CSCI 345 – Homework 4

Buffer overflow & Putting everything together with pen testing

This homework puts together what you learned through capture the flag competitions as it is applied for penetration testing and vulnerability discovery. The learning goals are:

1. Perform a buffer overflow, understand and observe the results.
2. Complete the phases of pen testing: reconnaissance, exploitation, persistence, cover tracks.
3. Apply offensive knowledge, suggest defenses for a system.

Part 1: Buffer Overflow

Download the virtual machine protostar https://drive.google.com/folderview?id=0B9RbZkKdRR8qbkJjQ2VXbWNlQzg&usp=sharing.

Credentials:

1. Username: user, Password: user
2. Username: root, Password: godmode

On this virtual machine execute the code given below and perform two buffer overflow attacks (BO1, BO2).

BO1

You are given the code:

```
#include <stdlib.h>

#include <unistd.h>

#include <stdio.h>



int main(int argc, char **argv)

{

 volatile int modified;

 char buffer[64];



 modified = 0;

 gets(buffer);
 if(modified != 0) {
  printf("you have changed the 'modified' variable\n");
 } else {
  printf("Try again?\n");
 }
}
```

Give the program a specific input that will change the ‘modified’ variable.

BO2

You are given the following code:

```
#include <stdlib.h>
#include <unistd.h>
#include <stdio.h>
#include <string.h>

int main(int argc, char **argv)
{
 volatile int modified;
 char buffer[64];

 if(argc == 1) {
  errx(1, "please specify an argument\n");
 }

 modified = 0;
 strcpy(buffer, argv[1]);


 if(modified == 0x61626364) {
  printf("you have correctly got the variable to the right value\n");
 } else {
  printf("Try again, you got 0x%08x\n", modified);
 }
}
```

Set the 'modified' variable to value: `0x61626364`

What to submit: a short report on your thought process and the commands that you ran to complete BO1 and BO2. Screenshots of the completed BO attacks.

Part 2: Penetration Testing and Defenses

1. Download the virtual machine: https://www.vulnhub.com/entry/rickdiculouslyeasy-1,207/
2. Execute all phases of pen testing (hints for the specific VM are included):
    a. Scan with nmap
    b. Lookup vulnerable services on the internet
    c. Try netcat command (lookup what it is doing) for several fishy, unusual ports
    d. Exploit web application: look for interesting file in the web application, try to find an exposed user
    e. Use Metasploit to find any vulnerabilities that the OS or the web application may have.
3. **What to submit**: a short report on:
    a. How you found the vulnerabilities, your detailed thought process and steps.
    b. Include screenshots of the completed attacks.
    c. Add suggestions for possible defenses for the attacks that you performed. How can we defend from scanning, application exploits, and OS exploits? Write a paragraph with minimum 300 words describing possible defense mechanisms.