MAKERERE UNIVERSITY

COLLEGE OF COMPUTING & INFORMATION SCIENCES

SCHOOL OF COMPUTING & INFORMATICS TECHNOLOGY

CSC 3207: COMPUTER SECURITY

TEST TWO - 2018/2019

Attempt All Questions

1. The software company Socknet is selling a new defense against DDoS attacks. Their software looks at the source IP address on all incoming packets, and if it finds any IP address that accounts for more than 5% of traffic over the last hour, it installs an entry in the router that blocks all packets from that address for the next 24 hours. Their marketing people are claiming that this will stop all DDoS attacks. Give two distinct reasons why this is not a good solution for stopping DDoS attacks. **[6 Marks]**

    - *IP address spoofing, the attacker may be able to ensure that no spoofed IP accounts for more than 5% of the traffic.*
    - *With distributed denial of service, the attacker may be able to use more than 100 machines, so no IP would account for more than 5% of the traffic.*

2. Discuss three ways that a worm uses to replicate itself as a means of accessing remote systems. **[6 Marks]**

    - ***Electronic mail** or instant messenger facility: Worm emails a copy of itself to other systems, or sends itself as an attachment via an of instant message service.*
    - ***File sharing**: Worm either creates a copy of itself or infects other suitable files as a virus on removable media such as a USB drive.*
    - ***Remote execution capability**: Worm executes a copy of itself on another system, either by using an explicit remote execution facility*
    - ***Remote file access** or transfer capability: Worm uses a remote file access or transfer service to another system to copy itself from one system to the other*
    - ***Remote login capability**: Worm logs onto a remote system as a user and then uses commands to copy itself from one system to the other, where it then executes.*

3. Describe three different virus properties that prevent viruses from being detected by an anti-virus software. **[6 Marks]**

- *polymorphism*
- *metamorphism*
- *compression*
- *encryption*

4. One of the categories of malware involves social engineering.

   a. Explain what is meant by a social engineering. **[3 Marks]**
   "Tricking" users to assist in the compromise of their own systems or personal information. This can occur when a user views and responds to some SPAM e-mail, or permits the installation and execution of some Trojan horse program or scripting code.

   b. Describe two main things that could be done to prevent a social engineering attack from succeeding. **[4 Marks]**

   - *Carry out appropriate* ***user awareness and training*** *- This aims to equip users to be more aware of these attacks, and less likely to take actions that result in their compromise*
   - *Set your* ***spam filters to high****. Your email software has spam filters. Check your settings, and set them to high to avoid risky messages flooding into your inbox. Just remember to check them periodically as it is possible legitimate messages could be trapped there from time to time.*

5. Suppose you receive a letter from a finance company stating that your loan payments are in arrears, and that action is required to correct this. However, as far as you know, you have never applied for, or received, a loan from this company.

   a. What may have occurred that led to this loan being created? **[2 Marks]**
   Such a letter strongly suggests that an attacker has collected sufficient personal details about you in order to satisfy the finance company that they are you for the purpose of establishing such a loan. Having taken the money, they have then left you responsible for the repayments.

   b. What type of malware, and on which computer systems, might have provided the necessary information to an attacker that enabled them to successfully obtain this loan? **[4 Marks]**
   Could be one of the following:

   - *This was most likely done using either a* ***phishing attack,*** *perhaps persuading you to complete and return some form with the needed personal details; or*
   - *By using* ***spyware*** *installed on your personal computer system by a worm or trojan horse malware, that then collected the necessary details from files on the system, or*
   - *By* ***monitoring your access*** *to sensitive sites, such as banking sites.*

6. RBAC defines constraints as a relationship among roles or a condition related to roles. Briefly explain the three main types of contraints in RBAC. **[9 Marks]**

   - ***Mutually exclusive roles*** *- are roles such that a user can be assigned to only one role in the set. This limitation could be a static one, or it could be dynamic,* *in the sense that a user could be assigned only one of the roles in the set for a session.*

- ***Cardinality*** *- refers to setting a maximum number with respect to roles. One such constraint is to set a maximum number of users that can be assigned to a given role.*
- *A system might be able to specify a* ***prerequisite role****, which dictates that a user can only be assigned to a particular role if it is already assigned to some other specified role.*

7. In a capability ticket, each user has a number of tickets and may be authorized to loan or give them to others. Since tickets may be dispersed around the system, they present a greater security problem than access control lists.

   a. Explain what this security problem is. **[4 Marks]**
   A capability ticket specifies authorized objects and operations for a particular user. Each user has a number of tickets and may be authorized to loan or give them to others. Because tickets may be dispersed around the system, they present a greater security problem than access control lists.

   b. Explain two ways how the integrity of these capability tickets can be protected and guaranteed. **[6 Marks]**

   - *Have the* ***operating system hold all tickets*** *on behalf of users. These tickets would have to be held in a region of memory inaccessible to users.*
   - *Include an* ***unforgeable token in the capability****. This could be a large random password, or a cryptographic message authentication code. This value is verified by the relevant resource whenever access is requested.*