할 수 있다는 것을 보증해야 한다. 이 시험은 기본 센서 설정을 사용하여 수행된다.

- 공격 탐지 및 차단: 개방 세션의 수가 만에서 백만으로 단계별로 증가될 때 센서가 새로운 익스플로잇을 계속 탐지 및 차단 할 수 있다는 것을 보증해야 한다.
- 상태 보존: 개방 세션의 수가 만에서 백만으로 단계별로 증가될 때 센서가 사전-기존 세션의 상태를 유지할 수 있다는 것을 보증해야 한다.
- 합법적인 트래픽 차단: 개방 세션의 수가 만에서 백만으로 단계별로 증가될 때 센서가 합법적인 트래픽을 차단하는 것을 시작하지 않음을 보증해야 한다.

(3) 동시 개방 연결(튜닝 후)

앞의 시험이 상태 테이블의 크기를 증가하기 위하여 벤더에 의해 권고되는 튜닝 후 반복된다. 공격 탐지 및 차단, 상태 보존, 합법적인 트래픽 차단

라. 부하에서 탐지/차단 성능

이 부분의 목적은 벤더에 의하여 지원된다고 주장된 최대 대역폭까지 증가하는 백그라운드 트래픽의 부하에서 센서가 익스플로잇을 탐지하고 차단할 수 있는지를 검증하는 것이다. 가장 최근의 시그니처 팩이 벤더로부터 얻어져, 센서들은 모든 이용 가능한 공격 시그니처를 실행 가능하게 하여 설치된다. 각 센서는 의심스러운 트래픽을 탐지 및 차단하기 위하여 구성된다.

센서가 기준선 공격을 탐지할 수 있는지를 보증하기 위하여 백그라운드 트래픽 없이 고정된 수의 익스플로잇이 개시된다. 일단 이것이 확립되면, 증가되는 레벨의 여러 가지 형태의 백그라운드 트래픽이 센서가 공격을 놓치기 시작하는 점을 결정하기 위하여, IPS 장치를 통하여 생성된다. 모든 시험은 백그라운드 트래픽의 250Mbps, 500Mbps, 750Mbps 와 1,000Mbps 로 반복된다.

탐지 및 차단 성능을 위하여 다음 두개의 율이 정의된다.

- 공격 차단율: 각 백그라운드 부하에서의 ABR 은 차단 모드에 있을 때 센서에 의하여 차단되는 익스플로잇 수의 백분율로 표현된다.
- 공격 탐지율(Attack Detection Rate: ADR): 각 백그라운드 부하에서의 ADR 은 차단 모드를 불능시키고 센서에 의하여 탐지되는 익스플로잇 수의 백분율로 표현된다.

각 형태의 백그라운드 트래픽에 대하여, IPS 가 패킷을 탈락시키고 경보를 놓치기 시작하기 전에 견딜 수 있는 최대 부하를 또한 결정해야 한다. 이 시험에서 100% ABR 이지만 100% 미만의 ADR 을 보여주는 장치는 유사한 부하들에서 합법적인 트래픽을 차단하기 쉽다는 것은 주목할 만하다.

(1) 임의의 유효한 포트에 대한 UDP 트래픽

이 시험의 목적은 IPS 장치의 원래 패킷 처리 능력을 결정하기 위함이며, 다음과 같이 세 가지 형태로 수행된다. 시험은 모두 250Mbps, 500Mbps, 750Mbps 및 1,000Mbps 백그라운드 트래픽을 가지고 반복된다.

- 64 바이트 패킷-초당 최대 1,480,000 패킷: 어떤 실제 네트워크에서도 초당 거의 1,500,000 개의 64 바이트 패킷을 볼 수 없기 때문에 “고문 시험”이라고 불려진다. 그러므로 이 시험은 가장 극도의 조건 하에서 패킷 처리 능력을 측정한다.
- 440 바이트 패킷-초당 최대 260,000 패킷: 이 시험은 실제 네트워크에서와 유사한 평균 패킷 크기를 사용하여, 실제 패킷 혼합과 비교하기 위하여 수행된다. 이 시험에서는 어떠한 세션도 생성되지 않으며 탐지 엔진이 프로토콜 평가면에서 거의 할 일이 없다. 이 시험은 평균적인 네트워크상에서 와이어로부터 패킷을 처리하는 장치 능력의 합리적인 지표를 제공한다.
- 1,514 바이트 패킷-초당 최대 81,720 패킷: 이 시험은 64 바이트 패킷 시험의 완전한 반대이다. 이 시험을 통하여 대형 패킷을 사용하여 좋은 결과를 얻는 것이 쉬움을 보여줄 수 있다.

(2) 거래 지연 없는 HTTP "최대 스트레스" 트래픽

이 시험의 목적은 HTTP 탐지 엔진에게 부담을 주어 가변적인 평균 패킷 크기와 가변적인 초당 연결의 네트워크 부하 하에서 어떻게 센서가 익스플로잇을 탐지하고 차단하는가를 결정하기 위한 것이다. 가변적인 세션 길이를 가진 순수한 세션-기반 트래픽을 생성함으로써 IPS 는 유효한 세션을 추적해야 하며, 그리하여 단순한 패킷-기반 백그라운드 트래픽보다 더 높은 작업 부하를 확보한다. 이것이 실험실 환경에서 얻을 수 있는 가능한한 실제 세계에 가까운 시험 환경을 제공한다. 각 거래는 하나의 HTTP GET 요구로 구성되며 거래 지연은 없다. 즉, 웹 서버가 모든 요구에 대하여 즉시 응답한다.

이 시험은 네 가지 형태로 수행되며 250Mbps, 500Mbps, 750Mbps 및 1,000Mbps 의 백그라운드 트래픽으로 반복된다.

- 초당 최대 2,500 신규 연결-평균 패킷 크기 1200 바이트-초당 최대 100,000 패킷: 상대적으로 낮은 연결율과 큰 패키 크기로, 모든 IPS 센서는 이 시험에서 100% 차단율을 성취해야 한다.
- 초당 최대 5,000 신규 연결-평균 패킷 크기 540 바이트-초당 최대 230,000 패킷: 평균 연결율과 평균 패키 크기로, 이것은 실제 네트워크의 좋은 근사화로, 모든 IPS 센서는 이 시험에서 좋은 성능을 성취해야 한다.
- 초당 최대 10,000 신규 연결-평균 패킷 크기 440 바이트-초당 최대 280,000 패킷: 매우 높은 연결율과 평균 패킷 크기를 결합한 것으로, 이것은 모든 IPS 센서에게 힘든 시험이며, 매우 심하게 사용되는 실제 네트워크를 나타낸다.
- 초당 최대 20,000 신규 연결-평균 패킷 크기 350 바이트-초당 최대 360,000 패킷: 작은 패킷 크기와 극도로 높은 연결율로, 이것은 어떤 IPS 센서에게도 극도의 시험이다. 이 시험의 모든 레벨에서 많은 센서들이 수행을 잘하지 못할 것이다.

(3) 거래 지연 있는 HTTP "최대 스트레스" 트래픽

이 시험은 각 거래에 대한 서버 응답에서 10 초 지연을 도입하는 것을 제외하고 앞의 시험과 동일하다. 이것은 시험을 통하여 높은 수의 개방 연결을 유지하는 효과를 가지며, 그리하여 센서가 그런 연결을 추적하기 위하여 부가적인 자원을 사용하도록 한다. 이 시험은 다음과 같이 두 가지의 형태로 수행되며, 250Mbps, 500Mbps, 750Mbps 및 1,000Mbps 의 백그라운드 트래픽으로 반복된다.

- 초당 최대 5,000 신규 연결-평균 패킷 크기 540 바이트-초당 최대 230,000 패킷-10 초

거래 지연-최대 50,000 개방 연결: 평균 연결율과 평균 패킷 크기로, 이것은 실제 네트워크의 좋은 근사화로, 모든 IPS 센서는 이 시험에서 잘 수행하여야 한다.

- 초당 최대 10,000 신규 연결-평균 패킷 크기 440 바이트-초당 최대 280,000 패킷-10 초 거래 지연-최대 100,000 개방 연결: 매우 높은 연결율과 평균 패킷 크기가 결합된 것으로, 이것은 어떤 IPS 센서에게도 힘든 시험이며, 심하게 사용되는 실제 네트워크를 나타낸다.

(4) 프로토콜 혼합 트래픽

앞의 두 시험은 가변적인 연결율과 평균 패킷 크기를 가진 순수한 HTTP 환경을 제공하는 반면에, 이 시험의 목적은 정확하게 반복 가능하고 일관성 있는 백그라운드 트래픽 부하를 여전히 유지하면서 추가적인 프로토콜을 도입함으로써 실제 환경에 더욱 유사하게 만들기 위함이다. 결과는 이전의 시험보다는 덜 힘든, 심하게 사용되는 "정상(normal)" 실제 네트워크상에서 발견될 수 있는 것에 더욱 가까운 백그라운드 트래픽 부하이다.

- 72% HTTP 트래픽(560 바이트 패킷) + 20% FTP 트래픽 + 6% UDP 트래픽(256 바이트 패킷) 초당 최대 380 신규 연결-평균 패킷 크기 555 바이트-초당 최대 22,000 패킷-최대 136 개방 연결. 더 낮은 연결율, 평균 패킷 크기와 통상적인 프로토콜 혼합으로, 이것은 심하게 사용되는 실제 네트워크의 좋은 근사화이며, 모든 센서가 이 시험에서 잘 수행하여야 한다. 시험은 250Mbps, 500Mbps, 750Mbps 및 1,000Mbps 의 백그라운드 트래픽으로 반복된다.

(5) "실제" 트래픽

이 시험은 실험실 조건에서 진정한 실제 환경에 가능한한 가깝게 되도록 하기 위함이다. 이 시험을 위하여 기가비트 인터페이스를 가진 웹 서버를 설치한다. 이 서버는 950Mbps 의 트래픽을 처리할 수 있다. 그리고 나서 메뉴 페이지, 긴 문자-기반 보고서 및 복수의 그래픽 이미지의 혼합을 접근하면서, 웹 사이트상의 대표적인 클라이언트 브라우징 세션을 캡처한다. 그리고 Avalanche 로 하여금 초당 최대 25 개의 신규 사용자로부터의 복수의 동일한 세션을 재생하게 한다.

이전의 시험들이 매우 예측 가능하고, 변하지 않는 일관성 있고 반복 가능한 백그라운드 부하인 반면에, 이번 시험의 성질은 트래픽이 특성상 훨씬 더 버스티(bursty)하다는 것을 의미한다.

이 시험은 두 가지 형태로 수행되며, 250Mbps, 500Mbps, 750Mbps 및 1000Mbps 의 백그라운드 트래픽으로 반복된다.

- 순수 HTTP 트래픽(웹 사이트상에서 시뮬레이트된 브라우징 세션): 초당 최대 100 신규 연결- 초당 25 신규 사용자- 평균 패킷 크기 1,000 바이트- 초당 최대 110,000 패킷.

세션마다 복수의 거래로 이루어진 진정한 브라우저 세션에 대한 진정한 서버 응답으로, 이것은 비록 순수한 HTTP 이지만, 전형적인 실제 백그라운드 부하이다. 웹 서버와 네트워크가 더 높은 트래픽 부하에서 극도로 바쁠지라도, “정상” 연결율과 패킷 크기로 이 시험의 모든 부하 레벨에서 대부분의 IPS 센서들이 잘 수행하도록 해야 한다.

- 프로토콜 혼합(72% HTTP 트래픽 + 20% FTP 트래픽 + 6% UDP 트래픽(256 바이트 패킷)): 초당 최대 550 신규 연결- 평균 패킷 크기 900 바이트- 초당 최대 130,000 패킷- 최대 11,000 개방 연결. FTP 와 UDP 트래픽과 함께 혼합된, 세션당 복수의 거래들로 구성된 진정한 브라우저 세션에 대한 진정한 서버 응답을 가지고 있는, 전형적인 실제 백그라운드 부하이다. 웹 서버와 네트워크는 더 높은 트래픽 부하에서는 극도로 바쁠지라도, “정상” 연결율과 패킷 크기로 이 시험의 모든 부하 레벨에서 대부분의 IPS 센서들이 잘 수행하도록 해야 한다.

마. 지연 및 사용자 응답 시간

이 부분의 목적은 다양한 부하 조건 하에서 IPS 센서가 통과하는 트래픽에 대하여 가지는 영향을 결정하기 위함이다.

(1) 지연

IPS 어플라이언스를 통하여 복수의 트래픽 플로우를 생성하고 센서를 통한 기본 처리율, 패킷 손실, 지연을 측정한다. 이 시험은 실제 네트워크 트래픽을 나타내지는 않지만, 센서가 자신을 통과하는 트래픽 플로우에 얼마나 많은 영향을 미치는가에 대한 지표를 제공한다. 이 데이터는 네트워크 안의 주요한 지점에 위치할 어떤 형태의 인-라인 장치의 영향을 측정할 필요가 있는 네트워크 관리자에게 특별히 유용하다.

양방향으로 250Mbps 에서 1Gbps 까지, 250Mbps 단위로 트래픽 부하를 변경하면서 여러 번 시험을 반복하게 된다. 이것은 다른 IP 주소와 포트를 가지고 여러 가지 패킷 크기(64 바이트, 440 바이트, 1,518 바이트)의 UDP 트래픽에 대하여 반복된다. 시험의 각 반복에서 평균 및 최대 지연과 함께, 탈락된 패킷 수를 기록한다. 이 시험은 세 가지 형태로 수행된다.

- 백그라운드 트래픽 없는 지연: 패킷 손실과 평균 지연이 각 패킷 크기와 각 부하 레벨에서 기록된다.
- 백그라운드 트래픽 부하가 있는 지연: IPS 센서를 통하여 고정된 양의 백그라운드 HTTP 트래픽을 생성하기 위하여 구성된다. 이것은 시험 중인 장치의 정격 대역폭의 50%까지이며, 최대 500Mbps- 초당 최대 2,500 신규 연결- 평균 패킷 크기 540 바이트- 초당 최

대 115,000 패킷에 해당한다. 그런 후 다양한 패킷 크기(64 바이트, 440 바이트, 1,514 바이트)에서 250Mbps 부하(125Mbps 양방향)의 트래픽이 장치를 통과하며, 패킷 손실과 평균 지연이 기록된다.

- 공격 받을 때의 지연: 시험 중인 장치의 최대 정격 대역폭 10%의 고정된 DOS/DDOS 트래픽 부하를 생성한다(최대 100Mbps). 그런 후 다양한 패킷 크기(64 바이트, 440 바이트, 1,514 바이트)에서 250 Mbps 부하(125Mbps 양방향) 트래픽이 장치를 통과하며, 패킷 손실과 평균 지연이 기록된다.

(2) 사용자 응답 시간

이 시험에서는 장치를 통하여 HTTP 세션을 발생시켜, 지연의 증가가 실패된 연결과 증가된 웹 응답 시간 측면에서 어떻게 사용자 경험에 영향을 미치는가 측정하기 위하여 사용된다. 이 시험은 다음과 같이 두 가지 형태로 수행된다.

- 백그라운드 트래픽 없는 웹 응답: 시험 중인 장치의 최대 정격 대역폭의 50%까지 HTTP 트래픽을 발생하기 위하여 구성된다. 이것은 최대 500 Mbps- 초당 최대 2,500 신규 연결- 평균 패킷 크기 540 바이트- 초당 최대 115,000 패킷에 해당한다. 정상 트래픽 조건에서 기대되는 응답 시간의 지표를 제공하기 위하여 최소, 최대 및 평균 페이지 응답 시간과 실패된 연결의 수가 기록된다.
- 공격 받을 때의 웹 응답: 위와 같이 IPS 센서가 구성되고, 시험 중인 장치의 최대 정격 대역폭 10%까지 고정된 DOS/DDOS 트래픽 부하를 생성한다(최대 100Mbps). IPS 장치가 공격 받을 때 기대되는 응답 시간의 지표를 제공하기 위하여 최소, 최대 및 평균 페이지 응답 시간과 실패된 연결의 수가 기록된다.

바. 안정성 및 신뢰성

이 시험은 다양한 극도의 조건에서 시험하는 장비의 안정성을 검증하기 위함이다. 장기간 안정성은 인-라인 IPS 장치가 고장나면 네트워크가 정지되기 때문에 특별히 중요하다. 이 시험은 다음과 같이 세 가지 형태로 수행된다.

- 확장된 공격을 받을 때 차단: 이 시험은 차단 성능의 일관성 의미에서 단순히 신뢰성 시험을 위한 것이지 트래픽 부하 관점에서의 스트레스 시험을 위한 것은 아니다. 약간의 합법적인 세션과 혼합된 연속적인 익스플로잇 스트림이 추가적인 백그라운드 트래픽 없이 8 시간 동안 최대 100Mbps 로 전송된다. 이것은 초당 최대 50,000 패킷, 120~350 바이트 범위 안의 평균 패킷 크기에 해당한다.

이 시험은 차단과 경보 취급 메커니즘의 효율성에 대한 지표를 제공한다. 장치는 이 시험을 통하여 운용적이며 안정을 유지해야 하며, 100%의 인식 가능한 익스플로잇을 차단하고, 각각에 대하여 경보를 생성해야 한다. 결과는 단순한 통과/실패로 나타낸다. 만일 어떤 인식 가능한 익스플로잇이 트래픽 양이나 어떤 이유에서든지 IPS 장비의 개방 실패로 인하여 통과된다면, 이것은 결과적으로 실패가 된다.

- 확장된 공격을 받을 때 합법적인 트래픽 통과: 이 시험은 위와 동일한 외부 인터페이스 조건에서 수행된다. 장치는 이 시험을 통하여 운용적이며 안정을 유지해야 하며, 100% 합법적인 트래픽을 통과시켜야 한다. 결과는 단순한 통과/실패로 나타낸다. 만일 어떤 합법적인 트래픽이 트래픽 양이나 어떤 이유에서든지 IPS 장비의 닫힘 실패로 인하여 차단된다면, 이것은 결과적으로 실패가 된다.
- ISIC/ESIC/TCPSIC/UDPSIC/ICMPSIC: 이 시험은 시험 중인 장치의 프로토콜 스택을 ISIC 시험 도구로부터의 트래픽에 노출시켜 스트레스를 시도한다. 트래픽 부하는 최대 350Mbps 이며 초당 60,000 패킷이다. 평균 패킷 크기는 690 바이트를 사용한다. 결과는 단순한 통과/실패로 나타낸다. 장치는 시험을 통과하기 위하여 시험 동안 운용적으로 남아 있어야 하며, 익스플로잇을 탐지하고 차단할 수 있어야 한다.

사. 관리 및 구성

이 부분의 목적은 공격에 저항하기 위하여 시험 받는 장치상의 관리 포트의 능력과 함께, 관리 시스템의 특징을 결정하기 위함이다.

(1) 관리 포트

센서에 의하여 수집된 경보 데이터를 관리하는 능력은 IDS/IPS 시스템의 주요한 부분이다. 이런 이유로, 공격자는 탐지 인터페이스가 아닌 장치의 관리 인터페이스를 공격하는 것이 더욱 효과적이라고 결정할 수 있다. 관리 네트워크에 대한 접근이 주어지면, 이 인터페이스는 흔히 탐지 인터페이스보다 더욱 분명하고 쉽게 파괴될 수 있다. 그렇다고 관리 인터페이스를 불능화 시키면, 관리자는 공격 받고 있는 네트워크를 알 수 있는 방법이 없다.

- 개방 포트 시험: 관리 인터페이스상의 개방 포트와 활성 서비스를 스캔하고 알려진 취약성에 대하여 보고를 해야 한다.
- ISIC/ESIC/TCPSIC/UDPSIC/ICMPSIC: 이 시험은 시험 중인 장치 관리 인터페이스의 프로토콜 스택을 ISIC 시험 도구로부터의 트래픽에 노출시켜 스트레스를 시도한다. 트래픽 부하는 최대 350Mbps 이며 초당 60,000 패킷이다. 평균 패킷 크기는 690 바이트를 사용

한다. 결과는 단순한 통과/실패로 나타낸다. 장치는 시험을 통과하기 위하여, (a)시험 동안 운용적으로 남아 있어야 하며 익스플로잇을 탐지하고 차단할 수 있어야 한다. (b) 시험 기간 동안 관리 서버/콘솔과 양방향으로 통신할 수 있어야 한다. 관리 포트를 목표하는 ISIC 공격도 센서에 의하여 탐지되는지를 조사해야 한다.

V. 맺음말

침입탐지 시스템을 이용한 보안 관리의 한계를 극복하기 위하여 국내에서도 침입방지 시스템의 도입에 대한 관심이 증대되고 있으며, IPS 로의 자연스러운 이동이 거부할 수 없는 대세로 보여진다[4]. 먼저 IPS 의 도입이 이루어지기 전에 제품에 대한 성능 평가가 이루어져야 한다. 그러나, IPS 제품의 성능 시험이 매우 어려운 것이 사실이다. 2003 년의 조사 결과에 의하면, 잠재 수요처로 볼 수 있는 통신부문을 제외한 국내 공공, 교육, 일반 금융 부문에서 각 50 개사를 선정, 총 200 개에 대하여 설문조사를 실시한 결과, 67%의 응답자들이 성능이 검증되면 IPS 를 도입할 것이라고 대답한 결과를 보여준다[5].

국내에서도 침입방지 시스템에 대한 평가인증제가 실시되고 있지만, 국내 보안 제품이 세계 시장에서 경쟁력을 가지기 위하여는 IPS 제품 성능 평가 방법의 사실상의 국제적인 표준이 되기 위하여 노력하고 있는 NSS 의 시험 방법론에 따른 성능 기준에 대하여도 관심있게 보아야 할 것으로 생각된다[3]. 이에 따라 본 고에서는 NSS 에서 수행한 IPS 의 성능 평가 방안을 기초로 성능 평가 기술 동향에 대하여 기술하였다.

향후, 본 고에서 기술된 시험 방법론을 기초로 국내에서 개발하고 있는 고성능 보안 게이트웨이 시스템에 대한 성능 평가 방법론을 개발하여 성능 시험을 수행할 예정이다. 국내의 IPS 에 대한 공통평가기준과 비교를 해보는 것도 향후 과제가 될 수 있다.

<참 고 문 헌>

[1] 정보흠, 김정녀, 손승원, “침입방지 시스템 기술 현황 및 전망,” 주간기술동향 통권 1098 호, 2003. 6. 3.

[2] Pete Lindstrom, Intrusion Prevention Systems(IPS): Next Generation Firewalls, A Spire Research Report, Spire Security, Mar. 2004.

[3] An NSS Group Report V 1.0, Intrusion Prevention Systems(IPS), Group Test, NSS, Jan., 2004.

[4] 전용희, 류걸우, 장종수, “침입탐지 시스템과 침입방지 시스템의 기술 비교 및 동향,” 주간기술동향 통권 1149 호, 2004. 6. 9, pp13-24.

[5] 심상현, IPS, 허구인가 진실인가, 정보보호 21C, 2003 년 8 월호.