SC3010 Computer Security

Tutorial 1 – Introduction & Buffer Overflow

1. Circle the correct answers in the following questions.

   1) Which of the following statement(s) is/are true about malware?
      (i) Worms try to propagate to different computers without user intervention. ✓
      (ii) Viruses try to propagate to different computers without user intervention.
      (iii) Rootkits aim to obtain root privileges to compromise the victim computer. ✓
      (iv) Trojans aim to allow a remote party to gain access to the victim computer

      [✓ A. (i) and (iii)] ✓
      B. (i) and (iv)
      C. (ii) and (iii)
      D. (ii) and (iv)

   2) Which of the following statement is false?

      A. Security cannot be established in a computer system without trusting any components. ✗
      B. A threat model should clearly define the TCB, adversary's capabilities and security properties to be achieved. ✗
      [✓ C.] The three security strategies to protect a system is detection, ~~mitigation~~, and reaction. ✗
      ~~D.~~ Defense in depth can increase the difficulty of attacking the entire system, but also the cost and complexity of implementing the system. ✗

   3) Which of the following statements are true about Trusted Computing Base (TCB)?
      (i) We need to assume all components in TCB are secure. ✓
      (ii) We need to introduce security solutions to protect all components in TCB. ✗
      assume components are trusted
      (iii) It is easier to design a system with a smaller TCB. ✗
      (iv) It is more secure to design a system with a smaller TCB. ✓

      ✗ A. (i) and (iii)
      [✓ B. (i) and (iv)] ✓
      ✗ C. (ii) and (iii)
      D. (ii) and (iv)

2.1)Vulnerability: weakness that allows an attacker to reduce a system's information assurance

Exploit: technique that takes advantage of a vulnerability, used by the attacker to attack the system

Payload: custom code attacker wants the system to execute ✓

2. Answer the following questions.

   1) What do vulnerability, exploit, and payload refer to?

   2) What could be the potential consequences of a buffer overflow attack?

   3) What are the steps to utilize a buffer overflow vulnerability to execute shellcode?

1. Convert shellcode from C to assembly code then binary
2. Store binary code in buffer that is allocated in the victim stack
3. Use buffer overflow vulnerability to overwrite the return address with the address of the binary shellcode

3. Home Depot, the world's largest home improvement retailer, was hacked from April to September 2014. The attacker used a third-party vendor's username and password to enter the Home Depot's internal network and launched the malware programs on a number of self-checkout registers in

2.2) Corruption of program data, unexpected transfer of control, memory access violation, execution of code chosen by attacker ✓

System Crash
Control flow hijacking

2.3) 1. Inject malicious code into memory of the target program. 2. Find buffer on runtime stack and overwrite the return address with malicious address. 3. When function completed, it jumps to the malicious address and runs the malicious code ✗

Threat model

entire Home Depot computer system including trustedsoftware and hardware

trusted: internal network

not trusted: third party vendor

adversarial capabilities: malware programs on self checkout registers

security properties: protect the computer system so that malware cannot steal payment cards and email address information

confidentiality: protecting the system from leaking sensitive information

the U.S. and Canada. This attack lasted for about four months before being detected. About 56 million payment cards and 53 million e-mail addresses were stolen by the attacker. Write a threat model that would cover the Home Depot attack.

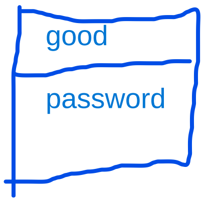
4. The following program is designed to generate a random number. It takes a password as input, but always fails to generate a random number. Luckily, this program is vulnerable to a buffer overflow attack. Our goal is to leverage this advantage to generate a random number. Please figure out a password that can achieve this.

gets: can lead to buffer overflow

```
char CheckPassword() {
  char good = ‘N’;
  char Password[100];
  gets(Password);
  return good;
}
int main(int argc, char* argv[]) {
  printf(“Enter your password:”);
  if(CheckPassword() == ‘Y’)
    printf(“Your random number is %d\n”, rand()%100);
  else{
    printf(“You don’t have the permission to get a random number”);
    exit(-1);
  }
  return 0;
}
```

password is "A..." of length 100 and "\x59\x00\x00\x00"

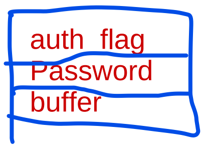
password of length 101 characters and ending with "Y" to overwrite good



5. A developer writes the following program for user authentication for his system. However, this program is vulnerable to buffer overflow attacks. Please give some examples of malicious input that an attacker can use to bypass the authentication.

```
int check_authentication(char *pwd) {
  int auth_flag = 0;
  char Password[] = “qwertyu”;
  char buffer[8];
  strcpy(buffer, pwd);
  if (strncmp(buffer, Password, 8) == 0)
    auth_flag = 1;
  return auth_flag;
}
int main(int argc, char* argv[]) {
  if(check_authentication(argv[1]))
    printf(“Access Granted\n”);
  else{
    printf(“Access Denied\n”);
  }
  return 0;
}
```

"AAAAAAAA\x01\x00\x00\x00", 8As and hypothetical value to overwrite auth_flag variable assuming little endian architecture and "auth_flag" is adjacent to "buffer"



attacker can leverage the strcpy to overflow the stack and bypass the authentication

-Overwrite the Password: pwd = "abcdefgh" + "abcdefgh"

-Overwrite the auth_flag:pwd = "xxxxxxxx" + "xxxxxxxx" + abcd" -> corresponding integer is 0x61626364