LKD
Şenlikleri
2002

İleti Sunucuları Seviyesinde Virüslü İletilerden Korunmak

Oğuz YILMAZ
Teknoloji Danışmanı
oguz.yilmaz@gantek.com

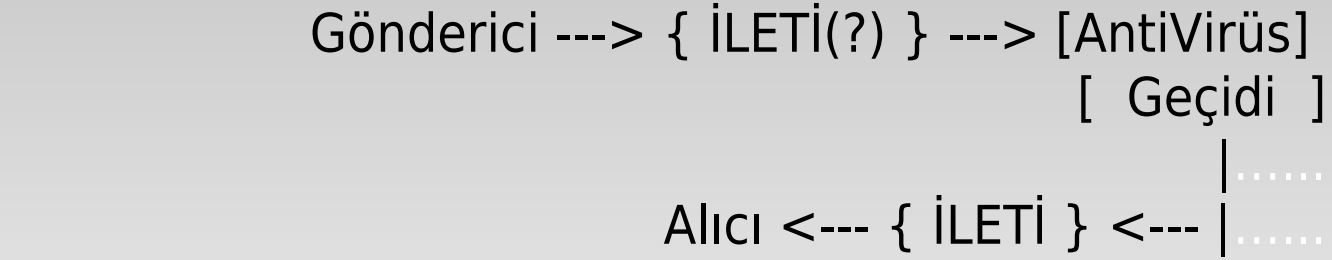
LKD Şenlikleri 2002

İleti Sunucuları Seviyesinde Virüslü İletilerden Korunmak

- Virüsler, Nasıl Yayılır?
- Nasıl Bir Çözüm?
- İleti Sunucular ve UNIX
- AMaViS - A Mail Virus Scanner
- Bir Uygulama Örneği
- Diğer AntiVirüs Geçidi Çözümleri
- İnternet Bağlantıları

- Virüsler = Bilgisayar programları...
- Virüsler nasıl yayılır?
  - İnternet'ten yüklenen dosyalar
    - İletiler
      - Virüslü çalıştırılabilir dosyalar(.exe ...)
      - Virüslü çalıştırılabilir betikler(.vbs ...)
      - Virüs içerebilecek diğer dosyalar(.doc ...)

- Yayılma nasıl engellenebilir?
  - Kullanıcı virüslü iletiyi almadan virüs kontrolü yap



  - Kullanıcı platformu önemsiz

- Dünyadaki ileti sunucuların %90+ UNIX

sendmail	%55
qmail	%17

- İletiyi alır
- Eklentileri ayıklar
- AntiVirüs programlarını çalıştırır

- Virüs yoksa iletiyi yoluna devam ettirir
- Virüslü ise iletiyi durdurur
- Kurulum

- İletiyi alır
  - sendmail
  - qmail
  - postfix
  - exim
- sendmail ya da postfix => çift yönlü (relay)

- Eklentileri ayıklar
  - MIME eklentileri için:
    metamail, reformime
    - olmayanlar için : doc/amavis.html#mime
  - Sıkıştırılmış dosyalar için:
    uudecode, compress, gunzip, unzip, unarj, unrar, xbin, LHArc, bunzip2, zoo, arc, tnef, freeze
    - olmayanlar için : doc/amavis.html#decomp
  - Tüm eklentileri bir geçici dizine koyar

- AntiVirüs programlarını çalıştırır

- Virüs yoksa iletiyi yoluna devam ettirir
  - yerel dağıtım ajanına gönder (local delivery agent)
- Virüslü ise iletiyi durdurur
  - İsteğe göre;
    Göndericiyi, alıcıyı, antivirüs yöneticisini bilgilendirir.
  - Virüslü iletiyi belirli bir dizine kaydet

- Kurulum (yerel dağıtım ajanı yöntemi)
  - dal: v.x.x.x --> shell script
  - dal: amavis-perl-x --> Perl <---- önerilen
  - dal: amavisd --> Perl
- http://www.amavis.org/dist/perl/amavis-perl-11.tar.gz
- ./configure --disable-qmail --disable-postfix --disable-exim --with-origconf=/etc/mail/sendmail.cf --enable-syslog --with-syslog-level=mail.info --with-amavisuser=amavis --with-warnrecip
- make
- make install

- sendmail.cf

amaç 1: geçici olarak sendmaili 587 inci porttan çalıştırmak.

/etc/rc.d/init.d/sendmail stop

sendmail.cf yi düzenle:

```
# SMTP daemon options
O DaemonPortOptions=Name=MTA
O DaemonPortOptions=Port=587, Name=MSA, M=E
                    --------değiştir---------
# SMTP daemon options
#O DaemonPortOptions=Name=MTA
#O DaemonPortOptions=Port=587, Name=MSA, M=E
O DaemonPortOptions=Port=587
```

- sendmail.cf

amaç 2: amavisi yerel dağıtım ajanı olarak göstererek iletileri amavise iletebilmek

```
Mlocal, P=/usr/bin/procmail, F=lsDFMAw5:/|@SPfhn,
S=10/30, R=20/40, T=DNS/RFC822/X-Unix,
A=procmail -Y -a $h -d $u
```

---------değiştir-------->

```
Mlocal, P=/usr/sbin/scanmails, F=lsDFMAw5:/|@SPfhn,
S=10/30, R=20/40, T=DNS/RFC822/X-Unix,
A=scanmails -Y -a $h -d $u
```

amaç 3: test
/etc/rc.d/init.d/sendmail start

- Kurulum (filtreleme birimleri yöntemi)

Postfix: content_filter

Sendmail: milter

http://www.amavis.org/dist/perl/amavisd-snapshot-20020300.tar.gz

- ./configure --enable-postfix --enable-syslog --with-smtp-port=10025 --with-amavisuser=amavis --with-warnrecip
- make, make install

- Postfix main.cf:

content_filter = vscan:

- Postfix master.cf:

vscan unix - n n - 10 pipe
user=amavis argv=/usr/sbin/amavis ${sender} ${recipient}

localhost:10025 inet n - n - - smtpd
-o content_filter=

- Sistem başlangıcı:

su - amavis -c "/usr/sbin/amavisd"

- test

Netscape'de;

outgoing mail server: localhost:587

yeni ileti;

eklenti: http://www.eicar.org/download/eicar.com

yolla...

eicar.com:

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

- test

```
root@test3:/# telnet localhost 587
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 test3.local.ankara.gantek.com ESMTP Sendmail 8.11.3/8.11.3; Sat, 21 Apr 2001
16:56:41 -0200 (GMT)
helo localhost
250 test3.local.ankara.gantek.com Hello localhost [127.0.0.1], pleased to meet you
mail from: nobody@linux.org.tr
250 2.1.0 siz@lkd.org.tr... Sender ok
rcpt to: root
250 2.1.5 root... Recipient ok
data
354 Enter mail, end with "." on a line by itself
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
.
250 2.0.0 f3LIv5Q04395 Message accepted for delivery
QUIT
221 2.0.0 test3.local.ankara.gantek.com closing connection
Connection closed by foreign host.
```

- tamam?

1- Antivirus yöneticisi:

Super-User FOUND VIRUS IN MAIL -f siz@linux.org.tr -d root

2-Gönderici, Alıcı: Özelleştirilebilen iletiler...

3-Virüslü ileti bir dizine kayıt edildi

4-Kayıt dosyalarına satırlar eklendi

TAMAM! :)

- tamam değil! :(

kayıt dosyalarına bak

Yazma-çalıştırma izin problemleri !

amavis-user ileti listesi arşivleri
http://marc.theaimsgroup.com/?l=amavis-user&r=1&w=2

amavis-user ileti listesi

dene

TAMAM! :)

UNIX ler için antivirüs programları

- H+B EDV AntiVir/X (http://www.antivir.de/)
- Sophos Sweep (www.sophos.com)
- Network Associates VirusScan(uvscan) (www.nai.com)
- Trend Micro File Scanner (www.trendmicro.de)
- CyberSoft VFind (www.cyber.com)
- KasperskyLab AVP (www.kasperskylab.ru)
- DataFellows F-Secure Antivirus (www.f-secure.com)
- Computer Associates InoculateIT (www.cai.com)
- Panda Antivirus (www.pandasoftware.com)
- Norton Antivirus

Diğer Antivirüs Geçitleri

- H+B EDV AntiVir MailGate (http://www.antivir.de/)
- Trend Micro Interscan Viruswall (www.trendmicro.de)
- KasperskyLab AntiVirus For Mail Servers (www.kasperskylab.ru)
- DataFellows F-Secure Antivirus (www.datafellows.com)
- Mail::IspMailGate (CPAN'den www.cpan.org)
- Qmail Scanner (qmail-scanner.sourceforge.net)
- Inflex (www.spyda.co.za/inflex)
- GeCAD Antivirus for sendmail/qmail/postfix
- Symantec
- Aladdin E-Safe

İnternet Bağlantıları

- http://www.amavis.org
- http://www.openantivirus.org
- http://www.openantivirus.org/av-unix_e.txt
- http://av-linux.w3.to
- http://www.decros.cz/~reho/check_virus/ (başka bir proje)
- http://marc.theaimsgroup.com/?l=amavis-user&r=1&w=2&b=200101
  --> benchmarks

Sunum Powerpoint dosyasına ve bağlantılar listesine ***http://seminer.linux.org.tr/*** 'den ulaşabilirsiniz.

-o-

Tüm sorularınız için

oguz.yilmaz@gantek.com
o.yilmaz@ieee.org