Bài 1 **CÔNG CỤ TRUY XUẤT MẠNG NETCAT**

netcat là một tiện ích mạng dành để đọc và ghi các kết nối mạng TCP hoặc UDP. Khi kết nối được thiết lập netcat sẽ thực hiện chương trình mà NSD chọn và kết nối chuẩn xuất và nhập của chương trình cho kết nối mạng.

Mở trình duyệt Web hoặc Windows Explore, gõ :

ftp://192.168.104.18

hoặc \\192.168.104.18\public

Tải file *netcat.rar* về ổ đĩa C và giải nén vào thư mục C:\netcat

1.1. Xây dựng chương trình netcat Client/Server theo giao thức TCP

1) Mở cửa sổ lệnh thứ nhất:

   + Chuyển đến thư mục hiện hành C:\netcat>

   + Chạy chương trình netcat TCP Server:

```
C:\netcat> nc -l -t -p 8888
```

2) Mở cửa sổ lệnh thứ hai:

   + Chuyển đến thư mục hiện hành C:\netcat>

   + Chạy chương trình netcat TCP Client:

```
C:\netcat> nc -t 127.0.0.1 8888
```

3) Nhắn tin trao đổi giữa hai chương trình:

   + Tại Client, gõ Hello Server, Nhấn Enter

   + Tại Server: Hello Client

>> Thực hiện triển khai chương trình Server trên một máy và chương trình Client trên một máy khác.

1.2. Xây dựng chương trình netcat Client/Server theo giao thức UDP

1) Mở cửa sổ lệnh thứ nhất:

   + Chuyển đến thư mục hiện hành C:\netcat>

   + Chạy chương trình netcat TCP Server:

   ```
   C:\netcat> nc -l -u -p 8888
   ```

2) Mở cửa sổ lệnh thứ hai:

   + Chuyển đến thư mục hiện hành C:\netcat>

   + Chạy chương trình netcat TCP Client:

   ```
   C:\netcat> nc -u 127.0.0.1 8888
   ```

3) Nhắn tin trao đổi giữa hai chương trình:

   + Tại Client, gõ Hello Server, Nhấn Enter

   + Tại Server: Hello Client

>> Thực hiện triển khai chương trình Server trên một máy và chương trình Client trên một máy khác.

1.3. Xây dựng chương trình netcat Client/Server cho phép điều khiển từ xa

1) Mở cửa sổ lệnh thứ nhất:

   + Chuyển đến thư mục hiện hành C:\netcat>

   + Chạy chương trình netcat Trojan TCP Server:

   ```
   C:\netcat> nc -L -t -p 8888 -e cmd.exe
   ```

   + Mở cửa sổ lệnh thứ hai:

   + Chuyển đến thư mục hiện hành C:\netcat>

   + Chạy chương trình netcat Trojan TCP Client:

   ```
   C:\netcat> nc -v 127.0.0.1 8888
   ```

2) Nhắn tin trao đổi giữa hai chương trình:

   + Tại Client, lần lượt thực hiện các lệnh sau:

   ```
   DIR C:\
   DIR D:\
   MD C:\HAHA
   DIR C:\
   SHUTDOWN -s -f -t 30
   ```

>> Thực hiện triển khai chương trình Server trên một máy và từ chương trình Client trên một máy khác kết nối đến Server:

```
C:\netcat> nc -v <IPServer>  8888
```

1.4. Sử dụng netcat quét cổng dịch vụ trên máy Server

1) Quét cổng không truy vấn tên DNS

```
C:\netcat> nc -z -n -v  192.168.104.18 1-1024
```

```
C:\netcat> nc -z -n -v  <IPMáyTrongMạng> 1-1024
```

2) Quét cổng dịch vụ của một Server trên Internet

```
C:\netcat>ping vnexpress.com
```

```
Pinging vnexpress.com [185.53.179.8] with 32 bytes of data:
Reply from 185.53.179.8: bytes=32 time=274ms TTL=52
…
```

```
C:\netcat>nc -z -n -v 113.171.23.95  1-1024
```

```
(UNKNOWN) [113.171.23.95] 723 (?): TIMEDOUT
(UNKNOWN) [113.171.23.95] 650 (?): TIMEDOUT
(UNKNOWN) [113.171.23.95] 445 (?): TIMEDOUT
(UNKNOWN) [113.171.23.95] 443 (?) open
(UNKNOWN) [113.171.23.95] 139 (?): TIMEDOUT
(UNKNOWN) [113.171.23.95] 138 (?): TIMEDOUT
(UNKNOWN) [113.171.23.95] 137 (?): TIMEDOUT
(UNKNOWN) [113.171.23.95] 135 (?): TIMEDOUT
(UNKNOWN) [113.171.23.95] 80 (?) open
(UNKNOWN) [113.171.23.95] 21 (?) open
(UNKNOWN) [113.171.23.95] 1 (?): TIMEDOUT
```

3) Quét cổng dịch vụ UDP

```
C:\netcat> nc -u 192.168.104.18
```

4) Xem thông tin hệ thống

```
C:\netcat> nc -v -z 192.168.104.18 1-255
```

>> Thay địa chỉ 192.168.104.18 bằng địa chỉ/tên của một Server trên internet để quét cổng dịch vụ.

1.5. Sử dụng netcat lấy thông tin WebServer

1) Ghi nhật ký truy xuất WebServer

```
C:\netcat> nc -v -o nhatky.log 192.168.104.18 80 HTTP
```

```
TKHOI [192.168.104.18] 80 (http) open
```

```
∩╗┐<!DOCTYPE    html    PUBLIC    "-//W3C//DTD    XHTML    1.0    Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html dir="ltr">
<head>
    <meta http-equiv="content-type" content="text/html; charset=UTF-8" />
<link                          rel="stylesheet"                          type="text/css"
href="http://192.168.104.18/theme/standard/styles.php" />
<link                          rel="stylesheet"                          type="text/css"
href="http://192.168.104.18/theme/college15_fixed/styles.php" />
<meta name="description" content="" />
     <meta name="keywords" content="moodle, Hß╗ç thß╗æng ─æ├áo tß║ío trß╗▒c tuyß║┐n "
/>
```

```
      <title>Hß╗ç thß╗æng ─æ├áo tß╗ío trß╗▒c tuyß╗╗n</title>
                                          <link          rel="shortcut          icon"
href="http://192.168.104.18/theme/college15_fixed/favicon.ico" />
                                      <!--<style         type="text/css">/*<![CDATA[*/
body{behavior:url(http://192.168.104.18/lib/csshover.htc);} /*]]>*/</style>-->

   ….
   </body>
   </html>
```

```
C:\netcat> type nhatky.log
< 00000000 ef bb bf 3c 21 44 4f 43 54 59 50 45 20 68 74 6d # ...<!DOCTYPE htm
< 00000010 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 # l PUBLIC "-//W3C
< 00000020 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 # //DTD XHTML 1.0
< 00000030 54 72 61 6e 73 69 74 69 6f 6e 61 6c 2f 2f 45 4e # Transitional//EN
< 00000040 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 # " "http://www.w3
< 00000050 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 # .org/TR/xhtml1/D
< 00000060 54 44 2f 78 68 74 6d 6c 31 2d 74 72 61 6e 73 69 # TD/xhtml1-transi
…
…
< 000000b0 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 # ntent-type" cont
< 000000c0 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 # ent="text/html;
< 000000d0 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f # charset=UTF-8" /
< 000000e0 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 # >.<link rel="sty
< 000000f0 6c 65 73 68 65 65 74 22 20 74 79 70 65 3d 22 74 # lesheet" type="t
```

>> Thay địa chỉ 192.168.104.18 bằng địa chỉ/tên của một WebServer trên Internet

2) Lấy thông tin WebSite

```
C:\netcat> nc  -v 192.168.104.18  80 HEAD/HTTP/1.0
```

3) Lấy thông tin Website trên internet.

```
C:\netcat> nc  -v www.dut.udn.vn  80 HEAD/HTTP/1.0
```

1.6. Sử dụng netcat kết nối POP3 Mail Server bằng lệnh

```
C:\netcat> nc -v pop.gmail.com 995
```

1.7. Sử dụng netcat kết nối SMTP Mail Server bằng lệnh

```
C:\netcat> nc -v alt2.gmail-smtp-in.l.google.com 25
```

Hoặc:

```
C:\netcat> nc -v alt1.gmail-smtp-in.l.google.com 25
```

1.8. How To Use Netcat as a Simple Web Server

First, let's make a simple HTML file on one server:

nano index.html

<html>

<head>

```
        <title>Test Page</title>
    </head>
    <body>
        <h1>Level 1 header</h1>
        <h2>Subheading</h2>
        <p>Normal text here</p>
    </body>
</html>
```

We can have netcat serve the page indefinitely by wrapping the last command in an infinite loop, like this:

```
while true; do printf 'HTTP/1.1 200 OK\n\n%s' "$(cat index.html)" | netcat -l 8888; done
```

Now, in your browser, you can access the content by visiting:

http://server_IP:8888
