메일서버의 SPAM RELAY TEST

해킹바이러스 상담지원 센터 cert@certcc.or.kr
김상철 kims@certcc.or.kr

1. 개요

E-Mail의 보편화와 맞물려서 스팸(Spam)메일이라 일컬어지는 악성 광고메일이 요즘 극성을 부리는 통에 메일서버 관리자들(Postmasters)은 메일 송수신 에이전트(MTA : Mail Transport Agent) 프로그램의 환경 설정 방법에 많은 주의를 기울일 필요가 있다. 많은 관리자들은 메일서버를 설치시 Anti-Spam 메일서버의 정확한 설치와 환경설정방법을 몰라 메일서버가 스팸 릴레이 서버로 이용되는 불미스러운 일이 발생하기도 한다. 뿐만아니라 국내 메일 서버들이 스팸메일 서버로 오인되게끔 하여 메일 서버로서의 제 기능을 담당하지 못하도록 하는 일이 종종 발생하기도 한다.

이 문서에서는 국내에서 보편적으로 많이 사용되는 메일서버의 메일 릴레이 테스트방법에 대하여 서술하였으며, 각각의 메일서버가 릴레이되고 있는 경우에는 참고문헌 사이트를 통하여 메일서버관리자들에게 대응방법을 제공하고자 하였다.

2. Mail Relay 테스트

아래의 스크립트는 kisa.or.kr(211.252.150.11)의 위치에서 실행되는 메일 릴레이 테스트의 세부명령 및 명령어의 실행결과에 대한 상세내용을 보여준다. 메일 릴레이 테스트를 위해 사용된 MTA (172.16.4.140 : certlinux.certcc.or.kr)는 Sendmail 8.11.0을 사용하였다. ksch90@korea.com은 현재 테스트를 위해 사용되고 있는 korea.com의 웹메일 계정이다. 다음의 시험들은 현재 사용되고 있는 MTA가 외부에서 Spam 메일 릴레이로 악용될 취약점이 있는지를 체크하도록 구성되어졌다. 아래의 19가지 시험 항목중에서 하나 이상의 시험 결과에 성공하였다면 해당 메일서버가 스팸메일서버로 악용될 취약점을 갖고 있음을 의미한다. 그렇기 때문에 해당 기관의 보안정책을 잠재적으로 위반하게 될 것이다. 당신의 메일 서버가 메일 릴레이에 취약하다면 3절의 "문제해결"을 참조하여 대응하기 바란다.

이러한 메일 릴레이 테스트를 자동화 시켜주는 자동화된 메일 릴레이 테스트 도구들인 인터넷 상에 많이 공개되고 있다. 이러한 도구를 사용해서 테스트 하는 방법도 좋은 방법이지만 공개도구들에는 여러 가지 세부사항에 맞추어 테스트 하기가 어렵게 구성되어 있다.

이 스크립트 중에서 "<<<"는 실행결과를 표준 출력장치(모니터)에 출력된 결과를 의미하며, ">>>"는 표준입력장치(키보드)에 의해 입력되는 명령어를 의미한다.

```
[tomcat:root]:/ > telnet 172.16.4.140 25
Trying 172.16.4.140...
Connected to 172.16.4.140.
Escape character is '^]'.
<<< 220 certlinux.certcc.or.kr ESMTP Sendmail 8.11.0/8.11.0; Sun, 18 Feb 2001 23:54:18 +0900
>>> helo kisa
<<< 250 certlinux.certcc.or.kr Hello tomcat.cyber118.or.kr [211.252.150.7], pleased to meet you
>>> mail from:<ksch@certlinux.certcc.or.kr>
<<< 250 2.1.0 <ksch@certlinux.certcc.or.kr>... Sender ok
```

>>> rcpt to:<ksch90@korea.com>
<<< 550 5.7.1 <ksch90@korea.com>... Relaying denied
>>> rset
<<< 250 2.0.0 Reset state

이 테스트는 스팸 메일 릴레이의 가장 기본적인 테스트로서 사용되는 방법이다. 내부 도메인 및 내부 IP주소가 아닌 곳에서의 Relay 테스트가 "250 2.1.5 ksch90@korea.com... Recipient ok"로 응답하면 릴레이를 허용하는 것이므로 허용정책 설정을 반드시 재점검하여 "550 5.7.1 <ksch90@korea.com>... Relaying denied"메시지가 뜨도록 설정해 주어야만 한다. 이러한 설정방법에 대한 3절의 문제해결을 참조하기 바란다.

Relay test #1: 출발지와 목적지의 Email 주소가 동일한 경우의 릴레이 시도 테스트

>>> maill from:ksch@kisa.or.kr
<<< 250 2.1.0 ksch@kisa.or.kr... Sender ok
>>> rcpt to:ksch@kisa.or.kr
<<< 550 5.7.1 ksch@kisa.or.kr... Relaying denied

Relay test #2 : 올바르지 않은 출발지 주소를 사용하여 시도할경우

>>> mail from: spamtest@spam.mail.kisa.or.kr
<<< 501 5.1.8 spamtest@spam.mail.kisa.or.kr... Sender domain must exist

Relay test #3 : 출발지 주소를 localhost 호스트명을 사용할 경우

>>> mail from: relaytest@localhost
<<< 553 5.5.4 relaytest@localhost... Real domain name required

Relay test #4 : 메일을 보내려고 하는 시스템이 로컬 도메인에 있는것처럼 속이기 위해 전체적인 도메인 이름을 생략하여 메일을 보내려고 할때

>>> mail from: <relaytest>
<<< 553 5.5.4 <relaytest>... Domain name required

Relay test #5 : 출발지 메일주소 없이 메일을 보내기 위한 시도

>>> mail from:<>
<<< 250 2.1.0 <>... Sender ok
>>> rcpt to:ksch90@korea.com
<<< 550 5.7.1 ksch90@korea.com... Relaying denied

Relay test #6 : 피해서버의 FQDN(Fully qualified domain name)을 출발지 주소로 지정하여 시도

>>> mail from: root@certlinux.certcc.or.kr
<<< 250 2.1.0 root@certlinux.certcc.or.kr... Sender ok
>>> rcpt to: ksch90@korea.com
<<< 550 5.7.1 ksch90@korea.com... Relaying denied

Relay test #7 : 피해 SMTP서버의 IP주소를 []를 사용하여 시도

>>> mail from: spamtest@[172.16.4.140]

<<< 250 2.1.0 spamtest@[172.16.4.140]... Sender ok
>>> rcpt to: ksch90@korea.com
<<< 550 5.7.1 ksch90@korea.com... Relaying denied

Relay test #8 : %스타일의 relay를 사용하여 시도. 많은 예전의 MTA들은 이러한 문법들을 지원할 수 있다.

>>>mail from:ksch@kisa.or.kr
<<<250 2.1.0 ksch@kisa.or.kr... Sender ok
>>>rcpt to:ksch90%korea.com@certlinux.certcc.or.kr
<<<550 5.7.1 ksch90%korea.com@certlinux.certcc.or.kr... Relaying denied

Relay test #9 : FQDN대신에 피해 SMTP서버의 IP주소를 사용하여 %스타일의 relay를 시도

>>> mail from:ksch@certlinux.certcc.or.kr
<<< 250 2.1.0 ksch@certlinux.certcc.or.kr... Sender ok
>>> rcpt to:ksch%kisa.or.kr@[172.16.4.140]
<<< 550 5.7.1 ksch%kisa.or.kr@[172.16.4.140]... Relaying denied

Relay test #10 : 이중인용부호("")를 사용하여 목적지 주소를 지정하여 relay를 시도

>>> mail from:ksch@certlinux.certcc.or.kr
<<< 250 2.1.0 ksch@certlinux.certcc.or.kr... Sender ok
>>> rcpt to:"ksch90@korea.com"
<<< 550 5.7.1 "ksch90@korea.com"... Relaying denied
>>> rcpt to:"ksch@kisa.or.kr"
<<< 550 5.7.1 "ksch@kisa.or.kr"... Relaying denied

Relay test #11 : %스타일의 문법과 이중인용부호("")를 사용하여 Relay를 시도

>>> mail from:ksch@certlinux.certcc.or.kr
<<< 250 2.1.0 ksch@certlinux.certcc.or.kr... Sender ok
>>> rcpt to:"ksch90%korea.com"
<<< 550 5.7.1 "ksch90%korea.com"... Relaying denied
>>> rcpt to:"ksch%kisa.or.kr"
<<< 550 5.7.1 "ksch%kisa.or.kr"... Relaying denied

Relay test #12 : 출발지 E-Mail주소의 호스트명이 피해SMTP 서버의 IP주소이고, 또한 목적지 E-mail주소가 이중인용부호를 사용된 @@ 릴레이 문법을 사용하여 릴레이 시도

>>> mail from:ksch@[172.16.4.140]
<<< 250 2.1.0 ksch@[172.16.4.140]... Sender ok
>>> rcpt to:"ksch90@korea.com@certlinux.certcc.or.kr"
<<< 550 5.7.1 "ksch90@korea.com@certlinux.certcc.or.kr"... Relaying denied

Relay test #13 : 목적지 E-Mail주소에 이중인용부호를 사용하고 피해 SMTP버서의 IP주소를 사용해서 relay 시도

>>> mail from:ksch@certlinux.certcc.or.kr
<<< 250 2.1.0 ksch@certlinux.certcc.or.kr... Sender ok
>>> rcpt to:"ksch90@korea.com"@[172.16.4.140]

<<< 550 5.7.1 "ksch90@korea.com"@[172.16.4.140]... Relaying denied

Relay test #14 : 인용부호 없이 Style을 사용하고 SMTP서버의 IP주소를 사용하여 릴레이 시도

>>> mail from:ksch@certlinux.certcc.or.kr
<<< 250 2.1.0 ksch@certlinux.certcc.or.kr... Sender ok
>>> rcpt to:ksch90@korea.com@[172.16.4.140]
<<< 550 5.7.1 ksch90@korea.com@[172.16.4.140]... Relaying denied

Relay test #15 : Relay를 허용할 수 있는 또다른 email syntax

>>> mail from:ksch@[172.16.4.140]
<<< 250 2.1.0 ksch@[172.16.4.140]... Sender ok
>>> rcpt to:@certlinux.certcc.or.kr:root@kisa.or.kr
<<< 550 5.7.1 @certlinux.certcc.or.kr:root@kisa.or.kr... Relaying denied

Relay test #16 : 피해 SMTP서버의 IP주소를 사용하여 릴레이를 허용할 수 있는 또다른 E-mail Syntax 방법

>>> mail from:ksch@certlinux.certcc.or.kr
<<< 250 2.1.0 ksch@certlinux.certcc.or.kr... Sender ok
>>> rcpt to:@[211.252.150.11]:root@kisa.or.kr
<<< 550 5.7.1 @[211.252.150.11]:root@kisa.or.kr... Relaying denied

Relay test #17 : E-mail 주소의 문법을 변조하고, IP주소가 출발지의 E-Mail주소로 사용하여 릴레이시도

>>> mail from:ksch@[172.16.4.14]
<<< 250 2.1.0 ksch@[172.16.4.14]... Sender ok
>>> rcpt to:<kisa.or.kr!root>
<<< 550 5.7.1 <kisa.or.kr!root>... Relaying denied
>>> rcpt to:kisa.or.kr!nobody
<<< 550 5.7.1 kisa.or.kr!nobody... Relaying denied
>>> rcpt to:kisa.or.kr!root
<<< 550 5.7.1 kisa.or.kr!root... Relaying denied

Relay test #18 : E-mail 주소의 문법을 변조하고 피해 SMTP서버의 IP주소를 목적지 주소로 사용하여 Relay 시도

>>> mail from:ksch@certlinux.certcc.or.kr
<<< 250 2.1.0 ksch@certlinux.certcc.or.kr... Sender ok
>>> rcpt to:kisa.or.kr!nobody@[172.16.4.14]
<<< 550 5.7.1 kisa.or.kr!nobody@[172.16.4.14]... Relaying denied

Relay test #19 : "Postmaster"의 계정이름을 사용하여 시도할 경우, 아마도 이러한 경우는 어떤 SMTP서버는 특별한 경우로 취급되어져서 릴레이가 허용될 수 도 있다.

>>> mail from:postmaster@certlinux.certcc.or.kr
<<< 250 2.1.0 postmaster@certlinux.certcc.or.kr... Sender ok
>>> rcpt to:root@kisa.or.kr
<<< 550 5.7.1 root@kisa.or.kr... Relaying denied

3. Fix The Problem (문제 해결)

이 절에서는 국내에서 가장 보편화 되어 많이 사용되는 MTA에 대해서만 언급하였다. UNIX기반에서는 sendmail, exim에대해서만 기술하였거, Window Workgroup에서는 EMWAC와 Microsoft의 Exchange Server에 대해서만 기술 하였다.

3.1 UNIX

3.1.1 Exim

o Status : Freely Avaliable

o Systems : UNIX

o Info : http://www.exim.org

o Description :

Exim MTA의 장점들은 메일 필터링과 메일의 효과적인 처리능력에 있다. 최근 버전은 디폴트로 메일 릴레이가 차단되도록 설정되어 있다. 호스트, 도메인, 네트워크에 대한 릴레이를 제어하기 위한 몇가지의 환경 설정 옵션들이 있다. 이러한 옵션들을 설정하는 방법들을 기술하고 있는 다음의 사이트 정보를 참조하기 바란다. (http://www.exim.org/howto/relay.html)

또한 Exim은 사용자로 보내어지는 Spam을 줄이기 위한 다양한 MAPS 필터기능을 사용할 수 있다. 더 자세한 정보는 다음의 howto문서를 참조하기 바란다. (http://www.exim.org/howto/rbl.html)

3.1.2 Sendmail Version 8

o Status : Freely Avaliable

o Systems : Unix

o Info : http://www.sendmail.org

o Description :

버전 8.8.4이전의 버전은 해킹취약점이 존재한다. 심지어 전체적으로 안전하지 않은 MTA이므로 Upgrade하기 바란다.

8.8.x버전에 대한 Ruleset들은 sendmail.org에 있는 Claus Asmann의 웹사이트 (http://www.sendmail.org/~ca/email/check.html)를 방문하면 관련된 최신의 정보들이 있다. 물론 다른 사이트들도 관련된 많은 좋은 정보들이 있지만 Calus의 사이트가 가장 빈번하게 자료를 업그레이드하는 경향이 있다. 그리고 8.8.x버전들이 동작하고 있는 많은 사이트들이 anti-relay구성설정 기능을 추가하였지만, 여전히 해킹당할 가능성이 있다.

또다른 좋은 접근방법중의 하나는 POP 패스워드를 사용하여 그들 자신들을 인증한 사용자들에게만 메일서버의 접근을 하도록 제한하는 것이다. 이것은 소위 POP-before-SMTP 솔루션이라 불리는 방법이다. 이렇게 사용하기 위해서 sendmail의 환경설정을 하는 것이 복잡하다 할지라도 "roaming" 사용자들를 가진 프로바이더(Provider)들에게는 훌륭한 솔루션중의 하나라 할 수 있다.

http://spam.abuse.net/tools/smPbS.html

8.9.0버전에서는 디폴트로 메일 릴레이 기능을 제한하도록 되어 있으며 이러한 기능들을 제어하기 위한 많은 환경변수들을 제공한다. 이러한 환경파라미터들의 설정을 올바르게 사용하기 위해서는 cf/README 파일을 Anti-Spam configuration Control부분을 참조하기 바란다.

(http://www.sendmail.org/m4/anti-spam.html)

o Caution :

대부분의 이러한 Anti-Spam Relay 솔루션들은 메일관리자가 허용되는 Relay 도메인들의 리스트들을 설정하는 것을 필요로 한다. 이 리스트에는 보든 허가 인증된 도메인들를 포함하고 있는지 반드시 확인하여야 하며 주의하여야 할점은 반드시 MX (Mail Exchanger)뿐만 아니라 당신의 도메인에서 사용하고 있는 가상의 도메일들이 포함되도록 설정하여야 한다. 그렇지 않으면 당신이 보낸 메일이 거절될 수도 있을 것이다.

당신의 메일 서버가 FEATURE(relay_entire_domain)을 사용해서 8.9.x버전 이상의 sendmail을 구성하였다면, 이는 당신의 도메인내에 있는 모든 호스트로부터의 릴레이를 허용한다는 것을 의미한다. 만약 "relay_entire_domain"이 호스트 이름("host." : host.domain.com)을 사용한다면 불행히도 디폴트로 sendmail은 당신의 시스템에 있는 모든 IP 주소를 체크해서 "reverse lookups"를 수행한다. 메일서버의 시스템부하를 가중시키게 될 것이다. Spam Relay의 가장 좋은 해결방법은 .cf파일을 포함하여 relay_entire_domain을 사용하는 대신에 IP주소를 사용하여 Relay호스트를 설정하는 것이 설정상의 오류를 해결할 수 있는 좋은 방법이 될 수 있다..

3.2 Windows

3.2.1 EMWAC IMS

o Status : Freeware

o Systems : Windows

o Info : http://www1.sica.com/IMS

o Description :

EMWAC(European Microsoft Windows NT Academic Centre : http://emwac.ed.ac.uk/)는 무료용 Window/NT 메일서버인 IMS(Internet Mail Server)를 만들었다. 가장 최근 버전인 0.83는 허가되지 않는 메일 릴레이 차단을위한 해결책을 제공하지 않는 단점이 있다. 그래서 SICA Consulting Service (http://www.sica.com/)는 이 문제에 대한 가능한 해결책으로 add-on서비스를 제공하였다. 첫 번째로 IMS에 필터링 기능을 부여해주는 SCMSFILTER (http://www.sica.com/freestuf/scsmfilt.htm)를 설치하고 나서 Gorden Fecyk의 Antirelay Plugin을(http://www.orca.bc.ca/win95/antirelay.zip) 설치하면 스팸릴레이에 대한 문제점을 해결할 수 있을 것이다.

3.2.2 Microsoft Exchange Server

o Status : Commercial (Microsoft Corp.)

o Systems : Win/NT

o info : http://www.microsoft.com

o Description :

Version 5.0은 릴레이에 취약하다. 다시 말하면 Exchange Server 5.0이 인터넷상에 연결되어 있으면 외부의 스팸메일 공격자에게 relay를 허용할 것이다.

5.5 버전부터 허가되지 않은 relay를 예방할 수 있는 기능을 지원한다. 이러한 Anti-Relay 에 대한 상세한 설명은 다음 사이트를 참조하기 바란다.

(http://www.microsoft.com/technet/exchange/relay.asp)

만약 당신의 Exchange Mail Server가 5.5버전 보다 낮은 버전을 사용하고 있다면 지금 업그레이드해야만 한다.

4. 참고 문헌 및 웹사이트

[1] http://sendmail.net/
[2] http://sendmail.org/
[3] http://www.whitehats.com/library
[4] http://www.rahul.net/falk/index.html
[5] http://www.plus.or.kr
[6] http://www.exim.org/
[7] http://www1.sica.com/IMS/
[8] http://www.microsoft.com/

Korea Computer Emergency Response Team Coordination Center : CERTCC-KR, cert@certcc.or.kr