1° APPELLO (GIUGNO 2018)

1. Describe at least one technique to determine which services are running or listening on a remote host. Discuss pro and cons, and which tools you may use in practice
2. Describe at least one attack method to gain remote access on a UNIX system. Describe at least one attack method to gain root access. Discuss pro and cons.
3. Describe at least one method for attacking WPA. Which countermeasures can be used?
4. Explain differences between Cross-Site scripting and Cross Site Request Forgery. Which countermeasures can be used?

2° APPELLO (LUGLIO 2018)

1. Discuss the differences between scanning and enumeration. Describe at least one enumeration technique.
2. 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 areas 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 line commands to be used, etc.
3. Describe UNIX permission system and the main attack vectors related to permission system.
4. Describe the SQL injection technique in web applications. Discuss the possible countermeasures. Describe at least one automated SQL injection tool.

3° APPELLO (SETTEMBRE 2018)

1. What is footprinting and which goals does it achieve. Describe the basic steps that should be performed for a through footprinting analysis.
2. Briefly describe at least two main services in Unix Systems that are often remotely attacked. For each of these services explain how the remote attack occurs and discuss the possible countermeasures.
3. An ongoing Advanced persistent threat (APT) attack has compromised one of the Windows servers. With this assumption how do you plan and implement the forensics methodology, the tools, the command lines, etc. to be used, to analyze the "suspicious' host.
4. Explain what is the Advanced Technology Attachment security mechanism (ATA security). Describe the steps of the attack which is able to bypass ATA security. How to defend against such a bypass?

4° APPELLO (GENNAIO 2019)

1. Explain what steps an attacker should take to cover his tracks after successfully gaining administrator privileges on Windows system in order to avoid detection. How attackers can hide their files in the system?
2. Explain briefly what a buffer overflow attack is. Describe at least one buffer overflow technique that allows attackers gain remote access to a UNIX system even when Data Execution Prevention (DEP) is enabled. Describe at least two countermeasures against standard buffer overflow attacks in UNIX systems.
3. Describe at least one method to attack WPA Enterprise. What are the possible countermeasures?

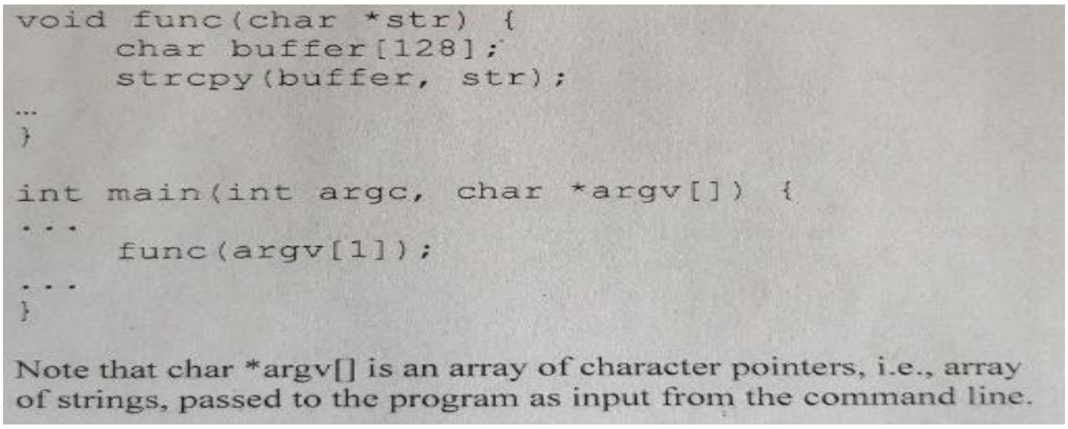
4. Describe the SQL injection technique in web applications. Discuss the possible countermeasures. Describe at least on automated SQL injection tool.

5° APPELLO (FEBBRAIO 2019)

1. What are ping sweeps? Describe at least two host discovery techniques, and at least one tool used to perform host discovery.
2. What are the three main network password exchange protocols used in Windows systems? Describe the pass-the-hash and pass-the-ticket attacks and countermeasures
3. How attackers use back channel to gain remote access to a Unix system? Describe an attack scenario and explain the possible commands that attackers use to create a back channel. Discuss the possible countermeasures.
4. Hacking Other Androids: Describe at least two methods to attack others Android devices. What are the possible countermeasures?

6° APPELLO (GIUGNO 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 areas 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 line commands to be used, etc.
2. Symlink. What are symlinks and how do they work? How can an attacker exploit symlinks (provide an example)? Provide 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, bt 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.