|  |
| --- |
| **WhiteHat School 1기**  포트 스캐닝 취약점 대안 |

Team: 과부화

Writer: 정진교

**취약점**

포트 스캐닝을 통해 쉽게 얻을 수 있는 열려있는 포트로 인해서 개발자들이 설정해 둔 일정 포트에서의 백엔드 관련 파일들을 얻어낼 수 있었다.

**보안대책**

1. Port Knocking, 포트 노킹을 이용하여 방화벽 포트를 닫아 서버를 보호하는 방법이다.

서버는 닫혀 있는 포트에 대해 패턴을 설정하며 클라이언트는 닫혀있는 포트에 대해 특정 패턴을 연결 요청하게 되면 서버의 특정 포트를 개방하거나 폐쇄할 수 있다.

포트 스캐닝 툴을 이용해 개방된 포트가 노출될 수 있을 때 이를 숨기고자 사용한다.

Port Knocking, 포트 노킹을 설정하는 방법

- knockd 설치하기(sudo apt-get install knockd)

- iptables에서 개방 포트 막기(간단한 예시)

```bash

ubuntu @ ubuntu123 ~

- $ > sudo iptables -A INPUT -p tcp --dport 22 -j DROP

ubuntu @ ubuntu123 ~

- $ > sudo iptables -L

Chain INPUT (policy ACCEPT)

target prot opt source destination

DROP tcp -- anywhere anywhere tcp dpt:ssh

```

파일 설정하기, /etc/knockd/conf 예)

[options]

UseSyslog

[openSSH]

sequence = 22, 80, 5000

seq\\_timeout = 5

command = /sbin/iptables -A INPUT -s $IP$ -p tcp --dport 22 -j ACCEPT

tcpfalgs = syn

[closeSSH]

sequence = 5000, 80, 22

seq\\_timeout = 5

command = /sbin/iptables -D INPUT -s $IP$ -p tcp --dport 22 -j ACCEPT

tcpflags = syn

[OpenSSH]

sequence - 특정 포트를 열기 위한 패턴, 22, 80, 5000 이므로 순서대로 요청

seq\_timeout - sequence의 패턴을 입력하는 시간, seconds 단위이므로 설정에서는 5초

command - sequence가 seq\_timeout 내에 성공했을 때 실행되는 명령어

- iptables를 명령어를 이용하여 특정 IP 특정 포트를 개방 혹은 폐쇄 가능

tcpflags - sequence 패킷을 어떤 방식으로 지정할 것인지 지정하는 옵션

- 위 옵션에서는 syn 패킷을 받을 때 인식

[CloseSSH] - OpenSSH와 반대로 sequence 패턴이 입력되었을 때 포트를 닫음

2. IDS (Instrusion Detection System)  
IDS란 침입 탐지 시스템이다.  
네트워크에서 사용되는 자원의 무결성, 비밀성, 가용성을 저해하는 비정상적인 사용과 오용, 남용 등의 행위를 가능한 한 실시간으로 탐지하여 관리자에게 경고 메세지를

보내주고 대응하는 시스템을 말한다.

IDS의 특징  
A. 내, 외부망의 접속점에 위치하여 방화벽의 부족한 부분을 보강하기 위해 사용되는

침입탐지 시스템  
B. IDS 도구의 기본 목적은 네트워크 상에서 발생하는 의심스러운 행동을 발견하고

관리자에게 경고음 전달  
C. 시스템의 침해여부를 보기위해 액세스 로그들을 조사하여 파일을 분석하는

시스템으로 활용됨  
  
2. IPS (Intrusion Prevention System)  
IPS란 침입 방지 시스템이다.  
다양하고 지능적인 침입기술에 대항해 다양한 방법의 보안기술을 이용하여 침입이

일어나기 전에 실시간으로 침입을 막는 시스템이다. 침입탐지가 목적인 IDS의 기능을 넘어서 침입을 탐지했을 경우에 대한 대처까지 수행한다.

IPS의 특징  
A. 방화벽은 IP주소 또는 포트에 의해 네트워크 공격을 차단할 수 있지만

IPS는 응용프로그램 수준의 공격과 패턴에 대해서 대응 가능하다.  
B. 실시간으로 탐지만하는 것 뿐만이 아니라 알려지지않은 공격까지도 방어할 수 있는

침입방지 시스템이다.

|  |  |  |  |
| --- | --- | --- | --- |
| 구분 | Firewall | IDS | IPS |
| 목적 | 접근통제 및 인가 | 침입 여부의 감지 | 침입 이전의 방지 |
| 특징 | 수동적 차단 내무망 보호 | 로그, Signature 기반의 패턴 매칭 | 정책, 규칙 DB 기반의 비정상행위 탐지 |
| 장점 | 엄격한 접근 통제 | 실시간 탐지 사후분석 대응기술 | 실시간 즉각 대응 세션 기반 탐지 가능 |
| 단점 | 내부자 공격 취약 네트워크 병목현상 | 변형된 패턴에 대해서는 탐지가 어려움 | 오탐 현상 발생 가능 장비 고가 |

3 . 포트 무작위화

- 포트 범위를 결정

- 지정된 범위 내에서 임의의 포트 번호를 생성하는 함수 또는 스크립트 생성

- 생성된 포트 번호 풀에서 임의의 포트 번호를 할당하도록 설정. (서버 소켓 바인딩을 처리하는 구성이나 코드를 업데이트하여 수행 가능)

4. 포트 허니팟 생성

- 허니팟(honeypot) 또는 허니 포트(honey pot)는 비정상적인 접근을 탐지하기 위해

의도적으로 설치해 둔 시스템을 의미한다. 공격자만 접근할 수 있는 가짜 서비스나 개방형 포트를 만들어 실제 시스템을 노출시키지 않고도 공격자의 행동과 의도에 대한 정보를 수집할 수 있다

5. 네트워크 주소 변환(NAT):

- NAT(Network Address Translation)를 활용하여 내부 네트워크 구조를 숨깁니다. NAT를 사용하면 내부 IP 주소가 단일 외부 IP 주소로 변환되므로 공격자가 개별 호스트나 열린 포트를 식별하기가 더 어려워진다.