网络安全检测的理论和实践（一）

卿斯汉 （中科院信息安全技术工程研究中心主任/研究员）

编者按：

信息化和网络化是当今世界发展的大趋势，由于因特网所具有的开放性与共享性，其安全性也成为人们日益关切的问题。在世界范围内，针对计算机网络的攻击层出不穷，网络犯罪日趋严重。我国信息化、网络化建设在技术与装备上对别国的极大依赖性，使网络安全问题尤为突出。因此，增强全社会安全意识，普及计算机网络安全教育，提高计算机网络安全技术水平，促进计算机网络安全的自主研发创新，是一项十分重要的课题。

有鉴于此，本刊从这一期开始，设立“系统安全”栏目，连载有关信息安全的系列文章，邀请我国著名信息安全专家卿斯汉研究员执笔，就有关信息安全的重要问题，作较为全面和深入的阐述，以飨读者。

1 信息安全保障

网络安全的防护手段多种多样，例如，密码技术、安全协议、防火墙、安全WEB服务器等等。但是，单纯依靠防御是不够的，我们必须重视保障网络的整体安全。对于攻击者，他总是选择网络安全最薄弱之处进行攻击，但对于防卫者，他要设法使整个网络没有明显的安全漏洞。对于攻击者，他可以选择他认为最适宜的时间进行攻击，但对于防卫者，他必须全天候地保障网络的安全。对于攻击者，他可以只应用一种技术或几种技术，就可以入侵一个网络，但对于防卫者，他必须防备入侵网络的全部手段。网络安全系统不但需要针对已知的黑客入侵技术，还需要智能地防备新的攻击方法。因此，保障网络安全应该是比黑客入侵更加困难的任务。

其次，网络安全的技术不断发展，新的技术不断出现，网络攻击和反攻击的技术也互为依存地不断发展。例如，生物认证技术逐渐渗入网络安全领域。EyEDentify公司生产视网膜认证产品；全世界有十余家公司开发虹膜认证产品；多达三十余家公司生产指纹认证产品，并应用了许多新技术，诸如神经网络技术、模糊逻辑技术、超声扫描技术等。目前，Visa、Mastercard等大的信用卡公司，均在积极筹备拟在银行卡中采用上述生物认证技术。电子商务（e-commerce）在全球继续快速发展，PKI（公开密钥基础设施）技术、保障电子商务应用安全的技术被广泛应用。与此同时，针对电子商务安全的攻击技术也在相应发展。此外，移动商务（m-commerce）的概念正在兴起，以“兰牙（blue teeth）”计划为契机，低成本、近距离、无线接入成为新的时尚。但是，随之而来的问题又与安全有关。移动通信的安全问题、移动通信和电子商务结合的安全问题、无线－PKI（无线公开密钥基础设施）技术等，成为热门话题。新的需求呼唤无线通信安全标准，在这种背景下，1999年12月，建立了MESC（移动电子签名协议），参与者包括：Siemens、Nokia、Motorola、Ericsson、Brokat、Mannesmann等著名公司。

共享和安全历来就是一对矛盾，效率和安全也是一对矛盾。高安全等级是以牺牲共享程度和效率为代价的。系统和网络越安全，共享程度就越差，效率就越低（时间越慢，存储空间越多），应用就越不方便。

由以上的讨论可知，要求一个内部网络绝对安全是不可能的，也是不现实的。保障网络安全应当从系统工程的角度考虑，在此背景下，美国国防部（DoD）提出了“信息安全保障（Information Security Assurance）”的概念，它由4个部分组成，即防护（Protect）、检测（Detect）、反应（React）和恢复（Recovery），简称PDRR原则。

PDRR原则指出，保障信息安全是一项系统工程，单单依靠防火墙等防护工具是不够的。防护仅仅是信息安全保障完整链条中的一个环节，是保障信息安全的第一步。一方面，我们应当在网络中部署防火墙等安全防护产品，另一方面，同样重要的是，我们应当不断进行实时的检测，看看网络中出现了哪些安全漏洞，遭受到何种类型的网络攻击。一旦受到攻击，应当迅速反应，采取一切必要的措施，使网络攻击产生的损失降到最低，并设法查出攻击者。最后，由于没有一个绝对安全的系统或网络，因此，我们必须作好最坏的打算，作好恢复、甚至是灾难恢复的准备。一旦网络遭到破坏，应当尽快恢复系统和网络的正常运行。

2 黑客入侵网络的基本方法

2.1 端口扫描

端口扫描的目的是找出目标系统上提供的服务列表。它逐个尝试与TCP/UDP端口建立连接，然后根据端口与服务的对应关系，综合服务器端的反应判断目标系统上运行了哪一种服务。黑客应用的端口扫描程序很多，例如SATAN中有一种，它对TCP端口的扫描过程如表1所示。

表 1　TCP 端口的扫描过程

```
# tcp_scan ercist.com 1-65535
7:echo:
9:discard:
13:daytime:
19:chargen:
21:ftp:
23:telnet:
79:finger
111:sunrpc:
512:exec:
513:login:
514:shell:
515:printer:
540:uucp:
2049:nfsd:
4045:lockd:
6000:xwindow:
6112:dtspc:
7100:fs:
......
```

在端口扫描程序运行的结果中，如果发现下列服务：

finger, sunrpc, nfs, nis(yp), ftp, telnet, http, shell(rsh), login(rlogin), smtp, exec(rexec) ......则应引起特别注意。利用端口扫描，还可以大致判断目标主机的操作系统类型，如表2所示。

表 2　操作系统类型与端口开放情况

端口 / 操作系统	7(echo)	13(daytime)	21(ftp)	135	139
UNIX	Y	Y	O	N	N
Windows NT	N	N	O	Y	Y
Windows 95/98	N	N	N	N	Y

TCP端口扫描的方式有以下几种：

(1) TCP Connect扫描。这是最简单的扫描方式，扫描程序依次尝试和要扫描的各端口建立正常的TCP连接。如果成功，则说明该端口开放，否则端口不开放。表1中的端口扫描程序tcp_scan就是用这种方式实现的。

(2) TCP SYN扫描。又名半开扫描（half-scan），因为它不完成一次完整的TCP连接。扫描程序作为client端，不发送最后一个ACK包，这样server端认为没有建立一次TCP连接，因此通常不会在系统的审计记录中留下痕迹。

(3) TCP FIN扫描。一些防火墙软件或包过滤程序可以检测SYN扫描，因此产生了FIN扫描方法，即发一个FIN包给目标端口，如果该端口是开放的，则这个FIN包被忽略。如果该端口是关闭的，则返回一个RST包。通过识别这种差别，扫描程序就可以判断出端口的开放情况。

(4) TCP Fragmentation扫描。前几种扫描方式都不能通过防火墙，因为防火墙通常只允许以少数几个端口为目的端口的TCP报通过，这样就无法达到大面积扫描的目的。但通过把一个TCP报分割到多个IP包中，可使防火墙无法从一个IP包中找到完整的TCP报头，从而无法进行过滤。

这几种扫描方式中，方法（1）不需要特殊权限；方法（2）、（3）和（4）都需要程序能够打开Raw socket，自己拼装TCP/IP包，这是需要超级用户权限的。

UDP端口扫描的机理类似，仍然依次向目标系统的端口发送UDP包，若该端口上无服务程序守侯，则UDP协议层则会回送一个端口不可达包。如果在一定时间内没有收到这种包，就说明该端口有服务程序运行。再根据服务程序和端口号间的对应关系，即可判断目标系统上究竟运行哪些UDP服务了。

2.2 获取应用程序版本和操作系统类型

下面的例子说明，如何获取应用程序版本和操作系统类型，为远程攻击作准备。

在例1中，说明目标系统运行的是SunOS 5.7，即Solaris 2.7操作系统。

例 1

```
$ telnet ercist.com
Trying 192.168.0.111...
Connected to ercist.com.
Escape character is '^]'.

SunOS 5.7
login:
```

在例2中，说明目标系统运行HP9000系列777上的HP-UX B.10.20操作系统。

例 2

```
$ telnet somia.com
... ...
HP-UX HP9000 B.10.20 A 9000/777(ttyp2)
login:
```

例3是一个安全性好的例子，该系统的telnetd不提供关于操作系统的任何有用信息。

例 3

```
$ telnet virtual.com
Connecting to host virtual.com...Connected
Welcome to Virtual World!
Unauthorized computer usage is illegal!
virtual login:
```

SMTP协议的服务守护程序，最常见的是Sendmail。Sendmail一度曾是Unix上漏洞最多的程序，著名的蠕虫病毒就是利用Sendmail旧版本上的一个DEBUG命令的漏洞进行传播的。Sendmail同样也可能泄露操作系统的类型，如例4所示。从中，我们不仅知道了Sendmail的版本，同时也知道了目标系统是Sun。

例 4

```
$ telnet good.com smtp
Trying 1.2.3.4 ...
Connected to good.com.
Escape character is '^]'.
220 good ESMTP Sendmail 8.9.3+Sun/8.9.3;Fri,28 Apr
2000 11:45:35+0800(CST)
```

利用Sendmail中的expn和vrfy命令，可以确认目标主机上用户名的合法性，如例5所示。其中，“ftp”为合法用户名，“byron”则不是合法用户名。

例 5

```
# telnet ercist.com smtp
Trying xxx.xxx.xxx.xxx...
Connected to ercist.com.
Escape character is '^]'.
220 ercist.com ESMTP Sendmail 8.9.1 b+Sun/8.9.1;Fri,7
May 1999 14:01:39+0800(CST)
expn root
250 Super=User <root@ercist.ac.cn>
expn ftp
250 <ftp@ercist.ac.cn>
vrfy byron
550 byron... User unknown
```

3 利用网络堆栈特性探测远程操作系统

上节介绍的是一种古老而简单的技术，尽管如此，直到现在还为许多著名的网络探测器所采用，如SATAN和ISS。“网络堆栈特征探测”是一项新技术，其出发点在于，网络协议虽然有标准可依，但有一些边界情况的技术细节未被定义，所以就给具体实现留下了空间。利用这个空间中不同实现之间的差异，就可以区别不同的操作系统，甚至相当精确地定位操作系统的具体类型和版本。这项新技术已经被一些先进的探测器采用，如checkos、Queso、nmap等。以下列举一些这方面的技术：

3.1 FIN探测

发送一个FIN数据包（或任何未设置ACK或SYN标记位的数据包）到一个打开的端口，并等待回应。虽然RFC793定义的标准是“不”响应，但诸如MS Windows、BSDi、CISCO、HP/UX、MVS和IRIX等操作系统都会回应一个RESET包。大多数的探测器都使用了这项技术。

3.2 BOGUS（伪造）标记位探测

Queso是最先采用这种技术的探测器。它在一个SYN数据包的TCP头中设置未定义的TCP“标记”（64或128）。低于2.0.35版本的Linux内核会在回应包中保持这个标记，而其他操作系统则不然。不过，有些操作系统接收到一个SYN+BOGUS数据包时会进行复位连接。所以，这种方法能够比较有效地识别出操作系统。

3.3 TCP ISN取样

ISN（Initial Sequence Number）系指初始化序列号，即建立TCP连接时第一个TCP包中的Sequence Number

字段。这种探测的原理是，通过操作系统对连接请求的回应，寻找TCP连接初始化序列号的特征，从而判断操作系统的类型。目前可以区分的类别有：

(1) 传统的64K (旧UNIX系统)；(2) 随机增加 (新版本的Solaris、IRIX、FreeBSD、Digital UNIX、Cray等)；(3) 真正“随机”(Linux 2.0.*及更高版本、OpenVMS和新版本的AIX等)；(4) Windows平台等使用“基于时间”方式产生的ISN，随着时间的变化会有相对固定的增长；(5)“固定”ISN。有些机器总是使用相同的ISN，如某些3Com集线器使用0x83；Apple LaserWriter打印机使用0xC7001等。

根据计算ISN的变化、最大公约数和其他一些有迹可循的规律，还可以将这些类别分得更细、更准确。

3.4 “无碎片”标记位

有些操作系统在它们发送的数据包中设置IP“(无碎片) (No fragmentation)”位。这对于提高传输性能有好处，也是为什么nmap探测器不对Solaris系统进行碎片探测的原因。但是，并非所有操作系统都有这个设置，或许并不总是使用这个设置，因此通过这个标记位的设置可以收集到关于目标主机操作系统更多的有用信息。

3.5 TCP初始化“窗口”

“窗口”大小指的是，TCP缓存有多少字节没有得到应答的数据，当达到这个阈值后，TCP不再向对方发送新的数据，直到收到对方的应答确认包时为止。以前的探测器仅仅通过RST数据包的非零“窗口”值，标识为“起源于BSD 4.4”。queso和nmap这些新的探测器会记录确切的窗口值，因为该窗口随操作系统类型有较为稳定的数值。这种探测能够提供许多有用的信息，因为某些系统总是使用比较特殊的窗口值。例如，AIX是唯一使用0x3F25窗口值的操作系统。而在声称“完全重写”的NT5的TCP堆栈中，Microsoft使用的窗口值总是0x402E。同时，这个数值也被OpenBSD和FreeBSD使用。

3.6 ACK值

操作系统在ACK域值上的实现也有所不同。例如，我们向一个关闭的TCP端口发送一个FIN | PSH | URG包，许多操作系统会将ACK值设置为ISN值，但Windows和某些打印机会设置为seq+1。

3.7 ICMP错误信息查询

有些操作系统根据RFC 1812的建议对某些类型的错误信息发送频率作了限制。例如，Linux内核（在net/ipv4/icmp.h中）限制发送“目标不可到达”信息次数为每4秒80次，如果超过这个限制则会再减少1/4秒。一种测试方法是向高端随机的UDP端口发送成批的数据包，并计算接收到的“目标不可到达”数据包的数量。

在nmap探测器中，只有UDP端口扫描使用了这种技术。这种探测操作系统的方法需要较长的时间，因为需要发送大量的数据包并等待它们的返回。

3.8 ICMP信息引用

RFC定义了一些ICMP错误信息格式。如对于一个端口不可到达的信息，几乎所有的操作系统都只回送IP请求头加8字节长度的包，但Solaris返回的包会稍微长一点，Linux则返回更长的包。这样，即使操作系统没有监听任何端口，探测器nmap仍然有可能分辨应用Linux和Solaris操作系统的主机。

3.9 ICMP错误信息回显的完整性

我们在前面已讲过，机器必须根据接收到的数据包返回“端口不可到达”数据包。有些操作系统会在初始化处理过程中弄乱了请求头，这样，接收到这种数据包时会出现不正常。例如，AIX和BSDI返回的IP包中的“总长度”域会被设置为20字节（太长了）。某些BSDI、FreeBSD、OpenBSD、ULTRIX和VAX操作系统甚至会修改请求头中的IP ID值。

另外，由于TTL值的改变导致校验和需要修改时，某些系统（如AIX、FreeBSD等）返回数据包的检验和会不正确或为0。总之，探测器nmap使用了9种不同的ICMP错误信息探测技术区分不同的操作系统。

3.10 服务类型（TOS）

对于ICMP的“端口不可到达”信息，经过对返回包的服务类型（TOS）值的检查，几乎所有的操作系统使用的是ICMP错误类型0，而Linux使用的值是0xC0。

3.11 片段（碎片）处理

不同的操作系统在处理IP片段重叠时采用了不同的方式。有些用新的内容覆盖旧的内容，有些是以旧的内容优先。有很多探测方法能确定这些包是被如何重组的，从而帮助确定操作系统的类型。

3.12 TCP选项

这是收集信息最有效的方法之一。其原因是：它们通常真的是“可选的”，因此并不是所有的操作系统都使用它们。向目标主机发送带有可选项标记的数据包时，如果操作系统支持这些选项，会在返回包中也设置这些标

记。因此，可以一次在数据包中设置多个可选项，从而增加了探测的准确度。探测器nmap在几乎每一个探测数据包中都设置了如下选项：

Window Scale=10; NOP; Max Segment Size = 265; Timestamp; End of Ops;

当接收到返回包时，检查返回了哪些选项，它们就是目标操作系统支持的选项。有些操作系统（如较新版本的FreeBSD、Linux 2.1.x）支持以上所有选项，而有些（如Linux 2.0.x）则几乎都不支持。如果有几个操作系统支持相同的选项，可以通过选项的值进行区分。例如，如果向Linux机器发送一个很小的MSS值，它一般会将此MSS值返回，而其他系统则会返回不同数值。如果支持相同的选项，返回值也相同，又怎么办呢？我们可以通过返回选项的顺序进行区分。例如，同样的选项，同样的返回值，Solaris系统返回“NNTNWME”，而Linux 2.1.122系统却返回“MENNTNW”。

4 安全扫描器

安全扫描器（Security Scanner）是一种程序，它通过探测和模拟攻击，搜集主机和子网的安全漏洞。其中，SATAN（Security Analysis Tool for Auditing Networks）最为著名。它综合了上面介绍的各种方法，可以给出非常丰富的关于攻击目标的信息列表，包括系统类型、操作系统版本、提供的服务种类、系统漏洞等。

SATAN构造了一种非常灵活的框架，是可扩充的。只要根据扩充规则，可以把新的检测程序和检测规则加入到这个框架中去，使它与整个SATAN融为一体。在SATAN的基础架构上扩充的安全扫描器中，以“SAINT”（Security Administrator's Integrated Network Tool）最为著名。

其他一些有名的安全扫描器有：

4.1 NSS（Network Security Scanner）

NSS是用Perl语言编写的，运行在SunOS和IRIX上，扫描速度很快，动作也很隐蔽。

4.2 NMap（Network Map）

顾名思义，NMap为远程网络构造逻辑“地图”，实际上是检测网络上有哪些主机；这些主机的操作系统类型；提供哪些网络服务等。我们已经提到过，它在检测远程操作系统类型时十分有用。事实上，新版的SAINT在搜集这些信息时直接应用了NMap。

4.3 Nessus

Nessue是开放源代码的远程安全扫描器，可运行在Linux、BSD、Solaris和其他平台上。支持多线程和插件，目前可检查多达320个远程安全漏洞。

下一篇文章，我们将对黑客入侵网络的方法，作更为完整和详尽的介绍。■

作者简介：

卿斯汉，中国科学院信息安全技术工程研究中心主任。中国科学院软件研究所信息安全国家重点实验室研究员。博士生导师。享受政府特殊津贴。

卿斯汉是中国科学院“九五”重大项目的首席科学家，该项目获2000年国家科技进步奖二等奖。他主持过30余项国家和中科院的重要科研项目，包括国家攻关项目、国务院信息办重点攻关项目、973项目、863项目、国家自然科学基金项目、中国科学院重大科研项目、中国科学院创新重大项目、国家保密科研项目、国家密码基金项目等。他目前的研究方向是：密码学、INTERNET的应用与安全、智能卡安全集成系统、信息安全算法与协议、信息系统的安全标准与评测、安全操作系统与安全集成等。