분산 허니넷을 활용한 내부공격 탐지 방안에 관한 연구

김민정*, 박형민**, 유진호***
* ***상명대학교 경영학과
**상명대학교 지식보안경영학과
e-mail: *korea.minjeong@gmail.com
**sortms2@naver.com
***jhyoo@smu.ac.kr

Design for Attack Detection Methods Utilizing Distributed Honeynet

Min-Jeong Kim*, Hyoung Min Park**, Jinho Yoo***
* ***Dept of Business Administration, Sangmyung University
**Dept of Security Management, Sangmyung University

요 약

허니넷이란 공격자에게 인위적으로 침해된 후 공격자의 행동을 관찰할 수 있는 정보보호 체계 중 하나로 사전에 취약한 자원을 준비하여 공격자가 외부에서 접근할 수 있도록 구축하는 것이 일반적이다. 하지만 최근 사이버 공격은 외부에서 발생하기보다는 내부에 좀비PC를 만든 후 내부 경유지로 활용하여 공격하는 것이 추세이다. 따라서 기존 허니넷으로는 내부 경유지를 활용한 공격에 적극적으로 대응할 수 없는 것이 현실이다. '11년 농협 전산망 마비 사태의 경우 유지보수 업체의 PC가 내부 경유지로 활용되어 기업 내부망에 침입한 사례로 공격자는 내부 스캔을 통해 주요 자원을 식별하여 사이버 공격을 수행하였다. 이처럼 내부 경유지를 활용한 공격의 시작점은 내부 스캔단계로 사전에 이를 식별할 수 있다면 많은 피해를 사전에 예방할 수 있을 것이다. 이에 본 논문에서는 내부 스캔공격을 식별할 수 있는 Simple 허니팟을 구현하고 이를 활용한 분산 허니넷을 구축하여 내부공격에 대한 효과적인 대응방안에 대하여 제안하고자 한다.

1. 서론

우리는 현재 외부로부터 발생하는 위협에서 내부의 자산을 보호하기 위해 다양한 보호장비를 사용하고 있다. 그러나 침해의 유형이 다양해지고 기관 및 기업의 내부망 침투를 위해 내부 사용자를 경유지로 활용하는 공격이 증가함에 따라 기존의 대응방식으로 공격자를 적극적으로 식별하기에는 어려움이 있다.

2014년 한수원 해킹, 2013년 방송사와 금융사의 전산망 마비, 2011년 농협의 전산망 마비, SK컴즈 개인정보 유출 사건 등은 APT(Advanced Persistent Threat) 공격으로 인한 피해사례이다. 이러한 APT 공격은 공격자가 불특정 다수를 대상으로 제로데이(Zero-Day) 취약점, 루트킷과 같은 보안 위협을 이용하여 악성코드를 유포해 특정 기관의 내부에 침투해 은밀히 정보를 빼돌리는 킬체인(Kill Chain)을 생성한다[1]. 그리고 내부를 스캔하여 장악할 내부 자산을 식별하고 2차 공격을 통해 장악하게 된다.

이 때 공격자가 내부에 침투하여 스캔을 수행하는 과정을 탐지한다면 피해는 최초 감염자(감염자산)에서 차단할 수 있을 것이다. 그러나 스캔공격을 탐지하지 못한다면 2·3차 피해가 발생할 수 있다.

이에 본 논문에서는 내부 스캔공격을 탐지하기 위한 개선된 분산 허니넷 구축 방안에 대하여 기술하고 성능을 검증한 후 내부 스캔공격에 대응하기 위한 개선된 대응절차에 대하여 제안하고자 한다.

2. 기존연구

2.1 포트 스캔공격 대응 방안

포트 스캔공격에 대응하기 위한 첫 번째 방안은 네트워크 장비의 ACL을 이용하여 필터링하는 방법이다[2]. ACL은 장비에 접근할 수 있는 IP에 대하여 정의한 목록으로 ACL에 포함되어 있지 않은 공격자의 접근에 대해선 응답하지 않아 피해를 사전에 방지할 수 있다.

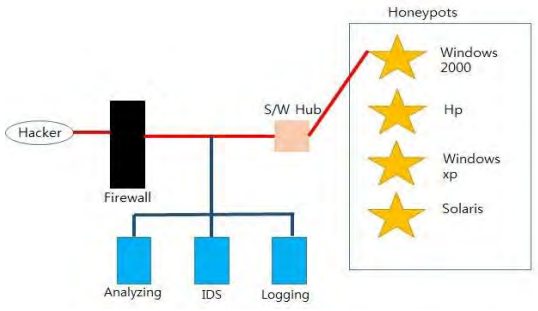
포트 스캔공격에 대응하기 위한 두 번째 방안은 서버의 불필요 서비스를 종료하는 방법이다. 서버 내 불필요 서비스를 종료하면 포트 스캔공격에 응답하지 않으므로 취약한 서비스를 차단하여 공격자로부터 사전에 공격을 예방하는 방법이다[2].

마지막 세 번째 방법은 IPS와 같은 정보보호 장비를 사용하여 스캔공격을 식별하는 방법이다. IPS와 같은 정보보호 장비는 스캔공격을 탐지할 수 있으며 탐지된 정보를

활용하여 공격자의 IP를 즉시 차단할 수 있다.[2]

2.2 허니넷의 구성

허니넷은 인위적으로 공격자의 공격을 유도해서 공격자의 신분을 확인하기 위해 사용하는 정보보호 체계의 일종이다. 일반적인 허니팟은 바이러스와 같은 외부 침입에 직접적으로 대응하는 동시에 실제서버로 위장한 허니팟 서버를 활용하여 공격자를 유인 및 장기간 관찰해 해킹경로와 해킹수법을 알아낸다[3].



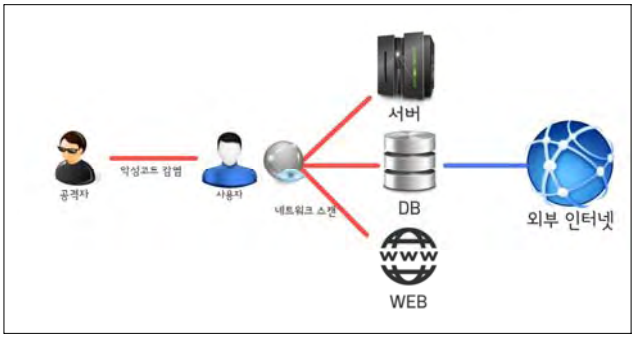
(그림 1) 허니넷의 구성

허니넷의 구성은 위험정보를 식별하기 위해 구성된 취약한 자원인 허니팟과 이를 관리하기 위한 허니 방화벽으로 구성되어 있다. 취약한 허니팟을 공격자에게 노출시켜 공격을 시도한 패킷 및 흔적을 모아서 공격자를 식별할 수 있다. 연구 분석용으로 많이 사용되고 있다[4].

3. 내부자 스캔공격 식별 방안

3.1 Simple 허니팟

내부자가 악성코드에 감염되어 공격자의 경유지로 활용된 후 내부 네트워크에 스캔공격 수행 시 사용하는 도구로 NMAP[5]이 있다. NMAP은 네트워크 대역에 활성화된 호스트를 식별하고 사용 중인 서비스를 확인하는 도구로 NMAP이 사용하는 스캔 기법은 TCP, UDP, ICMP 등의 다양한 프로토콜을 사용하여 활성화 여부를 식별한다.

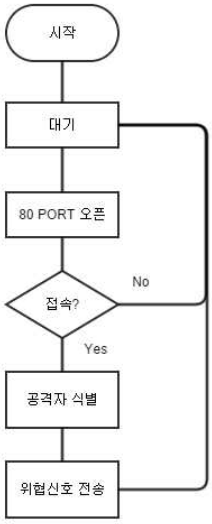


(그림 2) 내부 경유지를 활용한 스캔 공격

예를 들어 내부에 좀비PC를 확보한 공격자는 사용자의 내부 네트워크 구조를 정확하게 식별하기 위해 서비스가 주로 사용하는 포트인 22, 25, 80번과 같은 기본 서비스 포트를 탐지한 후 식별된 서비스의 취약점을 활용하여 공격을 수행한다.

이때 내부 스캔공격자의 대응방안으로 주요 포트를 활성화 한 Simple 허니팟을 제안한다. Simple 허니팟은 단순히 주요 포트만 활성화하고 응답은 하지 않는다. 하지만 주요 포트에 접속이 인지되면 어느 PC에서 접속하였는지를 확인하여 스캔공격을 탐지한다.

따라서 내부 네트워크에서 발생하는 스캔공격은 불법으로 주요 포트를 활성화 한 Simple 허니팟을 이용하면 내부 공격자에 대하여 적극적으로 대응할 수 있다.



(그림 3) Simple 허니팟 구동 알고리즘

다음은 Python언어를 활용한 기본적인 Simple 허니팟의 탐지분야 소스코드이며 Python을 지원하는 스틱PC(라즈베리파이)를 사용하여 구현하였다[8].

```
import socket
s = socket.socket
    (socket.AF_INET, socket.SOCK_STREAM)
s.bind(("127.0.0.1", 80))  # 웹 기본포트 80번 OPEN
s.listen(1)
conn, addr = s.accept()
print 'Attack by', addr
conn.close()
```

(그림 4) Simple 허니팟 탐지 소스코드

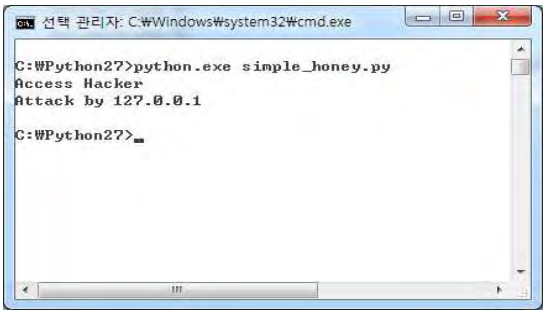
3.2 Simple 허니팟 검증

실험환경으로 가상의 네트워크 상 공격자와 Simple 허니팟 두 대의 PC를 구축하여 검증하였다.

실험순서는 사전에 웹 접속포트인 8080번 포트를 활성화한 Simple 허니팟을 구동시킨 후 공격자로 가장하여 8080번 포트에 접속 시 공격여부를 식별하는지를 확인하였다.

(그림 5) Simple 허니팟 검증 시나리오

실험결과 공격자가 공개되어 있는 웹포트에 접근하자 공격자의 IP를 출력하며 공격자의 접근을 알려주는 것을 확인할 수 있다.



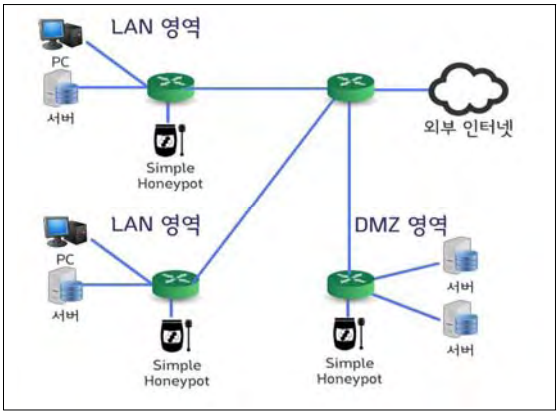
(그림 6) Simple 허니팟의 공격 탐지 예

4. 분산 허니넷 구축 방안

4.1 분산 허니넷

일반적인 허니넷은 보호하고자 하는 도메인의 서버를 가상으로 복사하여 공격자가 침투 시 정상적인 네트워크가 아닌 가상의 허니넷을 보여준 후 지속적으로 추적하는 시스템이다. 이러한 허니넷의 운용 효율성을 증가시키기 위해 가상의 환경, 하이브리드 환경들을 이용하여 구축하기도 한다. 하지만 기존의 허니넷은 가상의 서버를 구현하기 위해 많은 노력이 필요하며 서버의 규모가 커질수록 비용이 증가하는 특징이 있다[6][7].

본 장에서 제안하고자 하는 분산 허니넷은 3장에서 제안한 라즈베리파이 기반의 Simple 허니팟을 활용하여 LAN구간의 내부자 스캔공격을 식별하고 서버와 같은 주요한 자산 주변에 설치하여 DMZ 구간을 보호하여 전체 WAN구간을 보호하고자 한다.



(그림 7) 분산 허니넷의 구성도

각각의 영역에서 탐지된 공격신호는 중앙의 관제서버에서 종합되며, 식별된 위협정보를 2차 가공하여 전체 위협범위를 식별할 수도 있다.

따라서 분산 허니넷을 활용하면 보호해야 하는 도메인에 분산되어 있는 Simple 허니넷은 LAN구간에서 감염되어 있는 좀비PC를 식별하고 침해사실을 탐지하고 대응할 수 있다.

4.2. 분산 허니넷 평가

일반적인 허니넷은 서버를 이용하여 가상화 환경에 구축한다. 하지만 가상화 환경을 허니넷으로 구축하기 위해서는 기술적 분야의 노력이 필요하다[9]. 하지만 Simple 허니팟은 스틱PC를 활용하고 간단한 코드로 구현되어 있어 추가 확장 및 분산 허니넷 구축이 용이하며 비용이 저렴하다. 하지만 현 분산 허니넷은 스캔공격 이외의 공격탐지가 제한되는 문제점이 있다.

<표 1> 일반 허니넷과 분산 허니넷의 비교

구 분	일반 허니넷	분산 허니넷
비용	고가	저렴
크기	서버	스틱 PC
확장	어려움	쉬움
탐지기법	다양한 공격	내부망 스캔
영역	제한적	유동적

5. 결론 및 향후 과제

본 논문에서 제안한 Simple 허니팟을 이용한 분산 허니넷은 최근 공격자가 주로 사용하는 내부 경유지를 활용한 공격에 대응하기 위한 체계로 활용할 수 있으며, 구축 시 스틱PC를 사용하여 공간 및 비용적 측면에서 기존의 일반 허니넷보다 우수한 성능을 확인할 수 있다. 하지만 수집되는 정보의 처리가 미흡하여 단순 스캔 공격만을 식별할 수 있으며, 단순히 탐지한 결과에 대하여 관리자가 수동으로 대응할 수밖에 없다.

따라서 향후 과제로 스캔공격 이외의 다양한 공격을 탐지하고 대응할 수 있도록 분산 허니넷의 활용방법에 대하여 연구할 것이며 수집된 정보의 평판분석 등과 같이 사이버 인텔리전스 기법과 융합하여 고도의 위협정보를 식별할 수 있도록 개선할 예정이다.

참고문헌

[1] (사)한국정보보호학회, “고도화된 사이버 위협에 효과적으로 대응하기 위한 국가보안 Knowledge-Base 구축전략 연구”, 국가정보화전략위원회, 2011

[2] AhnLab Online Security. “포트 스캐닝의 이해”, 2004

[3] 한경수, 임광혁, 임을규. "허니넷을 이용한 P2P 기반 Storm 봇넷의 트래픽 분석." 정보보호학회논문지 19.4 (2009): 51-61.

[4] Lee, Gi-Sung, et al. "A Study of Network Forensic for IDS." Journal of the Korea Academia-Industrial cooperation Society 12.1 (2011): 467-473.

[5] NMAP, NMAP Free Security Scaner, http://nmap.org/

[6] 강대권, 현무용, and 김천석. "Cybertrap: 가상 허니넷 기반 신종공격 탐지시스템." 한국전자통신학회 논문지 8.6 (2013): 863-871.

[7] 이문구. "하이브리드 허니팟 시스템에 대한 연구." 전자공학회논문지 51.11 (2014): 127-133.

[8] Raspberry Pi, “Raspberry Pi”, http://www.raspberrypi.org/

[9] https://www.projecthoneypot.org/