피해 범위 기반 해킹 분류 기법

최양서*, 서동일*, 손승원*

*한국전자통신연구원, 사이버테러기술분석팀, **한국전자통신연구원 네트워크보안연구부

Damage Degree based Classification of Hacking Techniques

Yang-seo Choi*, Dong-il Seo*, Seung-won Sohn**

*ETRI Anti-Cyber Terror Team, **ETRI Network Security Dept.

요 약

인터넷을 이용한 다양한 서비스들이 제공되면서 인터넷 사용자가 급증하였고, 인터넷 침해 사고 역시 크게 증가하였으며, 그 피해는 점차 매우 광범위해졌다. 이와 같이 급증하는 해킹을 보다 효과적으로 분석하기 위해 몇몇 해킹 분류 기법들이 제안되었다. 그러나, 현재까지 제안된 해킹 분류 기법들은 단순히 해킹에 사용되는 취약점을 이용한 분류로, 이는 통계자료로만 활용될 뿐, 이를 통해 추가적인 정보를 얻을 수는 없었다. 이에 본 논문에서는 이와 같은 단점을 극복하기 위해, 해킹에 의해 발생할 수 있는 피해의 정도에 따라 해킹 기법들을 분류하고, 제안한 분류 기법을 통해 침해에 대한 기본적인 대응 방법을 제안함으로써 발생하는 다양한 침해에 대해 신속히 대처할 수 있는 기본 틀을 제공하도록 한다.

I. 서론

인터넷이라는 매체를 통해 생성된 사이버 사회(Cyber Society)를 통해 과거에는 실생활에서만 가능했던 일들 대부분을 수행할 수 있게 되었다. 이와 함께 실제 돈의 흐름이 인터넷을 통해 이루어지게 되었고, 이에 따라 해킹에 따른 피해도 증가하기 시작하였다. 특히 해킹의 형태가 과거 일반 시스템으로의 허락되지 않은 접속 및 권한 상승을 목표로 하던 방식에서 대형 네트워크에 대한 마비를 초래하는 형태로 변경되면서 그 피해는 가히 기하급수적으로 증가하였다.

이와 같이 해킹에 따른 피해가 급증하면서 해킹의 형태를 파악하기 위해 해킹 기법 분류 방안들이 제안되었으나, 이는 해킹에 사용되는 취약점을 기반으로 분류되어, 단순히 해킹 기법들을 분류한 것에 지나지 않았다. 또한, 해킹 기법에 대한 적절한 사후 조치 방안을 제시하지 못하여, 발생할 수 있는 피해 정도를 파악하는 것도 불가능 했다.

이와 같은 단점을 극복하기 위해 본 논문에서는 해커의 해킹 기법들을 실제 발생할 수 있는 피해의 정도에 따라 분류하고, 이를 바탕으로 대응방법을 제시하여, 해킹 탐지가 이루어지는 경우, 해당 해킹 기법이 속한 분류에 따라 더 큰 피해가 발생하기 전에 대처를 시작할 수 있는 기본 틀을 제공한다.

본 논문은 다음과 같이 구성되어 있다. 먼저, 제2장 관련 연구에서 과거 제안된 해킹 분류 기법들을 알아보도록 하고, 제 3장에서는 본 논문에서 제안하는 피해 정도에 따른 해킹 분류기법을 논의하며, 제 4장에서 결론을 내리도록 한다.

II. 관련연구

1. Marcus J. Ranum에 의한 해킹 기법 분류[3]

해킹 기법 분류를 위해 가장 널리 사용되고 있는 방법은 Marcus J. Ranum[1]에 의해 제안된 분류 기법으로 각 해킹 기법들이 사용하는 취약점을 이용하여 분류한 것이다. 본 분류에서 사용하는 항목들은 다음과 같다.

- 사용자 도용(Impersonation)
- SW보안오류(SW Vulnerability)
- 버퍼 오버플로우 취약점(Buffer Overflow)
- 구성설정오류(Configuration Vulnerability)
- 악성프로그램(Malicious Codes)
- 프로토콜취약점(Protocol Infrastructure Error)
- 서비스거부공격(Denial of Service Attack)
- E-Mail 관련 공격(Email Vulnerability)
- 취약점정보수집(Vulnerabilities Probing)
- 사회공학(Social Engineering)

CERTCC/KR에서는 발생한 각종 침해사고를 위 분류를 통해 분류하고 그 통계자료를 제공하고 있다. 본 분류 방법은 가장 널리 사용되고 있는 방법이기는 하나, 단순히 해킹 기법이 활용하는 취약점을 기반으로 분류한 것으로 추가적인 활용이 거의 불가능한 분류 기법이다.

2. 해커의 해킹 수준과 연계한 해킹 기법분류[4]

[4]에서는 해킹기법 분류를 해커의 수준과 연계하여 해커 수준에 따라 수행할 수 있는 해킹 기법을 분류하고 그 레벨을 정의하였고, 해커의 수준은 해킹을 위한 해킹코드(exploit code) 작성 가능 여부를 이용하여 분류하였다.

또한, Marcus J. Ranum에 의해 제안된 해킹기법을 재분류/통합 하여 다음과 같은 7개의 분류를 제안하였다.

- 시스템 및 서비스 설정 문제
- 프로그램(S/W) 오류 문제
- 프로토콜 취약점
- 정보 수집 공격
- 서비스 거부 공격
- 악성코드
- 기타

본 해킹 분류 기법은 해커의 수준과 해킹 기법을 병합하여 특정 수준의 해커가 사용할 수 있는 해킹 기법을 정의함으로써 이를 활용하여 네트워크의 보안 수준 평가에 활용할 수 있는 계기를 마련하였다. 그러나, 본 분류는 해킹 기법의 실제 난이도만을 활용하여 해킹 기법의 수준을 정의함으로써, 낮은 수준의 해커 역시 높은 수준의 해킹 기법을 사용할 수 있는 현재의 해킹 환경과는 거리가 있었다.

III. 피해 범위 기반 해킹 분류기법

본 논문에서는 기존의 취약점에 따른 해킹 분류 기법이 아닌 해킹에 의해 발생하는 피해 정도를 이용한 새로운 해킹 분류 기법을 제안한다.

1. 분류의 목적

본 논문에서 제시하는 피해 범위 기반 해킹 분류 기법은 해킹 시도에 의해 발생하는 그 피해 정도를 기준으로 해킹 기법들을 분류하여 해킹 발생 시 해당 해킹에 의해 발생할 수 있는 피해 정도를 신속히 파악함으로써 빠르게 대처할 수 있도록 하여, 피해를 최소화 할 수 있도록 하는 기반 정보를 제공하는데 그 목적이 있다.

2. 분류의 기준

본 논문에서는 해킹에 의해 발생할 수 있는 피해의 정도를 그 기준으로 하여 해킹의 형태를 분류한다. 여기서, 피해 정도라는 것은 공격의 대상이 어떤 시스템인가와 공격 기법이 무엇인가에 의해 결정되게 된다. 즉, 공격의 대상이 일반 시스템인가 혹은 네트워크 상의 노드들인가에 따라 그 피해 범위가 달라지고, 또한 공격 기법이 일반 시스템 해킹을 위한 공격 기법인가, 혹은 다량의 패킷을 생성시키는 분산 서비스 거부 공격 혹은 웜 해킹 형태의 공격인가에 따라 그 피해 범위가 달라지므로, 이와 같은 항목들을 분류의 기준으로 사용하도록 한다.

이와 같은 기준에 따라 다음과 같이 해킹 기법을 시스템 범위, 지역망 범위, 광역망 범위로 분류한다.

3. 해킹의 분류

1) 시스템 범위

시스템 범위라는 것은 그 피해 정도가 특정 시스템에 국한 되는 해킹 시도들을 포함하는 분류를 의미한다.

현재 발생하는 대부분의 해킹 시도들은 이와 같은 시스템 범위에 속하는 해킹으로, 그 피해 정도는 시스템의 중요도에 따라 다를 수 있으나, 대부분 그 피해가 국지적이기 때문에 전체 인터넷 혹은 시스템의 마비를 가져오는 타 해킹 기법들에 비해 피해 정도는 작다고 할 수 있겠다.

본 범위에 속하는 해킹은 그 대상이 일반 시스템이고, 공격 기법이 일반 시스템 해킹 기법 - 버퍼 오버플로우 공격 기법 등 - 인 경우를 포함한다. 즉, 비록 공격 기법이 일반 해킹 기법이라 하더라도 공격 대상이 네트워크 노드나 중요 시스템

인 경우에는 본 분류에서 제외된다. 또한 공격 기법이 웜이나 서비스 거부 공격인 경우 역시 본 분류에서 제외된다.

2) 지역망 범위

지역망 범위는 특정 네트워크 범위의 피해가 발생하는 해킹 기법을 포함하는 분류 단위이다. 본 분류에 포함되는 공격에 의한 피해는 시스템 범위의 피해에 비해 크다고 할 수 있다.

본 분류에 속하는 공격에는 공격 목표가 일반 시스템인 분산 서비스 거부 공격(Distributed Denial of Service, DDoS)[7], 혹은 웜 형태의 공격과, Local Network에 속하는 네트워크 노드에 대한 공격이 포함된다. 이는 비록 DDoS 공격의 대상이 특정 시스템이더라도 DDoS 공격에 의해 발생하는 다량의 공격 패킷이 해당 네트워크가 처리할 수 있는 능력을 넘어서는 경우, 네트워크 자체가 마비될 수 있기 때문이다. 인터넷 웜의 경우에도 과거에 비해 크게 발달된 네트워크 인프라를 통해 기하급수적으로 감염 시스템을 늘려나가고 이에 따라 막대한 양의 패킷을 발생시킴으로써 네트워크 마비를 유발한다. 또한 침입차단시스템(Firewall, F/W)이 공격의 목표가 되어 문제가 되는 경우, 특정 네트워크 마비가 유발되기 때문에, F/W를 공격하는 경우도 지역망 범위의 분류에 포함된다. 그리고, Local DNS 서버도 지역망 범위의 분류에 포함된다.

3) 광역망 범위

광역망 범위는 인터넷 망 자체를 마비시킬 수 있는 전역적인 네트워크 마비 공격을 포함하는 분류이다. 본 공격은 말 그대로 전체 인터넷을 마비시킬 수 있기 때문에 그 피해 정도가 매우 크다고 하겠다.

전체 인터넷에 대한 마비를 초래할 수 있는 이와 같은 공격에는 공격의 목표가 다음과 같은 경우가 포함된다.

- 백본망 및 Access망의 네트워크 노드 (라우터, 스위치 및 게이트웨이)
- Root DNS서버

이와 같은 대규모 네트워크에 대한 공격은 지난 2003년 1월 25일 발생한 인터넷 대란을 통해 발생 가능성을 확인할 수 있었다. 본 인터넷 대란은 인터넷 웜을 통해 발생된 다량의 패킷과 그 부산물로 발생한 패킷에 의해 DNS 자체가 마비되면서 한국 내 인터넷 전체가 마비되었던 사건이었다[8].

이와 같은 분류를 정리하면 표1과 같다.

표1. 공격 대상 및 기법 별 분류

공격기법 / 공격대상	일반 해킹기법	DNS류	웜
일반 시스템	시스템 범위	시스템 및 지역망 범위	시스템 및 지역망 범위
F/W	지역망 범위	지역망 범위	지역망 범위
DNS	지역 및 광역망 범위	지역 및 광역망 범위	지역 및 광역망 범위
지역망 노드 (라우터, 스위치, 게이트웨이)	지역망 범위	지역망 범위	지역망 범위
광역망 노드 (라우터, 스위치, 게이트웨이)	광역망 범위	광역망 범위	광역망 범위

표1은 각 공격 기법 및 대상에 따라 해당 해킹 기법이 어떤 분류에 포함되는지를 신속히 알 수 있도록 작성되었다.

3. 피해 범위에 따른 대처 방안

1) 시스템 범위

시스템 범위는 이미 언급한 바와 같이 개별 시스템에 대한 공격으로, 그 피해 범위가 특정시스템에 한정되는 해킹 기법으로 해당 시스템의 특성에 따라 다르나, 대부분 피해의 정도가 크지 않다고 할 수 있다. 이와 같은 경우에는 피해 시스템 분석 절차를 통해 시스템을 점검하고, 피해 상황을 CERT에 신고하여야 한다.

앞서 언급한 바와 같이 특정 시스템의 경우에는 그 중요도가 매우 높은 시스템일 수 있는데, 이런 경우에는 해당 시스템에 대한 공격이 시도되는 경우에 수행해야 하는 특별한 조치 사항들을 따로 작성하여 운영하여야 한다. 이러한 시스템으로는 중요 데이터를 저장한 시스템이나, 특정 서비스를 제공하는 시스템 등이 해당될 수 있다.

2) 지역망 범위

현재까지 발생한 지역망 범위의 공격은 대부분 DDoS 형태의 공격이거나, 인터넷 웜 형태의 공격이었다. 이때, 다량의 패킷을 생성하여 특정 네트워크를 공격하는 단순 DDoS의 경우에는 피해 시스템으로 향하는 패킷을 침입차단시스템을 이용하여 차단한다. 또한 패킷의 송신지를 분석하여 공격 시스템의 관리자와 연락 신속한 패킷 차단을 요구한다. 인터넷 웜의 경우에는 신속히 해당 웜이 사용하는 취약점에 대한 패치를 수행해야 한

다.

3) 광역망 범위

본 분류에 속하는 공격을 방어하기는 매우 어려운 것이 사실이다. 그러나 피해를 최소화 하기위해서는 다음과 같은 대처를 수행해야 한다.

해커는 특정한 목적을 가지고 백본망의 네트워크 노드나 Root DNS를 공격할 수도 있으나, 대부분 제작 의도와는 다르게 동작하는 인터넷 웜에 의해 특정 노드에 대한 공격이 발생하는 경우이다. 그러므로, 이와 같은 공격에 대한 가장 중요한 대처는 예방이다. 특정 노드로 향하는 패킷의 양을 지속적으로 확인하고 이에 대한 대처 방안을 구상해야 한다. 또한 중요 노드로 연결되는 네트워크 상의 경로에 패킷을 차단할 수 있는 기능을 포함시켜, 특정 네트워크를 보호하여야 한다.

이와 같은 방어가 가능하기 위해서는 가입자망, Access망, 백본망의 전체 네트워크가 유기적으로 정보를 공유하여야 하며, 이를 위해 대형 네트워크 상에서 정보 수집과 방어가 이루어 져야 한다. 현재 이와 같은 방어를 위한 과제가 한국전자통신연구원 정보보호기술연구본부에 의해 수행중이다.

IV. 결론

인터넷을 통한 다양한 서비스들이 제공되면서 인터넷 사용자가 급증하였고, 이와 함께 인터넷 침해 사고 역시 크게 증가하였다. 특히 최근에 발생되는 침해 사고들은 기존의 시스템 단위의 해킹의 형태에서 벗어나 대형화되고 있으며, 그에 따른 금전적인 피해역시 매우 큰 것이 현실이다.

이에, 해커의 해킹 기법 분류를 통해 보다 효과적으로 해킹 기법을 분석할 수 있도록 하기 위한 연구가 시작되었으나, 제안된 기법들은 단순히 해킹에 사용되는 취약점의 종류에 따른 분류가 주류를 이루고 있어서, 이를 통해 피해 정도를 파악할 수 있지 못했다. 이에 본 논문에서는 피해의 정도에 따라 해킹 기법들을 분류하고, 제안한 분류 기법을 바탕으로 침해 대응기법의 기본 방법을 제안하였다.

본 논문에서 제안한 해킹 분류 기법은 그 범위에 따라 크게 다음과 같이 분류하였으며, 세부적으로 표1과 같이 분류하였다.

- 시스템 범위
- 지역망 범위
- 광역망 범위

이와 같은 분류를 통해 발생한 해킹의 공격 대상 및 범위에 따라 신속히 대처하여 피해를 최소화할 수 있는 기본 틀을 제공하였다. 앞으로는 보다 세부적으로 해킹 기법을 분류하고, 그에 대한 침해 대응 수준을 정의하며, 자세한 대처 방안을 제안할 계획이다.

참고문헌

[1] http://www.ranum.com
[2] ETRI 지식정보센터, "정보보호 시스템 시장 동향", 주간기술동향 통권 988호, 2001. 3. 21
[3] 한국 정보보호 센터, "'99 국내외 해킹 현황 분석", 한국정보보호 센터, 2000
[4] 최양서 외 2명, "네트워크 보안평가를 위한 해커 및 해킹기법 수준 분류", 정보보호학회지 11권 5호, 2001.
[5] Aleph One, "Smashing The Stack For Fun And Profit", Phrack 49th Ed. File 14th of 16, Phrack.org, Nov. 1996
[6] 황석훈, "네트워크 이론과 해킹 기법", 도서출판 혜지원, 2002.
[7] 이현우, 정현철, "분산 환경에서의 서비스 거부 공격 분석서", KISA, 1999. 12.
[8] 전완근 외 2명, "MS-SQL 서버 웜 슬래머(Slammer) 공격 테스트 및 사고 대응", CERTCC-KR, 2003. 1.
[9] 이완희, "Windows NT/2000 시스템 해킹 분석 절차", CERTCC-KR, 2002. 11.
[10] Gilbert Alaberdian, "Hacker Society", Neo Corporation, 2000. 8.
[11] 해커스 랩, ""해커" 그것을 정의해 본다", (주) 해커스랩, 2001. 1. 17
[12] Lance Spitzner, "Know Your Enemy-The Tools and Methodology of the Script Kiddie", The HoneyNet2000. 7. 21
[13] 이현우, 김영직, 전숙, "UNIX 피해시스템 분석 및 침입자 모니터링 : Part I v1.0", CERTCC-KR, 2001.
[14] 정보보호올림페어 특별 취재반, "정보보호올림페어 2001 폐막", 정보보호21c 6월호,pp. 54-59, 2001. 6