정교한 스캐닝 탐지 방법

최연주[0], 정유석, 홍만표
아주대학교 정보통신전문대학원
choiyj2@madang.ajou.ac.kr

Sophisticated scanning detection mechanism

Yeun-Ju Choi[0], Yoo-Suk Jung, Man-Phou Hong
Graduate School of Information and Communication AJOU University

요 약

해킹사고가 증가하면서 시스템이 스캐닝(Scanning)당하는 사례도 증가하고 있다. 이는 해커들이 해킹의 전단계로 해킹하고자 하는 호스트(목적호스트)의 취약점을 파악하기 위하여 스캐닝하기 때문이다. 따라서 호스트가 스캐닝 당하는 것을 정확하게 탐지할 수 있다면 해킹이 이루어지는 것을 미연에 방지 할 수 있다. 또한 스캐닝 단계에서 해커는 목적호스트와 패킷을 계속 주고받아야함으로 자신의 IP 주소 등의 정보를 속이기 어렵다. 그래서 목적호스트는 차후 스캐닝한 해커의 IP를 이용해서 해커를 추적할 수도 있다. 하지만 기존의 스캐닝 대응 및 탐지방법은 이러한 정보를 사용하지 못하고 있다. 기존의 탐지 방법은 단순히 단시간 내에 발생하는 SIN, FIN패킷의 양을 바탕으로 스캐닝을 판단한다. 하지만 단시간 내에 대량의 패킷을 사용하여 스캐닝을 하는 경우는 대부분 툴을 이용한 경우이며 소량의 패킷만을 사용하여 스캐닝을 하는 경우는 탐지하지 못한다. 본 논문에서는 이러한 정교한 스캐닝을 탐지하기 위해서 들어온 패킷의 양이 적더라도 TCP 상태 다이어그램(TCP state diagram)의 순서에 맞지 않게 들어올 경우, 닫힌 포트로 들어오는 경우를 파악하여 스캐닝을 탐지하는 방법을 제시하고자 한다.

1. 서 론

최근 해킹에 의한 사고가 증가하면서 스캐닝을 당하는 사례도 또한 증가하고 있다. 이는 일반적으로 해킹을 하기 위해서 해커들이 목적호스트의 취약점을 알고자 먼저 목적호스트를 스캐닝(Scanning)하기 때문이다. 이러한 스캐닝 단계는 실제 공격은 아니지만 공격을 알리는 신호탄과 같다. 그러므로 이런 스캐닝을 정확하게 탐지한다면 해킹을 방지하는데 큰 도움이 될 수 있을 것이다.

하지만 기존의 스캐닝 탐지 방법은 스캐닝을 완벽하게 탐지하지 못하고 있다. 기존의 스캐닝 탐지 방법은 대부분 스캐닝 툴들에 의한 스캐닝을 탐지하는 방법으로서 단시간 내의 대량 패킷의 발생이나, 특정 패킷을 탐지함으로서 스캐닝을 탐지한다. 이런 방법들은 잘 알려진 스캐닝툴을 비교적 정확하게 탐지할 수는 있지만 새로운 스캐닝 툴을 이용하거나 또는 적은 양의 패킷을 이용한 스캐닝을 탐지할 수 없다. 그래서 좀 더 포괄적인 스캐닝 탐지 방법이 필요하다.

또한, 정보를 빼내을 목적이 아닌 공격을 목적으로 하는 일반적인 해킹에서 해커들은 자신의 IP 주소를 속이는 경우가 많다. 그렇기 때문에 해킹을 당하고도 해커를 찾아내기가 어려운 경우가 많았다. 하지만 해킹의 전단계인 스캐닝 단계에서는 목적 호스트와 해커는 지속적으로 패킷을 주고받아야 하기 때문에 자신의 IP를 속이기 힘들다. 따라서 이러한 스캐닝 단계에서 의심이 되는 정보를 로그로 남긴다면 후에 해커를 찾는데 유용한 정보로 이용될 수 있다.

2. 관련연구

기존의 스캐닝 탐지 방법들은 목적호스트로 들어오는 다량의 SYN과 FIN 패킷의 양을 측정하여 탐지하는 방법이다. 기존에 나와 있는 스캐닝 툴(NMAP, Nessus)툴을 이용하는 경우에는 목적호스트로 다량의 SYN 또는 FIN 패킷을 전송한다. 그러나 일반적인 프로그램의 경우 이렇게 단시간에 많은 SYN 또는 FIN 패킷을 발생시키지 않는다. 따라서 단시간 내에 발생하는 SYN 또는 FIN 패킷을 양을 보고 스캐닝을 판단할 수 있다. 하지만 이런 탐지 방법은 만약 공격자가 단시간 내에 많은 SYN 또는 FIN 패킷을 발생시키지 않는다면 스캐닝을 탐지할 수 없다. 따라서 전문적인 해커라면 소수의 패킷을 이용해서 스캐닝을 하거나 아니면 오랜 시간에 걸쳐 조금씩 패킷을 보내서 스캐닝의 탐지를 피할 수 있다.

두 번째로 기존의 스캐닝 탐지 방법으로 알려지지 않은 포트 이용하는 패킷을 탐지하는 것이다. 하지만 이것 또한 전문적인 해커라면 알려진 포트만을 이용해서도 충분히 스캐닝을 할 수 있다.

세 번째로 스캐닝 방지 방법으로 ICMP 같은 패킷이나 알려지지 않은 포트로 오가는 패킷을 방화벽(Firewall)이나 침입탐지 시스템(Intrusion Detection System)에서 버리는 방법이 있다. 이 방법은 스캐닝을 하는 것을 방해할 뿐 탐지하는 것은 아니다. 또한 스캐닝에 이용되는 일부의 패킷만을 버리기 때문에 근본적으로 스캐닝을 예방할 수 없다.

마지막으로 스캐닝 탐지 방법으로 잘 알려진 스캐닝 툴들이 이용하는 패킷의 시그네이쳐(signature)를 저장하였다가 그런 패킷이 전송되면 탐지하는 방법 있다. 하지만 이 방법은 기존의 잘 알려진 스캐닝 툴에 의한 스캐닝만을 탐지할 뿐 알려지지 않은 툴을 이용한 경우는 탐지할 수 없다.

스캐닝에 대한 연구 논문으로 Ofir Arkin의" Network Scanning Techniques" [2]에서 기본적인 스캐닝의 방법에 대한 설명이 자세히 나오고 있다. 또한 Ofir Arkin의" ICMP Usage In Scanning" [3]에서는 ICMP 패킷을 이용해서 할 수 있는 운영체제 스캐닝 방법을 설명하고 있다. 그래서 이 두 논문을 기본으로 스캐닝의 일반적인 방법을 정의하고 탐지하는 방법을 제시하고자 한다. 일반적인 스캐닝 방법을 정의하고 탐지에 이

본 논문은 한국전자통신연구원의 지원에 의한 것임

용하기 때문에 특정한 스캐닝 툴만을 탐지하지 않고 새로운 스캐닝 툴도 탐지할 수 있으며. 또한 TCP 상태 다이어그램을 이용하여 적은 양의 패킷으로 스캐닝을 하는 경우도 탐지할 수 있다.

3. 탐지 대상 스캐닝(Scanning)의 방법

스캐닝은 핑 스캐닝(Ping scanning), 포트 스캐닝(Port scanning), 운영체제 스캐닝(OS scanning)으로 나눌 수 있다.

3.1 핑 스캐닝

핑 스캐닝은 목적호스트가 네트워크에 연결되어 있는지 확인하는데 사용한다. 따라서 목적호스트의 존재여부를 판단하는 핑 스캐닝은 다른 여러 스캐닝들 중에서도 가장 먼저 이루어진다.

핑 스캐닝을 하는 대표적인 방법은 목적호스트에 ICMP echo 패킷을 보내본다. 만약, 목적호스트에 ICMP echo 패킷을 전송하고 응답이 있으면 목적호스트가 네트워크에 연결되어 있는 것이다. 하지만 아무런 응답이 없으면 목적호스트가 네트워크에 연결되어 있지 않은 것을 의미한다.

3.2 포트 스캐닝

포트 스캐닝은 특정 호스트가 네트워크에 연결되어 있는 경우 그 호스트의 열려진 포트를 번호를 알려준다.

3.2.1 TCP 포트의 스캐닝방법

TCP 패킷에는 8개의 선택 비트(Option bit) 필드가 존재한다. 그리고 선택 비트 필드를 어떻게 선택하는지에 따라서 TCP의 특정 포트가 응답하는 것이 다르며, 이것을 이용해서 TCP의 포트가 열려있는지 닫혀있는지를 파악할 수 있다. TCP 포트 스캐닝 방법은 아래와 같다.

첫째, 목적 호스트의 특정 포트에 접속(Connect)하는 것이다. 이 방법은 목적 호스트에 접속에 관한 로그가 남기 때문에 대부분은 피하는 방식이다.

둘째, 목적 호스트의 특정 포트에 SYN 패킷(SYN 선택 필드가 선택된 패킷)을 전송하는 방법이다. 이 때 특정 포트가 열려 있으면 SYN /ACK 패킷(SYN과 ACK 선택 필드가 선택된 패킷)이, 포트가 닫혀 있으면 RST /ACK 패킷이 전송되어 온다.

셋째, 목적 호스트의 특정 포트에 FIN 패킷을 보내거나, 모든 선택(option)비트를 ON 시키거나 또는 OFF 시킨 패킷을 보낸다. 이런 패킷을 보내면 열린 포트는 아무런 패킷도 전송하지 않지만 닫힌 포트는 RST 패킷을 전송한다.

3.2.2 UDP 포트의 스캐닝방법

UDP 포트를 스캐닝하는 방법은 목적호스트에 UDP 패킷을 전송하여 ICMP_PORT_UNREACHABLE 에러가 전송되면 닫힌 포트이고 열린 포트의 경우 아무런 패킷도 전송하지 않는다. UDP 패킷은 신뢰성을 보장하지 않기 때문에 한 번 스캐닝한 결과로는 열린 포트를 정확하게 판단할 수 없으며, 두 번 이상 반복해 보아야 정확한 결과를 알 수 있다. 또한 스캐닝하는 시간도 TCP 포트 스캐닝에 비해 스캐닝 시간이 길다.

3.3 운영체제 스캐닝

목적호스트의 운영체제를 알 수 있다면, 공개된 그 운영체제의 취약점등을 이용하여 보다 쉽게 해킹을 할 수 있다. 그래서 보통 해커는 스캐닝의 마지막 단계로 운영체제 스캐닝을 행하게 된다.

운영체제 스캐닝은 일반적으로 닫힌 포트나 열린 포트에 패킷을 전송하면 운영체제마다 약간씩 다른 반응을 보이는 것을 이용한다. 하지만 이 방법을 이용하려면 먼저 포트가 열려 있는지 닫혀 있는지 파악하고 있어야 한며, 따라서 이 방법을 이용하려면 포트 스캐닝이 선행되어야 한다.

첫째, 통신 요구의 응답내의 ISN(Initial Sequencing Number)중의 패턴(pattern)을 보고 운영체제를 구분한다.

둘째, 돌아오는 패킷의 윈도우 크기(Window size)를 확인함으로써 운영체지의 구분이 가능하다. 이는 윈도우의 크기가 운영체제에 따라 다르기 때문이다.

셋째, 목적호스트에서 만들어진 ICMP 패킷[3]을 이용한다. 운영체제들마다 ICMP 패킷을 생성할 때 패킷을 만드는 방법이 다르며 이것을 이용하여서도 운영체제를 구분할 수 있다.

4. 새로운 스캐닝 탐지 방법

기존의 스캐닝 방법으로는 적은 수의 패킷을 이용하여 스캐닝을 하는 경우나 장기간에 걸쳐 조금씩 패킷을 전송하여 스캐닝을 하는 경우는 탐지하지 못한다. 따라서 본 논문에서는 새롭게 제시하는 스캐닝 탐지 방법을 기존의 탐지 방법에 추가한다면 전문가에 의한 정교한 스캐닝 또한 탐지할 수 있다. 현재 개발 중인 대응 시스템에서는 스캐닝의 분석을 용이하게 하기 위해 스캐닝으로 의심되는 패킷을 모두 로그로 남기고 차후 로그의 정확한 분석을 통하여 해커를 탐지한다. 자세한 대응 방법은 아래와 같다.

4.1 닫힌 포트로 들어오는 패킷을 탐지한다.

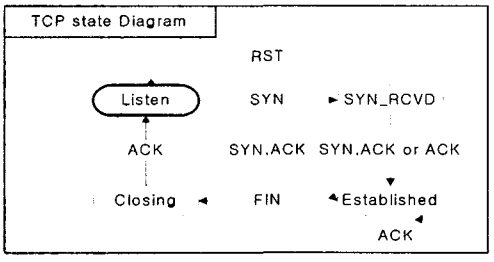
닫혀 있는 TCP 또는 UDP 포트로 오는 TCP나 UDP 패킷들을 스캐닝 공격으로 탐지하여 로그로 남긴다. 정상적인 통신과정에서는 닫힌 TCP 나 UDP 포트로 패킷이 전송되는 경우는 극히 드물다. 따라서 닫힌 포트로 들어오는 패킷은 스캐닝으로 의심해 볼 수 있다.

정교한 해커라면 전체의 포트를 스캐닝하지 않고 특정한 포트 몇 개만을 스캐닝 하는 경우가 있다. 이 경우에는 포트가 다 열려 있을 수도 있지만 하나 이상의 닫힌 포트일 경우가 많다. 그래서 해커가 장기간에 걸쳐 적은 양의 패킷으로 스캐닝을 하는 경우라도 하나의 패킷이 닫힌 포트로 오게 되면 스캐닝으로 탐지할 수 있다.

4.2 열린 TCP 포트로 들어온 패킷 중에서 TCP 패킷이 TCP 상태 다이어그램을 위반하면 탐지한다.

정상적인 TCP 패킷이라고 한다고 항상 TCP 상태 다이어그램 안에서 움직인다. 하지만 스캐닝의 경우는 정상적인 통신이 아니기 때문에 열린 TCP 포트로 TCP 상태 다이어그램과는 상관없이 TCP 패킷을 보내는 경우가 많다. 그래서 TCP 상태 다이어그램을 지키지 않는 TCP 패킷은 스캐닝으로 의심할 수 있다. 아래의 그림은 TCP 상태 다이어그램에서 패킷을 받는 부분만 새롭게 그린 것이다. TCP 상태 다이어그램에는 패킷을 주는 상태와 받는 상태의 그림이 같이 그려있다. 하지만 우리는 받는 패킷만을 보고 탐지를 하기 때문에 TCP 패킷을 받아서 생기는 상태 변화만 표현한 것이다.

만약 해커가 특정 포트만 열려 있는지 확인하고자 한다면 특정 포트에 하나의 FIN 패킷만 보낼 것이다. 이 경우에 기존의 스캐닝 탐지 방법은 FIN 패킷의 양이 적기 때문에 스캐닝을 탐지하지 못한다. 하지만 만약 그 포트가 닫혀 있다면 새롭게 제시한 첫 번째 방법에 의해 탐지가 될 것이다. 또한 그 포트가 열려 있다면 새롭게 제시한 TCP 상태 다이어그램에서는 통신이 시작할 때 FIN 패킷이 전송되어 오는 경우가 없다. 따라서 TCP 상태 다이어그램에 맞지 않기 때문에 스캐닝으로 탐지할 수 있다.



4.3 ICMP echo 패킷이 전송되어 오면 스캐닝으로 탐지한다.

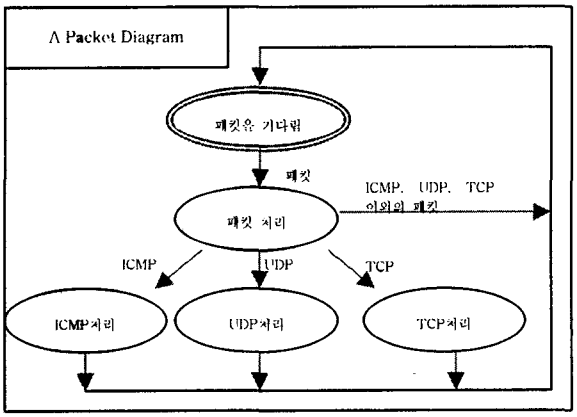
현재, 많은 사용자들이 ICMP echo 패킷을 이용해서 악의 없이 특정 호스트가 네트워크에 연결되어 있는지 확인하는 경우가 많다. 그래서 이 경우에는 악의가 있는 스캐닝과 악의가 없는 스캐닝을 구분할 필요가 있다. 스캐닝에 대한 로그가 남기 때문에 IP 주소를 확인하여 자신에게 ICMP echo 패킷을 보낼 가능성이 있는 IP 주소를 제외하고 스캐닝을 탐지할 수 있다. 그리고 ICMP echo 패킷을 이용하는 경우, 한 종류의 ICMP echo 패킷을 이용한다. 그런데 두 종류 이상의 ICMP echo 패킷이 전송되어 왔다면 그것은 확실히 스캐닝으로 의심할 수 있다.

5. 새로운 스캐닝 탐지 방법의 알고리즘

아래와 같은 순서대로 실행하면서 스캐닝을 탐지한다.

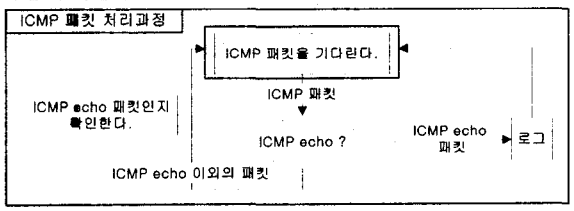
5.1 ICMP, UDP, TCP 패킷 분류

a. 하나의 패킷이 들어올 때마다 아래의 다이어그램에 따라 수행된다.
b. ICMP, UDP, TCP 패킷만 처리하고 그 이외의 패킷을 무시한다.
c. ICMP, UDP, TCP 패킷마다의 처리과정을 수행하고 스캐닝으로 판단되면 로그를 남긴다.



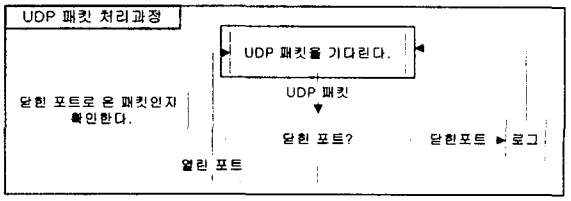
5.2 ICMP 패킷 처리과정

ICMP echo 패킷(ICMP echo request, ICMP time stamp request, ICMP address mask request,ICMP information request)인지 판단한다. ICMP echo 패킷이면 로그를 남기고 아니면 무시한다.



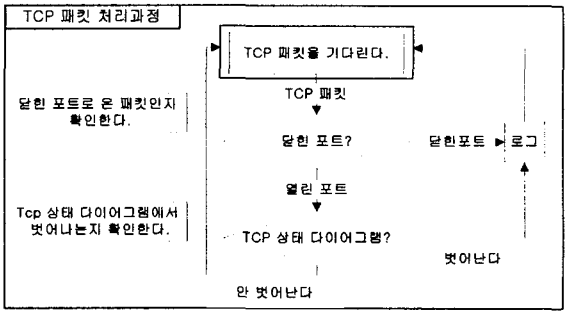
5.3 UDP 패킷 처리과정

들어온 UDP패킷이 닫힌 포트로 들어온 패킷인지 확인한다. 닫힌 포트로 들어온 패킷이면 로그를 남기고 열린 포트로 들어온 패킷이면 무시한다.



5.4 TCP 패킷 처리과정

우선 들어온 TCP 패킷이 닫힌 포트로 들어온 패킷인지 확인한다. 닫힌 포트로 들어온 패킷이면 로그를 남기고 열린 포트로 들어온 패킷이면 TCP 상태 다이어그램에 맞는지 확인한다. TCP 상태 다이어그램에서 벗어나면 로그를 남기고 벗어나지 않으면 무시한다.



6. 결론 및 향후 연구 방향

새롭게 제시한 방법을 기존의 스캐닝 탐지 방법과 함께 이용하다면 기존의 알려진 스캐닝 툴뿐만 아니라 새로운 스캐닝 툴도 탐지할 수 있다. 또한 적은 패킷을 이용한 스캐닝까지 탐지할 수 있다. 하지만 통신상의 오류 등에 의해 하나 이상의 패킷이 위의 세 가지 조건에 포함될 수 있다. 따라서 위의 조건을 만족하는 패킷이 하나만 존재한다면 스캐닝인지 구분하기 어려울 수 있다. 따라서 스캐닝으로 판단하기 위한 기준값(Threshold)을 결정해 주어야 한다.

또한, 스캐닝의 많은 패킷을 잡으면 그만큼 많은 데이터를 얻을 수 있지만 그 많은 데이터를 얼마나 효율적으로 종합할 수 있는지 또한 종합된 데이터를 얼마나 효율적으로 이용할 수 있는지는 많은 연구가 필요하다.

6. 참고 문헌

[1] Dethy " Examining port scan methods" 2001
[2] Ofir Arkin " Network Scanning Techniques" sys-security 1999
[3] Ofir Arkin " ICMP Usage In Scanning" sys-security 2001
[4] Jose Nazario " Passive System Fingerprinting uSYNg Network Client Applications" 2001
[5] Fyodor " Remote OS detection via TCP/IP StACK FingerPrinting" 1998
[6] W. Richard Stevens " TCP/IP Illustrated Volume I" book
[7] http://www.insecure.org/nmap/ - NMAP
[8] http://www.nessus.org - NESSUS
[9] http://www.snort.org - SNORT
[10] http://cert.certcc.or.kr -RTSD