

CIS 551 - Computer and Network Security Assignment 1 - Buffer Overflows

This project should be completed in groups of 2.
Consider the following program, which we might call badbuf.c:

```
#include <stdio.h>
int match(char *s1, char *s2) {
    while( *s1 != '\0' && *s2 != 0 && *s1 == *s2 ){
        s1++; s2++;
    }
    return( *s1 - *s2 );
}
void welcome(char *str) { printf(str); }
void goodbye(char *str) { void exit(); printf(str); exit(1); }
main(){
char name[128], pw[128]; /* passwords are eight characters - double this */
char *good = "Welcome to The Machine!\n";
char *evil = "Invalid identity, exiting!\n";

printf("login: "); scanf("%s", name);
printf("password: "); scanf("%s", pw);
if( match(name,pw) == 0 )
welcome( good );
else
goodbye(evil );
}
```

Here is your assignment:

1. Part 1: **Control** *Due Wednesday, February 8th* (50 %) Use a buffer overflow attack on this program so that it prints the welcome message for `name != pw`.
2. Part 2: **Data Payload** *Due Friday, February 17th* (50 %) Enhance your buffer overflow attack so that the program prints `''ownz_u!''`

You will be running the exploit and program on a VMWARE virtual machine.

Setting up VMware:

1. Download and install VMware Player*: <http://www.vmware.com/products/player/>
2. Download and extract the disk image: <http://www.seas.upenn.edu/~cis551/box.tar>
3. Open the extracted "box.vmx" file in VMware. The login and username is "root". If asked whether the image was copied or moved, select copied. You do not need to download any special VMware tools, if prompted.
4. To get files onto the VM, you can either:
 - SSH into the virtual machine. - use IFCONFIG to determine the IP address of the machine. It will be the inet addr for the eth0 device. You can ssh from your computer to this IP on port 22 using username/password "root"
 - SSH from the virtual machine to seas or any other machine
 - use "wget" to download a file. Provide wget with a url.
5. The virtual machine includes the nano editor. To install other programs or editors, you will need to use `apt-get install` followed by the name of the program you are installing. (Example: `apt-get install vim` will install the VI text editor.) Before you can use apt-get, you must do two things:
 - Update the `/etc/apt/sources.list` file by adding this line: `deb http://archive.debian.org/debian/ etch main non-free contrib`
 - run the command `apt-get update`
 - it might also be helpful to install the build essentials package, which includes many commonly used programs: `apt-get install build-essential`

**NOTE: VMware Player is free on windows and linux. If you need to run on OSX, you can either download a free trial of VMware fusion, or import the image into another virtualization program. Contact us for help if needed.*

Submission:

Please submit a zip or tar file containing (by the due dates indicated above):

1. A text file `group.txt` that includes the seas usernames of your group.
2. All source code used, including test cases and payload creation software.
3. A demonstration log captured on the virtual machine. Use the script command to do this.

Do not turn in executables. We suggest including a makefile so we can reproduce your setup - see `make(1)` in the Linux documentation accessible by typing in `man make` at the command prompt. The easiest way to submit is to create a tarball with the Linux `tar(1)` command and e-mail the tarball as an attachment to the course TAs, John Sonchack - `jsonch@seas.upenn.edu` and Sumanth M.S. - `sumanth@seas.upenn.edu`.

Advice:

- You will want to examine the contents of memory while the program is running. GDB is a debugging program useful for this. There are many tutorials online. Here is a good quick reference card: www.ece.utexas.edu/~adnan/gdb-refcard.pdf
- Your exploit string is likely to contain non ASCII characters. You will need to find some way of generating such strings from hexadecimal values. A shell script, python script, or C program are recommended.
- here are some introductions to basic techniques: <http://www.phrack.com/issues.html?issue=49&id=14#article> , <http://insecure.org/stf/smashstack.html>