SEC204 Alternative ICT

Duration: 6 hours. This is a closed book exam.

SEC204 Alternative ICT Assessment

This is the alternative assessment for SEC204. Please note that it forms 50% of the final module mark.

This is a timed exam, yo[illegible]me. Please read the questions carefully and complete your answers in this docume[illegible] submit the document on the SEC204 DLE alternative assessment submission

Submission Inst[illegible]

Once you have complet[illegible]mit your answers on DLE, via the module website.

This is a closed book exam. Use of notes or reference material (other than the ones provided in this document are strictly not allowed. You may only use the Internet to submit your answers on the DLE module website.

Questions

1. Identify the software vulnerability that might exist in the following C code and discuss the possible consequences of exploiting it:

```
int main(int argc
        int valu
        char bu                                    [8];

        strcpy(b
        strcpy(b

        printf("[                                  s at %p and contains \'%s\'\n", buffer_two, buffer_two);
        strcpy(buffer_two, argv[1]);
}
```

8 marks

2. Describe the type of threats you will be able to identify with the STRIDE mnemonic in the Microsoft Security Development Lifecycle.

12 marks

3. A digital computer's instruction set consists of 50 different operations. All instructions have an operation code part (opcode) and an address part (allowing for only one address). Each instruction is stored in one word of memory. How would you calculate the number of bits needed for the opcode?

2 marks

4. What security problems can you identify at the following piece of C code?


```
int main(int argc, char *argv[]) {
  char text[1024];
  strcpy(text, argv[1]);
  printf("\nPrinting user-controlled input:\n");
  printf(text);}
```


5 marks

5. What security problems can you identify at the following piece of C code? How could you avoid the following authentication mechanism from being exploited?

```
int check_authentication(char *password) {
        int auth_flag = 0;
        char password_buffer[16];
        strcpy(password_buffer, password);

        if(strcmp(password_buffer, "brillig") == 0)
                auth_flag = 1;
        if(strcmp(password_buffer, "outgrabe") == 0)
                auth_flag = 1;
        return auth_flag;
}
```

5 marks

6. What will be the value of register %ebx after the following program runs?:

```
    .section .text
.globl _start
_start:
   nop
```

```
    movl $1, %eax
    jmp overhere
    movl $10, %ebx
    int $0x80
overhere:
    movl $
    int $0
```

2 marks

7. How can the Ef[illegible] be exploited in security vulnerabilities?

2 marks

8. Which of the fol[illegible]T binary subtraction of 64 – 15, assuming 8-bit signed Two's compliment representation? Select one:
   a. 01000000 + 11110001 = 00110001
   b. 01001000 + 11001111 = 01001111
   c. 01000100 + 10010000 = 10010000
   d. 01111111 + 11010001 = 01010000
   e. 10000000 + 11110001 = 100110001

1 mark

9. Which of the following components is the fastest? Select one:
   a. Registers
   b. None. The access times are very similar
   c. RAM
   d. Cache
   e. USB

1 mark

10. Describe the difference between big endian and little endian representation.

2 marks

Total: 40 marks

Answers: