ポートスキャン実習

2002年9月19日

修士1年

兼子　譲

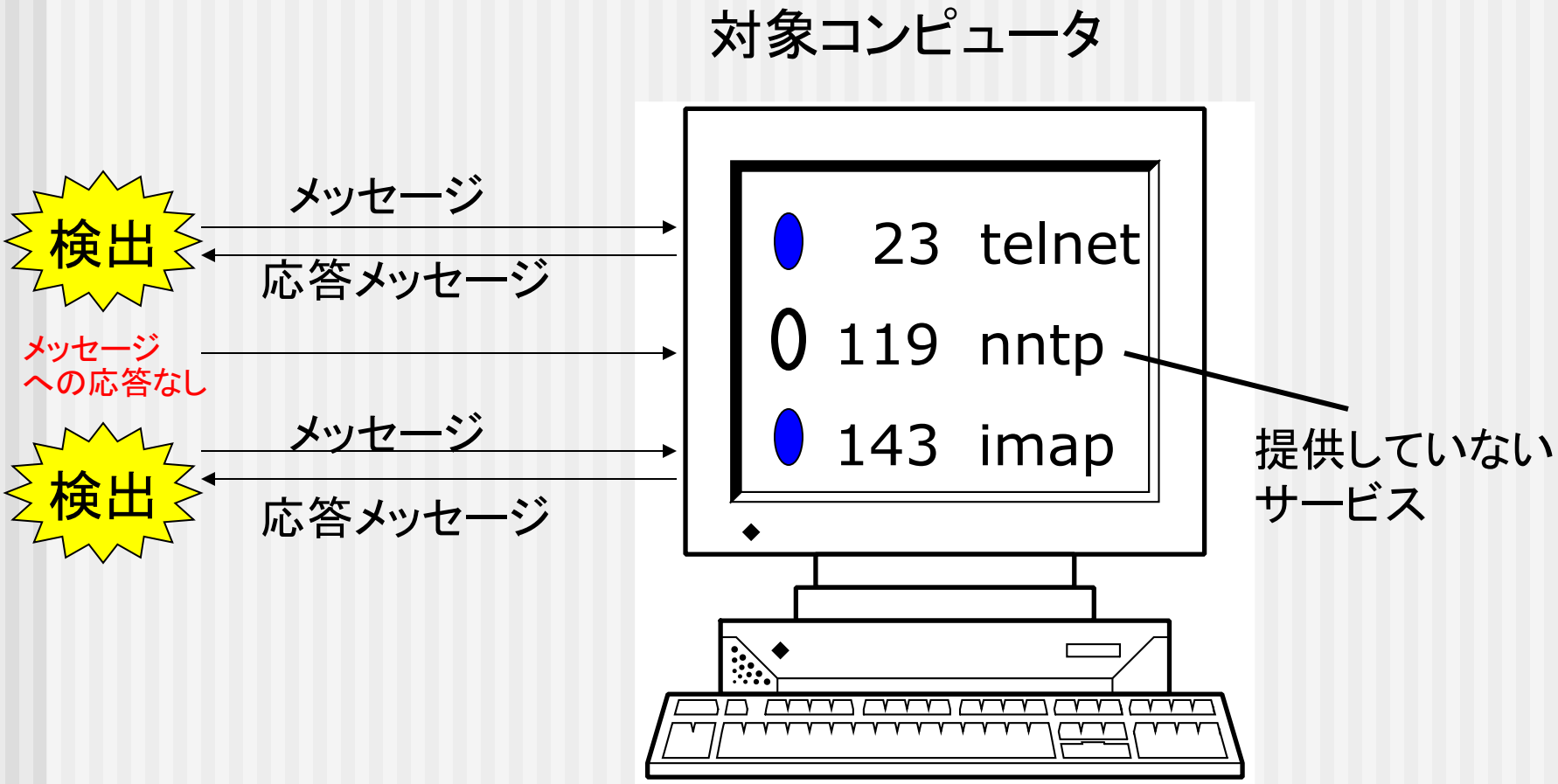
ポートスキャンとは

- メッセージを送った際の応答を元にコンピュータが提供しているネットワークサービスを探査
  - ネットワークサービスの稼動有無
  - 稼動しているネットワークサービスサーバのバージョン確認
- サーバ内で動作しているアプリケーションソフトやOSの種類を調べ、侵入口となりうる脆弱なポートがないかどうか調べる行為

ポートスキャンの目的

- セキュリティーホールを探し、侵入用のプログラムを使って不正侵入を行う
- ネットワーク管理者が自分の管理するシステムに弱点がないかどうか調査

ポートスキャンの探査方法



ポートスキャン実験用のソースプログラム (/u/kane/rinkou/scan/portscan.c)

```
#include <stdio.h>
#include <netdb.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>

#define SERV_HOST_ADDR      "192.168.33.33"
#define MAXPORT             1024
#define BUFLEN              1024
#define SBUFLEN             256

int main(int argc, char **argv)
{
  struct sockaddr_in addr;
  struct servent     *sent;
  int                fd, i, j, rtn, n;
  char               buf[BUFLEN];

  for (i = 1; i < MAXPORT; i++) {
    /* ソケットの準備 */
    fd = socket(AF_INET, SOCK_STREAM, 0);

    memset((char *)&addr, 0, sizeof(addr));
    addr.sin_family = AF_INET;
    addr.sin_addr.s_addr = inet_addr(SERV_HOST_ADDR);
    addr.sin_port = htons((short)i);

    /* サーバとの接続 */
    if ((rtn = connect(fd, (struct sockaddr *)&addr, sizeof(addr))) == -1) {
      //printf("e");
      close(fd);
      continue;
    }
    /* サービス名の取得 */
    if ((sent = getservbyport(htons(i), "tcp")) == NULL) {
      printf("unknown service (port %d) is available.¥n", i);
    } else {
      printf("%s¥tservice (port %d) is available.¥n", sent->s_name, i);
    }
    close(fd);
  }
}
```

← 対象サーバのIPアドレス

telnetコマンドによる実験(1)

FTPサービスへのアクセス例

```
%telnet lana 21                    ←"21"はFTPのポート番号
Trying 192.168.33.33...
Connected to lana.4f.db.is.kyushu-u.ac.jp.
Escape character is '^]'.
220 lana FTP server (SunOS 5.8) ready.
quit
221 Goodbye.
Connection closed by foreign host.
%
```

telnetコマンドによる実験(2)

HTTPサービスへのアクセス例

```
%telnet hatsune 80          ←“80”はHTTPのポート番号
Trying 133.5.18.167...
Connected to hatsune.db.is.kyushu-u.ac.jp.
Escape character is '^]'.
GET / HTTP/1.0
        ←[ENTER]
HTTP/1.1 200 OK
Date: Wed, 18 Sep 2002 05:41:36 GMT
Server: Apache/1.3.26 (Unix)
Last-Modified: Wed, 08 May 2002 10:44:00 GMT
ETag: “18b4d1-bef-3cd94a0d"
Accept-Ranges: bytes
Content-Length: 3055
Connection: close
Content-Type: text/html
（省略）
Connection closed by foreign host.
%
```

実習

- ポートスキャンプログラムを実行
  - ソースは/u/kane/rinkou/scan/portscan.c
  - 研究室外のマシンにポートスキャンを試みることはマナー違反となるので、研究室内のマシンに対してのみ実験
- 稼動しているサービスに対してtelnetでアクセスしてみる（ただし、アクセスする前にそのプロトコルがどのようなものかを調べておく）

ポートスキャン(Nmap)

Nmapとは

- ポートスキャンをするプログラム
- insecure.orgが提供している

Nmapの使用法

- # nmap [Scan Type(s)] [Options] <host or net list>
  - Scan Type
    - -sT　:TCPスキャン
    - -sU　:UDPスキャン
  - Options
    - -O　:OSを調べる
    - -p　:ポート番号の指定
    - -v　:スキャン中の様子を表示
- オプションによってはrootでしか実行できない

Nmapの使用例

- # nmap –sU –O ami
  - amiのUDPポートをスキャンする
  - OSを調べる
- # nmap –p 20-25 ‘192.168.33.*’
  - 20番から25番までのTCPポートをスキャンする
  - 192.168.33のネットワーク全体のコンピュータをスキャンする

実行結果

```
tei# nmap -O ami.db.is.kyushu-u.ac.jp

Starting nmap V. 2.54BETA34 ( www.insecure.org/nmap/ )
Interesting ports on ami.db.is.kyushu-u.ac.jp (133.5.18.197):
(The 1545 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
22/tcp     open        ssh
23/tcp     filtered    telnet
53/tcp     open        domain
111/tcp    open        sunrpc
139/tcp    open        netbios-ssn
1021/tcp   open        unknown
1022/tcp   open        unknown
1023/tcp   open        unknown
1024/tcp   open        kdm
6000/tcp   open        X11
Remote operating system guess: FreeBSD 4.3 - 4.4-RELEASE

Nmap run completed -- 1 IP address (1 host up) scanned in 8 seconds
tei#
```

Nmapのインストール方法

- 以下のページからファイルをダウンロードする
  - http://www.insecure.org/nmap/nmap_download.html
- FreeBSDではportsが用意されています
  - cd /usr/ports/security/nmap
  - make install

実習上の注意点

- ポートスキャンはサーバに対する攻撃方法の1つ
- ポートスキャンされた側はポートスキャンを行ったホストを悪意のあるホストとして認識する可能性がある
- 必ず研究室内のマシンに対してのみ実験を行う