Project 3 Review & Buffer Overflow

March 11th, 2015

Part 1.1 - 1.3

- What type of network?
  - It looks like a small home network
  - Router and two clients
- Active or Passive FTP?
  - Active: The client sends PORT, rather than PASV
- FTP vuln?
  - Lack of encryption. Passwords sent as plaintext.
  - HTTPS, SCP, or SFTP instead

Part 1.4

- Protect domain name leak?
  - No. TLS protocol requires presenting the certificate in plaintext form (includes the domain name).
- Cipher Suites
  - Can find client list in TLS Client Hello
  - Can find chosen cipher in TLS Server Hello

Part 1.5

- Insecure?
  - Session cookies passed over HTTP. You can also tell what the person is doing.
  - Could replay session cookie in your own connections.
  - To protect against this attack, use HTTPS for all connections.
- What did the user do?
  - Searched for Zakir Durumeric, sent him a Facebook

Part 2

- Follow aircrack tutorial
  - Configure wireless card
  - airmon, airdump, aircrack
  - We’re in!
- Attack the server
  - Analyze traffic, find local server ip address
  - Use nmap, see unprotected ftp server, get RSA key
  - Load into wireshark & decrypt traffic
  - You win!

Part 3

- Check for valid packet
  - Exceptions are your friend
- If SYN packet, add to SYN count. Elif SYN+ACK packet, add to SYN+ACK count
- For ip in count:
  - If SYN+ACK*3 < SYN: suspects.add(ip)
- Print suspects

Buffer Overflow (Review)

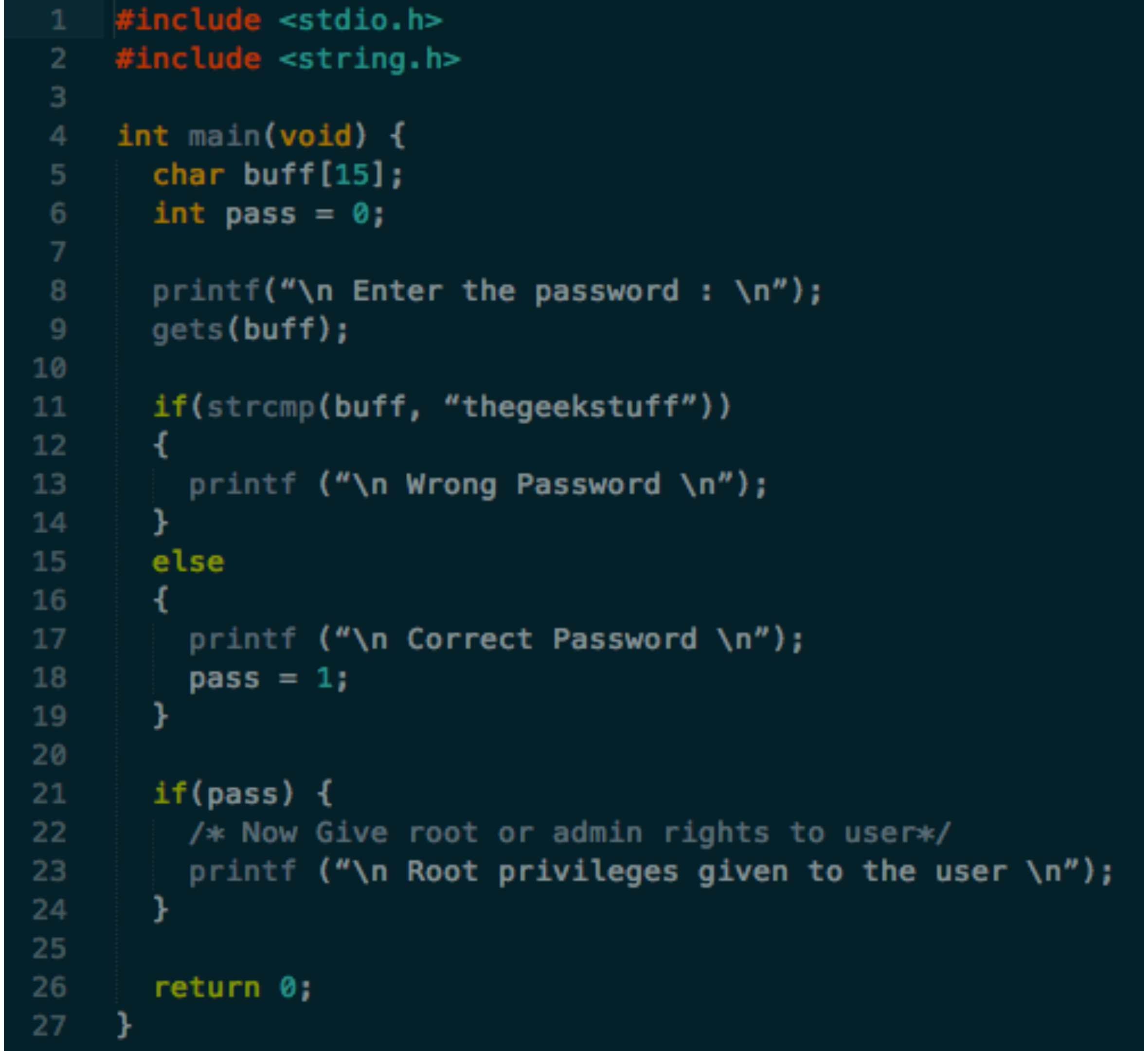
- Local variables go on stack
- Program data (return address, fn ptrs) *also* go on stack
- Insecure input methods let local variables overwrite program data

Buffer Overflow Examples

Hacking Pokemon Yellow, from within Pokemon Yellow:
http://aurellem.org/vba-clojure/html/total-control.html

Buffer overflow example:

- buffer_overflow.cpp - exploiting insecure c/c++ input



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

int main(void) {
  char buff[15];
  int pass = 0;

  printf(“\n Enter the password : \n”);
  gets(buff);

  if(strcmp(buff, “thegeekstuff”))
  {
    printf (“\n Wrong Password \n”);
  }
  else
  {
    printf (“\n Correct Password \n”);
    pass = 1;
  }

  if(pass) {
    /* Now Give root or admin rights to user*/
    printf (“\n Root privileges given to the user \n”);
  }

  return 0;
}
```