가상 시스템을 이용한 Mirai DDOS 공격/방어 훈련 시스템 구현

염성규*, 이해영**, 신동일*, 신동규*
*세종대학교 컴퓨터공학과
**(주)두두아이티
e-mail : ysk@gce.sejong.ac.kr, apizaco@duduit.co.kr,{dshin, shin}@sejong.ac.kr

Implementation of Mirai DDOS attack / defense training system using virtual system

Seong-Kyu Yeom*, Hae-Yeong Lee**, Dong-Il Shin*, Dong-Kyoo Shin*
*Dept. of Computer Engineering, Sejong University
**Inc. DuDu Information Technologies

요 약

최근 ICT 기술이 발전함에 따라 많은 편리함과 경제적 등 이점이 증대함과 동시에 각종 침해사고, 관리 미숙 및 부주의로 생기는 손실 또한 증가하는 추세다. 또한 침해 대응 실무자의 역량강화를 위하여 실제 시스템에서 실습하기는 어렵다. 본 논문에서 사물 인터넷(IoT) 장비들을 봇넷으로 구성한 Mirai 공격 사례를 바탕으로 가상 시스템을 통해 공격 및 방어 훈련 시스템을 구현하였다.

1. 서론

최근 사물의 신원확인, 의사소통이 가능한 네트워크 구축, 컨트롤 가능성 등의 기술적 환경 구축을 통하여 인터넷과 사물을 연결하는 사물 인터넷(IoT)가 다양한 분야에서 비용절감과 효율적 운영 등의 이유로 급부상하고 있다[1].

이처럼 실생활은 편리해졌지만 사물 인터넷(IoT)를 중심으로 한 스마트 시대에 사용되는 사물 인터넷(IoT) 장비들이 cctv 해킹, 스팸메일 대량 발송, 봇넷으로 활용 등의 범죄에 악용될 가능성이 커지고 있으며 대부분은 해킹에는 무방비 상태이다[2].

그리고 인터넷 발전으로 많은 이점이 있지만 그와 함께 각종 침해사고 및 관리 미숙, 부주의로 생기는 손실 또한 커지고 있다. 또한 침해사고 대응 능력 향상을 위하여 실제 시스템에서 공격 및 대응 해보는 실습을 하기는 어렵다[3].

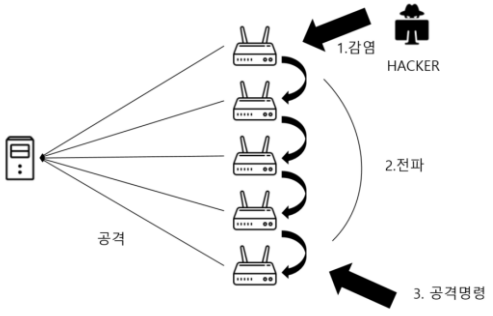
본 논문에서는 사물 인터넷(IoT) 기기들을 봇넷으로 이용한 대규모 분산 서비스 거부 공격(DDOS)인 Mirai 사례에 대하여 설명하고 실습을 위한 가상 시스템 및 문제 구성을 통하여 침해사고 대응 능력 향상을 위한 시스템을 제안한다.

2. Mirai 악성코드

Mirai 악성코드는 2016 년 9 월에 사물인터넷(IoT) 장비를 대상으로 봇넷으로 구성하고 약 600Gbps 이상에 해당하는 트래픽을 발생시킨 대규모 서비스 분산 거부 공격(DDOS)이다. 사물 인터넷(IoT) 장비들은 대부분 CPU 환경에 적합한 리눅스 운영체제를 사용하고 있다. Mirai 악성코드는 다양한 CPU 환경에서 실행 가능하도록 크로스 컴파일을 통해 제작되기 때문에 대부분의 사물 인터넷(IoT) 장비들이 공격의 대상이 된다[4-6].

동작하는 원리로는 크게 랜덤한 IP 주소를 생성하여 포트 22 번과 23 번으로 약 60 여개의 공장 출하 상태의 ID/PW 값을 이용하여 사전식 전사 공격을 시도하는 스캔 및 접속 단계와 접속이 성공시 Mirai 악성코드를 Busybox 의 wget 명령어를 이용하여 Mirai 악성코드를 다운로드 받아 실행시키는 감염 및 전파 2 가지 단계로 구분된다. 이 두가지 단계를 반복하여 다수의 좀비를 확보하게 된다[4-6].

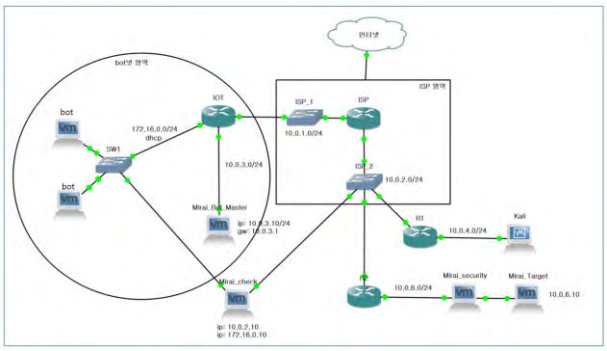
이렇게 형성한 사물인터넷(IoT) 봇넷은 C&C 서버에 접속하여 명령을 대기하다가 명령이 내려지면 공격을 수행한다.



(그림 1) Mirai 동작 원리

3. 설계 및 구현

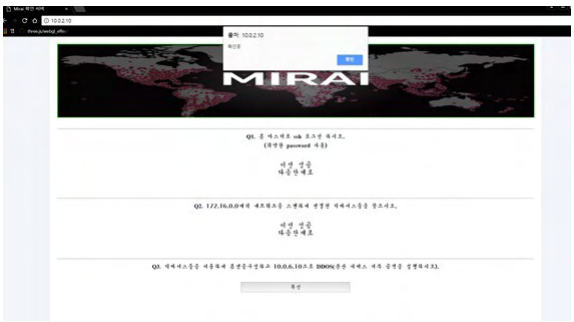
본 논문에서 구현한 시스템의 구조는 아래 그림 2 와 같다.



(그림 2) Mirai 사례를 이용한 공격/방어 훈련 시스템

IP 대역을 10.0.X.X 를 공인 IP 라는 가정하에 제작하였으며 172.16.X.X 대를 사설 IP 로 설정 하였다. 또한 시나리오를 공격적 측면에서 실습하고 공격 실습이 끝난 뒤에 방어적 측면에서의 실습을 진행할 수 있도록 구성을 하였다.

공격적 측면에서 먼저 Kali 로 접속을 한다. 다음 문제 1 번과 2 번을 통하여 공격자의 패스워드 추측 능력과 네트워크 스캔 능력을 테스트 한다. 문제 3 번을 통해 Mirai 사례를 실습한다. Kali 에 C&C 서버를 구성한 뒤에 Mirai 소스 파일을 다운 받아 컴파일 시키고 C&C 서버를 구성한다. 다음 봇 마스터로 접속을 한 뒤에 봇을 실행 시켜 bot 넷 영역 안의 봇들을 감염을 시킨다. 그 후 감염된 봇들을 활용하여 Mirai_Target 의 웹서버로 DDOS 공격을 진행하게 된다. 공격을 성공하면 Mirai_check 서버에서 아래 그림 3 과 같이 공격 확인을 요청한다. 공격이 성공하였을 경우 다음으로 진행하고 실패 시 다시 시도하게 된다.



(그림 3) DDOS 공격 확인 요청 중

방어적 측면에서는 문제 4 번을 통해 네트워크 보안 도구 활용을 실습하고 문제 5 번을 통해 Mirai 공격의 방지 방법을 실습한다.

문제 4 번은 Mirai_security 로 접속을 하여 snort 설정을 진행한 뒤 DDOS 공격을 켜 놓은 상태로 문제 의 확인을 요청하면 Mirai_check 서버에서 Mirai_Target 의 서버에 접속 가능 여부를 보고 정답 유무를 판단한다.

문제 5 번은 사물인터넷(IoT) 장비에서 불필요한 포트를 차단하여 감염을 예방하는 방법으로 사물인터넷(IoT)장비의 포트 차단 및 계정 정보 변경을 진행하고 Mirai_check 서버를 통하여 확인한다.

4. 결론

본 논문은 Mirai 악성코드에 대하여 알아보고 취약점 원리 및 공격방법을 실습을 통하여 능동적으로 학습할 수 있는 가상 환경을 구축하여 보았다.

또한 공격과 방어를 실습해보면서 실습자의 기술적 역량 즉 침해사고 대응 능력 및 공격 원리 이해가 강화될 것으로 기대된다.

향후 다양한 침해 사고를 컨텐츠화하여 하나의 프레임 워크로 개발이 필요하다.

ACKNOWLEDGMENT

본 연구는 2017 년도 중소벤처기업부의 기술개발사업 지원에 의한 연구임을 밝힙니다. [S2542353]

참고문헌

[1] Nam, Mee Kyung, "An Analysis on the Present Condition of Smart Health Care Product Design Industry Centered on IoT," JOURNAL OF THE KOREAN SOCIETY DESIGN CULTURE, Vol. 22, No. 1, pp. 115~126, Mar, 2016.

[2] 배상태, 김진경 “사물인터넷(IoT) 발전과 보안의 패러다임 변화”, 한국과학기술기획평가원, KISTEP InI 제 14 호, pp. 44~57, June 2016.

[3] 홍동완 외 7 인, “정보보호기술훈련장 시스템 업그레이드 소프트웨어 개발(2)”, [IITA] 정보통신연구진흥원 학술기사, 1990

[4] 한국인터넷진흥원(KISA) “2016 년 Mirai 악성코드 동향”, Dec, 2016.

[5] Sein Myung, Young-Jun Song and Jong-Hyouk Lee, "Source Code Analysis of Mirai DDoS Attacks," Proceedings of Symposium of the Korean Institute of communications and Information Sciences, , pp. 388~389, Jan, 2017.

[6] https://github.com/jgamblin/Mirai-Source-Code