Corso di laurea magistrale in Cybersecurity

Assignment of Ethical Hacking, Prof. L.V. Mancini

June 13, 2019

1. The administrator account of a Windows server has been compromised. Host software cannot be re-installed for business reasons. With these assumptions, how do you plan and implement post-exploit activities for the host recovery. In particular, list the parts of the system on which to intervene to restore the host's security. Discuss in detail at least one of these areas of intervention, listing the activities to be carried out, the tools, the command lines to be used, etc.

2. Symlink. What are symlinks and how do they work? How can an attacker exploit symlinks (provide an example)? Describe at least one countermeasure.

3. What does it mean that the HTTP protocol is stateless? What limitations come from this fact? What are HTTP sessions and what are the major techniques to implement sessions? Describe in detail the functioning of at least one of these techniques.

4. Describe at least one method to attack WPA Enterprise. What are the possible countermeasures?

5. Buffer overflow attack. Given the following code, identify and explain how you would perform a buffer overflow attack. Show step-by-step how the program stack changes during the execution of the function `func`. Finally, describe at least one countermeasure against standard buffer overflow attacks in UNIX systems.
   For simplicity, you can assume that there is no other function calls in the body of `func`. You do not need to use real bytecode for the exploit and/or real addresses, but rather you can use placeholders such as <payload> and <address_of_…>; please describe for each placeholder used what are the requirements for the exploit to work.

```
void func(char *str) {
    char buffer[128];
    strcpy(buffer, str);
…
}

int main(int argc, char *argv[]) {
...
    func(argv[1]);
...
}
```

   Note that char *argv[] is an array of character pointers, i.e., array of strings, passed to the program as input from the command line.

Test results to be delivered within 2.5 hours.
All answers should be given in English.