Computer Security

Buffer Overflows
Denial of Service

MIE456

Joseph Kong

Overview

- Program Exploitation
- Buffer Overflows
  - Memory Declaration
  - Smashing The Stack
- TCP/IP Three Way Handshake
- Denial of Service
  - SYN Flooding
  - Smurf Attacks
  - System Overloads
- Summary

Program Exploitation

- Definition:
  - Exploiting a program is simply a clever way of getting the computer to do what you want it to do, even if the currently running program was designed to prevent that action

- Programs follow the letter of the law

Buffer Overflows
Memory Declaration

- Null Byte Termination

- Program Memory Segmentation
  - text
  - data
  - bss
  - heap
  - stack

Buffer Overflows
Memory Declaration Cont.

- Extended Instruction Pointer (EIP)

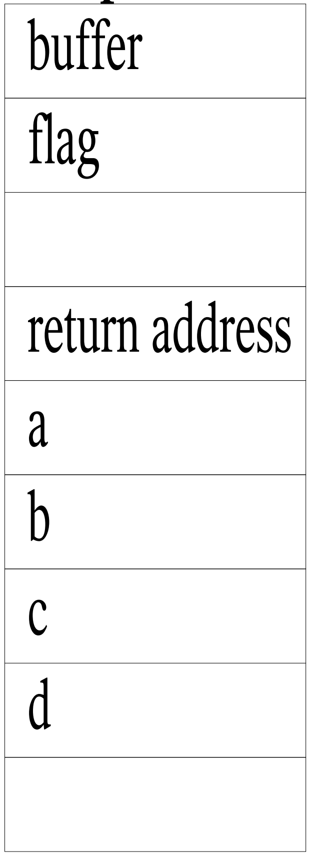
- Program Flow
  1. Read the instruction that EIP is pointing to
  2. Add the byte-length of the instruction to EIP
  3. Execute the instruction that was read in step 1
  4. Go to step 1

Buffer Overflows
Memory Declaration Cont.

```
void test(int a, int b, int c, int d){
        char flag;
        char buffer;
}

void main(){
        test(1, 2, 3, 4)
}
```

The top of the stack



buffer

flag

return address

a

b

c

d

Low addresses

High addresses

Buffer Overflows
Smashing The Stack

overflow.c code

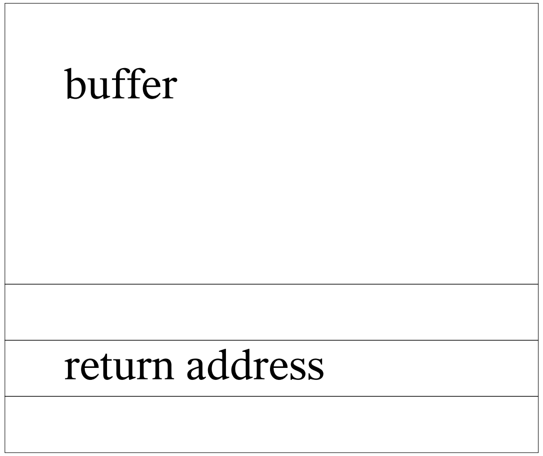
```
void overflow (char *str){
        char buffer [20];

        //function that copies str to buffer
        strcpy(buffer, str);
}

int main(){
        char big_string[128];
        int i;

        for(i=0;  i < 128; i++){
                //fill big_string with 'A's
                big_string[i] = 'A';
        }

        overflow(big_string);
        exit(0);
}
```



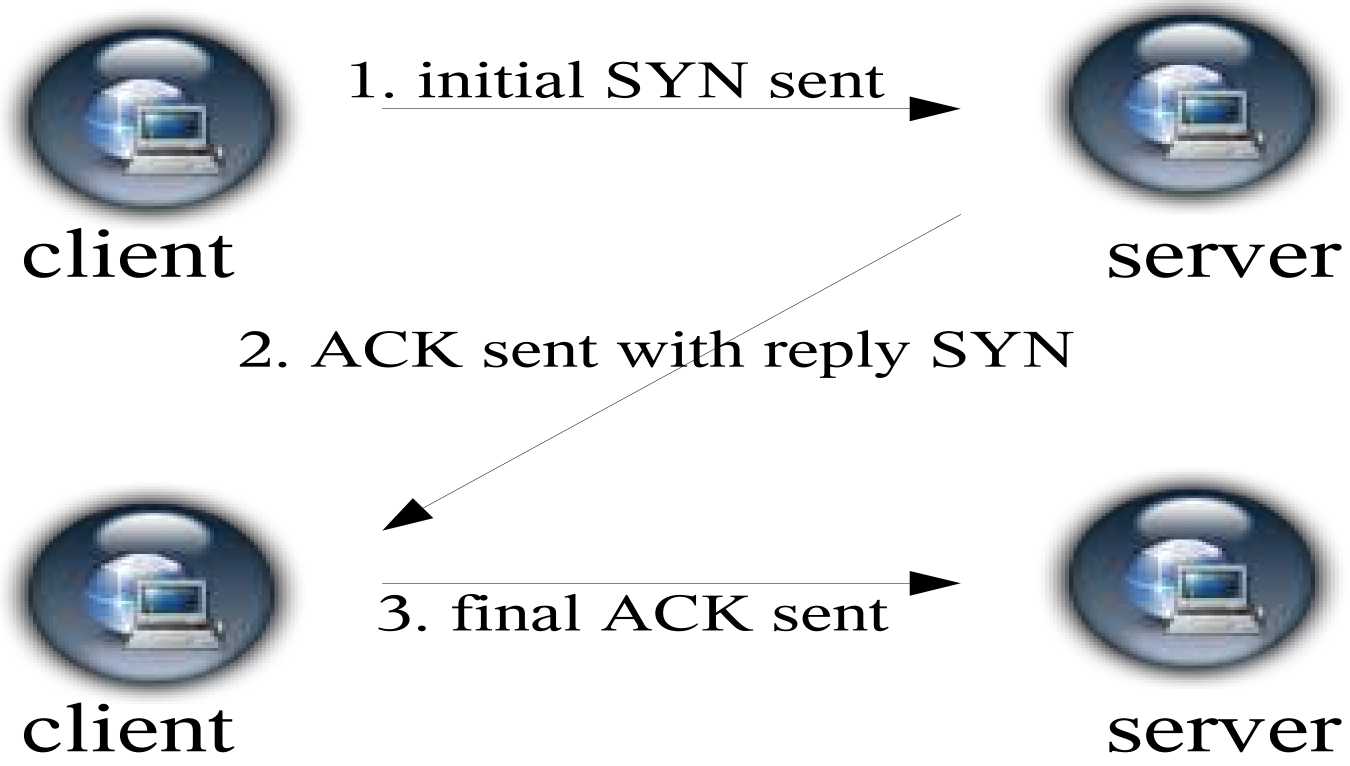
buffer

return address

overflow.c results

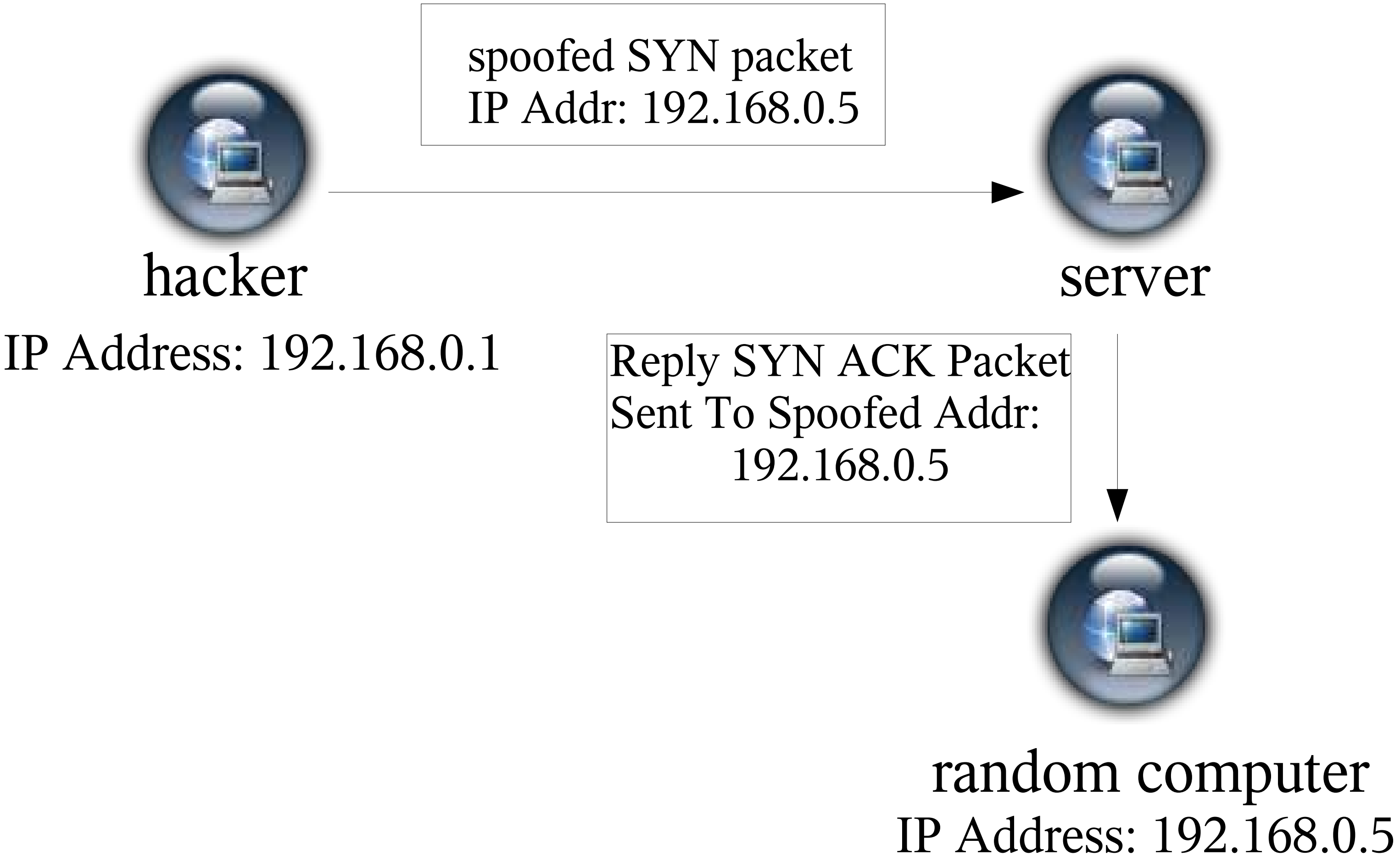
```
$ gcc -o overflow overflow.c
$ ./overflow
Segmentation fault
$
```

TCP/IP Three Way Handshake



Denial of Service
SYN Flooding

SYN Attack Using A Spoofed Return Address



spoofed SYN packet
IP Addr: 192.168.0.5

hacker

IP Address: 192.168.0.1

server

Reply SYN ACK Packet
Sent To Spoofed Addr:
192.168.0.5

random computer
IP Address: 192.168.0.5

Denial of Service
Smurf Attacks

- Broadcast Address
  - One address that every computer will answer to
  - Used to update name lists and other necessary items that computers need to keep the network up and running

- Broadcast Storm
  - send a request to a network using the broadcast address with the return address of the broadcast address

Denial of Service
System Overloads

- DOS attack directed against the software running on the target computer

- Average 5-50 bugs/thousand lines of code

- If an attacker knows how to exploit a specific bug, she can shut down the target computer

Summary

- Hacking is really just the act of finding a clever and counterintuitive solution to a problem
- A buffer overflow attack is exactly what its name implies
- A DOS simply prevents access to a service or resource

References

1. Erickson, Jon. (2003) Hacking: The Art Of Exploitation. San Francisco: No Starch Press

2. Hoglund, Greg, and Gary McGraw. (2004) Exploiting Software: How To Break Code. Boston: Addison Wesley

3. Peikari, Cyrus and Seth Fogie. (2003) Maximum Wireless Security. Indiana: Sams