서버 관리자용 침해 사고 대응 방법 요점 정리

침입이 의심되는 시스템을 검사하고, 사고 대응 절차에 돌입할지 말지 결정하는데 필요한 팁 모음

침입이 의심되는 상황에서 확인하는 방법

공격자의 침입 흔적을 그대로 보존해야 하므로, 가급적 파일에 접근하지 말고, 도구를 설치하지 말 것

시스템, 애플리케이션 로그에서 특이한 이벤트를 볼 것

네트워크 설정과 연결 상태를 확인할 것. 특이한 설정, 세션, 포트를 주의 깊게 볼 것.

사용자 중 특이하거나, 비활성화된 계정을 살펴볼 것

작동하는 프로세스와 예약된 작업 중에 특이한 것을 볼 것

자동으로 시작되는 특이한 프로그램을 볼 것

ARP 와 DNS 설정을 확인할 것; 설정파일에 포함되어있지 않은 설정이 있는지 볼 것

특이한 파일을 확인하고, OS 와 애플리케이션에 관련된 파일들의 무결성을 확인할 것

시스템에 설치되어 있거나, 별도로 사용 가능하다면 네트워크 스니퍼를 이용 해 특이한 활동을 확인할 것

루트킷이 공격을 숨길 수 있다; 시스템의 상태가 좋지 않다고 느낀다면, 당신의 감을 믿을 것

최근에 보고된 문제, 침입 탐지, 경고 등을 살펴볼 것.

만약 공격 당했다고 생각한다면

다음 단계로 넘어가기 위해 사고 대응 전문가를 부르고, 당신의 상관에게 보고할 것

부주의한 실수를 하지 않도록 집중할 것

네트워크를 끊어 진행중인 공격을 막을 것. 시스템을 끄거나 재부팅 하지 말 것.

무엇을 관찰했는지, 어떤 상황에 처했는지 기록을 남겨서 나중에 돌아볼 수 있도록 할 것

윈도우 시스템 초기 검사 방법

이벤트 로그 보기	`Eventvwr`
네트워크 설정 상태 살펴보기	`arp -a`, `netstat -nr`
네트워크 연결 목록 및 자세한 내용 보기	`netstat -nao`, `netstat -vb`, `net session`, `net use`
사용자와 그룹 목록 보기	`lusrmgr`, `net users`, `net localgroup administrators`, `net group administrators`
예약된 작업 보기	`schtasks`
자동 실행 프로그램 보기	`msconfig`
프로세스 목록 보기	`taskmgr`, `wmic process list full`
서비스 목록 보기	`net start`, `tasklist /svc`
DNS 와 호스트 설정 보기	`ipconfig /all`, `ipconfig /displaydns`, `more %SystemRoot%\System32\Drivers\etc\hosts`
OS 관련 파일 무결성 확인	`sigverif`
최근에 변경된 파일 찾기	`dir /a/o-d/p %SystemRoot%\System32`

탐색기가 파일과 시스템의 내용을 바꾸므로, 탐색기를 사용하지 말고 명령창을 쓸 것

유닉스 시스템 초기 검사 방법

이 디렉토리에 있는 로그 파일 보기	`/var/log`, `/var/adm`, `/var/spool`
최근 보안 이벤트 보기	`wtmp`, `who`, `last`, `lastlog`
네트워크 설정 살펴보기	`arp -an`, `route print`
네트워크 연결 목록 및 자세한 내용 보기	`netstat -nap` (Linux), `netstat -na` (Solaris), `lsof -i`
사용자 목록 보기	`more /etc/passwd`
예약된 작업 보기	`more /etc/crontab`, `ls /etc/cron.*`, `ls /var/at/jobs`
DNS 와 호스트 설정 보기	`more /etc/resolv.conf`, `more /etc/hosts`
설치된 패키지의 무결성 확인	`rpm -Va` (Linux), `pkgchk` (Solaris)
자동 시작 서비스 보기	`chkconfig --list` (Linux), `ls /etc/rc*.d` (Solaris), `smf` (Solaris 10+)
프로세스 목록 보기	`ps aux` (Linux, BSD), `ps -ef` (Solaris), `lsof +L1`
최근에 변경된 파일 찾기	`ls -lat /`, `find / -mtime -2d -ls`

사고 대응을 위한 통신 방법

관련 내용을 담당 부서 제외한 다른 사람과 공유하지 말 것

암호화 되지 않은 상태에서 이메일이나 메신저로 민감한 데이터를 전송하지 말 것

네트워크가 공격 당했다면, VoIP 전화기 같은 것을 사용하지 말고, 다른 방법으로 통신 할 것

사고 대응 핵심 단계

1. 준비: 필요한 도구를 모으고, 사용방법을 익힌다. 사고가 발생한 환경에 대해 익숙해진다
2. 확인: 사고 범위를 확인하고, 필요한 사람을 소집한다
3. 억제: 사고가 끼치는 영향이 최소화 되도록 조치한다
4. 퇴치: 공격을 퇴치하고, 필요하다면 복구 작업을 한다
5. 복구: 시스템을 정상 상태로 복구한다, 필요하다면 시스템을 재설치 하거나 백업본을 사용한다
6. 마무리: 사고의 상세한 내용을 정리하고, 수집한 내용과 사고로 배운 교훈에 대한 이야기를 나눈다

기타 사고 대응 관련 자료

윈도우 시스템 침입 탐지 요점 정리
http://sans.org/resources/winsacheatsheet.pdf

윈도우 시스템 침입 흔적 찾기
http://www.ucl.ac.uk/cert/win_intrusion.pdf

리눅스 시스템 침입 탐지 요점 정리
http://sans.org/resources/linsacheatsheet.pdf

리눅스/유닉스 시스템 침입 흔적 찾기
http://www.ucl.ac.uk/cert/nix_intrusion.pdf

Authored by Lenny Zeltser, who leads a security consulting team at SAVVIS, and teaches malware analysis at SANS Institute. Special thanks for feedback to Lorna Hutcheson, Patrick Nolan, Raul Siles, Ed Skoudis, Donald Smith, Koon Yaw Tan, Gerard White, and Bojan Zdrnja. 한국어 번역, 구동언 8con@nchovy.kr