NAME: ____

Reverse Engineering MIDTERM EXAM Review

Spring 2023
Computer Science Department, New Mexico State University

1 Review Topics

You can expect 10 multiple choice questions on the tools we have used in the course, and 10 open-ended questions based on a program similar to the one at the end of this handout.

1. You should know what each of the following tools do, and why they are useful to a reverse engineer
    1. InetSim
    2. Hypervisors
    3. Virtual machines
    4. Wireshark
    5. Procmon
    6. regshot
    7. strings
    8. PE Explorer
    9. DependencyWalker
    10. virtual machine snapshots
    11. sandbox services
    12. VirusTotal
    13. PEiD
    14. Ghidra
2. You should also know about the following concepts that are not specifically tools:
    1. network isolation
    2. process isolation
    3. ransomware
    4. viruses vs worms
    5. packers
    6. indicators of compromise
    7. common registers and instructions in x86
    8. static vs dynamic analysis

2 Reverse Engineering

You will be shown simulated output from the Ghidra decompiler like this. We will practice answering sample questions about this function in class.

```
    int main(int param_1, char** param2) {

        uint Uvar1;
        bool Bvar1;
        int Ivar1;
        int Ivar2;
        uint Uvar2;
        char * cptr;
        char c_array_1[6];

        // Loop A
        for (uint iVar1 = 0; iVar1 < 6; iVar1 = iVar1 + 1) {
            c_array_1[iVar1] = 0x00;
        }

        // Loop B
        for (uint iVar2 = 10; iVar2 < 15; iVar2 = iVar2 + 2) {
            c_array_1[iVar2] = ’A’ + iVar2;
        }

        cptr = (char*) ’\0’;

        // Code Label A
        // Hint: getline gets a line of input -- including the trailing newline
        // If the first parameter is null, the first parameter is changed to point to a
        // newly allocated, null-terminated string holding the new line
        getline(&cptr, &Uvar2, stdin);
        Uvar2 = strlen(cptr);
        *(cptr + Uvar2 - 1) = (char*) ’\0’;

        Ivar1 = 0xf;
        Ivar2 = 0x11;

        // Code Label B
        // Hint: strcmp(A,B) returns 0 when strings are equal
        Bvar1 = strcmp(cptr, (char *) c_array_1);
        free(cptr);

        if (Bvar1 != (int) ’\0’) {
            //Option A
            printf(DAT_s_NO_wrong_password, cptr);
            return Ivar1 ^ Ivar2;
        } else {
            //Option B
            printf(DAT_s_Yes_you_did_it_now_make_a_keygen);
        }

        // Code Label C
        Ivar2 = Ivar1;
        Ivar1 = Ivar1 - Ivar2;
        return Ivar1;
    }
```