FIT3031 TUTORIAL 10 SOLUTIONS

MALICIOUS SOFTWARE

REVIEW

Q1. What is the role of encryption in the operation of a virus?

Ans: A portion of the virus, generally called a *mutation engine*, creates a random encryption key to encrypt the remainder of the virus. The key is stored with the virus, and the mutation engine itself is altered. When an infected program is invoked, the virus uses the stored random key to decrypt the virus. When the virus replicates, a different random key is selected.

Q2. What are the typical phases of operation of a virus?

Ans: A **dormant** phase, a **propagation** phase, a **triggering** phase, and an **execution** phase

Q3. In general, terms, how does a worm propagate?

Ans:

1. Search for other systems to infect by examining host tables or similar repositories of remote system addresses.
2. Establish a connection with a remote system.
3. Copy itself to the remote system and cause the copy to be run.

Q4. What is a digital immune system?

Ans: This system provides a general-purpose emulation and virus detection system. The objective is to provide rapid response time so that viruses can be stamped out almost as soon as they are introduced. When a new virus enters an organization, the immune system automatically captures it, analyzes it, adds detection and shielding for it, removes it, and passes information about that virus to systems running a general antivirus program so that it can be detected before itis allowed to run elsewhere. See Fig. 10.5 and its description for details.

Q5. How does behaviour-blocking software work?

Behaviour-blocking software integrates with the operating system of a host computer and monitors program behaviour in real-time for malicious actions. The behaviour blocking software then blocks potentially malicious actions before they have a chance to affect the system.

Q6. What is a DDoS?

A denial of service (DoS) attack is an attempt to prevent legitimate users of a service from using that service. When this attack comes from a single host or network node, then it is simply referred to as a DoS attack. A more serious threat is posed by a DDoS attack. In a DDoS attack, an attacker is able to recruit a number of hosts throughout the Internet to simultaneously or in a coordinated fashion launch an attack upon the target.

Problems:

1. Consider the following code fragment:

```
Legitimate code
If date is Friday the 13th;
        Crash_computer();
Legitimate code
```

   What type of malicious software is this?

   Logic bomb.

2. Consider the following code fragment in an authentication program:

```
username = read_username ();
password = read_password ();
if username is "133t h4ck0r"
        return ALLOW_LOGIN;
if username and password are valid
        return ALLOW_LOGIN;
else return DENY_LOGIN;
```

   What type of malicious software is this?

   Backdoor.