온라인 게임 보안 강화

엔씨소프트

2003. 3. 18
김 동 균

Agenda

- 온라인 게임 해킹
- 네트워크적 보안 강화 방법
- 시스템적 보안 강화 방법
- 프로세스적 보안 강화 방법
- Q & A

- 기본적으로는 인터넷상에 존재하는 각종 해킹과 그에 상응하는 보안기법은 동일하다.
- MMORPG는 application특성상 동일한 공간과 시간에서 사용자들간의 상호작용에 의하여 진행되는 것인 만큼 그 작용에 의한 몇가지 특징적인 현상들은 존재한다.

- 게임해킹

- 주로 아이템 해킹
  계정도용을 통해서 사용자의 아이템을 빼내는 행위

- 해킹방법
  ① Key stoke hooking :
  클라이언트 PC에, 키보드 입력을 가로채어 비밀공간에 보관하거나 실시간으로 해커의 PC로 그 값을 전송케 하여 사용자 계정과 비밀번호를 가져가는 방법
  ② 운영자 사칭 :
  게임공간 안이나, 포럼의 게시판등에 운영자를 사칭하여 사용자의 각종 정보(게임내용,서버,계정,비밀번호등)를 속기 쉬운 메일계정으로 전송케 하여 유출 시키는 방법
  (예) lineage@hanmail.net, matis@golineage.com
  ③ 게임버그 이용 :
  Application 의 알려지지 않은 버그를 이용하여 아이템을 복사하거나, 취득하는 방법

- 게임방해

  - 상대방이 게임을 하지 못하는 상황을 만들어 게임을 의도대로 만드는 행위

  - 방해방법
    ① 공성전 방해 :
    공성전 당시에, 적 혈맹이 사용중인 PC방쪽에 대량의 네트웍 트래픽을 유발하도록 하는 행위
    (미리 해당 PC방 PC에 바이러스 프로그램을 심음)

- Fraud

  - 게임안에서 각종 거짓/술수/음모를 통한 아이템 취득

  - 방법은 너무나 다양하게 존재하며, 계속 개발(?)중에 있음

- 네트워크 , 서버 해킹

  - 타업계의 현황과 본질적으로 동일함

  - 최근에 두드러진 공격의 형태는 DDoS (분산 Dos)와 바이러스에 의한 자원 남용이 그것임

  - 특히 Windows 계열의 OS를 사용하는 서비스/사업장의 경우 더욱 취약하며 님다, 코드레드, SQL슬래머 등 최근의 가장 큰 이슈가 되었던 해킹들은 모두 DDoS형태의 바이러스임

7. 결 론

"완전 무결한 시스템은 존재하지 않는다."

- 지속적인 보안 관리 필요
  - 신속한 보안 패치
  - 보안 도구 이용
    - 취약성 검사 도구
    - 침입차단 및 침입탐지 시스템

위험 분석 → 보안 정책 → 보안 대책 → 보안 관리

- 위험 분석
  - 자산의 가치와 위협 및 취약점 분석

"보안 관리의 목표는 완전무결이 아니라
보안 위협으로 인한 피해를 최소화하고,
최대한의 가용성(availability)을
제공하는 것이다."

Hacker Academy 54 Copyright 2000 HackersLab Co., Ltd.

출처 : 해커스랩 보안교재 p.54

해킹에 관한 최근 동향

- 국가정보보호진흥원(KISA)에서 발간된 “2003년 2월 해킹바이러스 통계 및 분석 월보”에서 발췌
- 바이러스에 의한 피해건수가 전체의 86%
- Windows계열 OS에 대한 취약점 탐색이 급증하고 있는 추세

정점사항요약

ㅇ Netbus와 Subseven에 대한 사고는 감소한 반면 Opaserv 웜은 계속적으로 피해가 존재하고 있음
- Windows 사용자들의 취약점 패치 및 주기적인 점검 필요

ㅇ 구성설정 오류를 이용한 공격은 증가한 반면 악성프로그램을 이용한 공격은 감소하였음

- Null 패스워드 및 메일 릴레이 허용 등의 구성설정 오류 등에 의한 피해가 증가하므로 사용자는 반드시 패스워드를 설정하고 올바른 구성설정 여부를 체크해야 함

ㅇ 2월의 CERTCC-KR 신고접수 특징은 슬래머 웜이 기승을 부렸던 1월에 비해 신고접수가 감소하였으나 여전히 Klez, Opaserv, 그리고 Nimda에 대한 사고접수는 꾸준히 되고 있음

- W32.Opaserv.Worm의 변종인 W32.Opaserv.K는 Windows 95/98/Me 운영체제가 지니고 있는 패스워드 취약점을 이용하여 패스워드가 없거나 패스워드가 쉽게 설정되어 있는 네트워크상에 공유된 드라이브나 폴더를 대상으로 전파되고 있으므로 이용자들의 주의가 필요함

- 과거의 웜이 아직 수그러들지 않는 이유는 아직도 많은 사용자들이 백신을 사용을 하지 않거나 백신엔진 갱신을 하지 않는 것으로 판단

ㅇ 2월 한달간 바이러스로 인한 피해신고 건수는 총 3,238건으로 전월의 86%수준

- mIRCpack 등 IRC(채팅서버) 관련 트로이목마 피해 감소(683->125)
- Opaserv 등 네트워크 공유 취약점을 이용한 웜 피해 지속

ㅇ 국내로부터의 스캔탐지는 지난1월보다 전체 스캔탐지 건수가 감소하였음
- Windows 계열 NetBios 관련 TCP 445 포트스캔 증가
- 슬래머 웜에 대한 스캔은 감소하였음
- 국내에 출발한 스캔공격의 대부분은 미국 및 일본을 목표로 하고 있음

ㅇ 국외로부터의 스캔탐지는 지난 1월보다 22%증가(147 -> 179)하였으며 특히 21, 445번 포트 스캔이 급증하였음
- ftp취약점(21번) 스캔이 55건으로 가장 많았고
- Windows NetBios 포트(445번)이 26건으로 2위

- 방화벽은 신중하게 투입하자

  stateful infection을 사용하는 방화벽이라 할지라도 온라인게임의 특성상
  조그만 packet이 수많이 지나다니는 환경에서는 성능의 저하를 감수해야 한다.
  * 리니지의 한 개 서버의 평균 packet size : 36.74 bytes(서버→클라이언트)
  9.04 bytes (클라이언트 → 서버)
  약 4,869 pps (packet per second)

- 좋은(?) 라우터에서 ACL을 이용하라

  ASIC에서 동작하는 라우터의 ACL은 방화벽보다는 처리 능력이 뛰어나고
  운영경험적으로 투자대비 효율성이 가장 좋은 것으로 평가되었다.
  GSR12016의 게임용 interface에서 약 30만 pps 정도를 무리없이 처리중에 있음

- 네트워크 지연에 민감한 게임트래픽과 기타 트래픽은 회선/라우터를 분리하라

  라우터 ACL이 복잡해지는 것을 방지하기 위함이고, 실제로 게임회선과 웹서버 및
  기타 메일서버등이 사용하는 회선을 분리하여 운영함으로써 라우터의 보안적 부담을
  해소시킬 수 있다.

네트워크 보안 강화

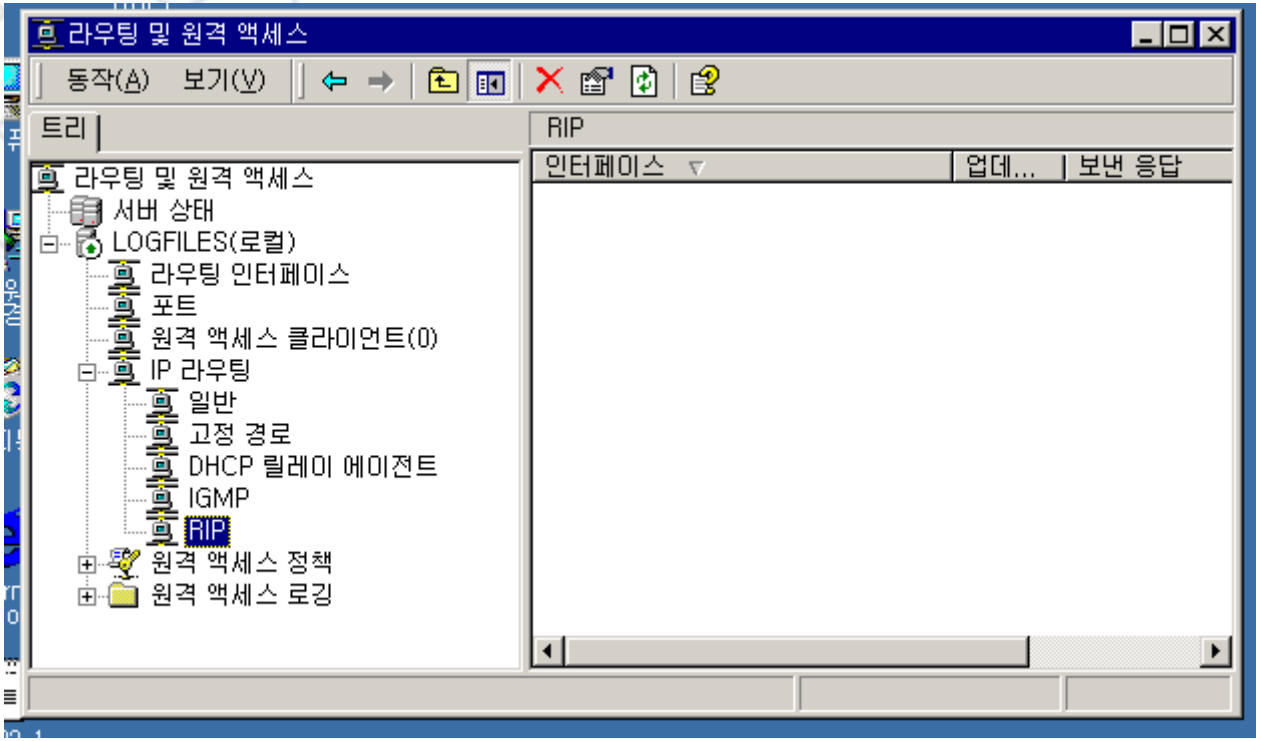
- 라우터의 접근에 대한 보안강화는 AAA로
  라우터 접근에 대한 AAA(Authentication, Authorization, Accounting)를 통하여 인증, 권한, 로깅을 시행하여 라우터 자체에 대한 보안을 강화한다.

- 벤더 보안권고 사항에 대하여 지속적인 IOS 업그레이드를 시행한다
  민감한 부분이긴 하지만, 보안관련 허점이 발견되고 그에 대한 IOS가 발표되면 테스트를 통하여 단계적인 업그레이드를 시행한다.

- MRTG를 통하여 정상상태에 대한 수준을 정확히 파악하고 있어야 한다
  백본 주요구간 및 ISP회선에 대한 pps, bps 를 측정하여 시각적으로 볼 수 있도록 MRTG를 사용하여 상시적인 모니터링을 시행하고 최고/최저/평균 등의 정상 서비스 상태를 파악하고 있으면서 이상징후가 발견될 때를 잡아내도록 한다.

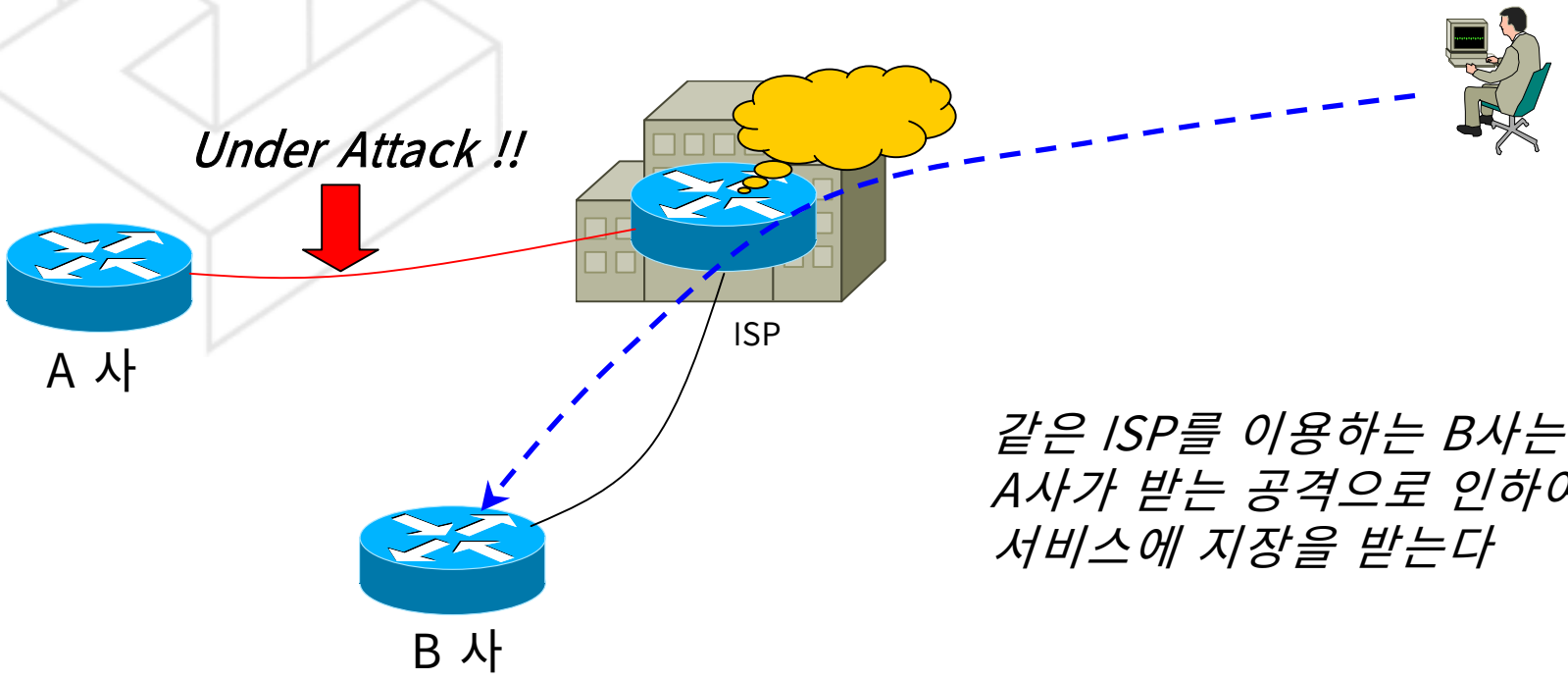
- # Backend network을 구성하라

Frontend server (웹서버, 게임서버)와만 통신이 필요한 시스템들은 인터넷과 분리된 내부 네트워크로 구성하여 연결한다.
내부네트워크가 복잡해지고 서브넷이 많이 추가된다면, 서버쪽에서 라우팅관련 서비스를 활성화시켜서 라우팅 정보를 전파시킨다.



- 게임업계 네트워크 관리자들간의 인적 네트워크를 구축하자

해킹/바이러스가 발생하면 업계의 네트워크 관리자들간의 신속한 정보와 대책 공유를 통하여 심각한 서비스 중단 사태를 미연에 방지해야 한다.



같은 ISP를 이용하는 B사는 A사가 받는 공격으로 인하여 서비스에 지장을 받는다

서버 보안 강화

- 표준 설치 가이드와 체크리스트를 운영하라

  각각의 사이트의 특성에 맞는 시스템 표준 설치 가이드를 운영하고, 각 시스템이 설치될 때 반드시 체크리스트를 이용하여 각각의 항목들을 점검하여 엔지니어의 경험에 의존하여 누락 될 수 있는 보안 위협 요소를 최소화해야 한다. 실제 운영에서 가장 큰 효과를 본 부분이다.

- Windows Hotfix와 Patch에 늘 관심을 가지고 릴리즈되면 바로 적용을 검토하라

  windows계열의 OS를 사용하는 사업장의 시스템관리자는 MS와 각종 보안사이트(cert-cc, kisa)에서 발견되는 각종 버그/바이러스 정보를 경청하고 MS에서 릴리즈되는 패치에 대해서는 능동적으로 적용할 수 있는 마음 자세가 필요하다.

- 그 외 필요에 따라서 각종 자료에서 권고하는 보안 사항을 적용하라

  윈도우NT/2000 서버보안-인터넷편, 한경민 저, 한빛미디어
  2003.02 KIDC 고객교육 – 윈도우 시스템 보안

서버 보안 강화

엔씨소프트에서 운영하는 작업요청서와 시스템설치 확인서의 예