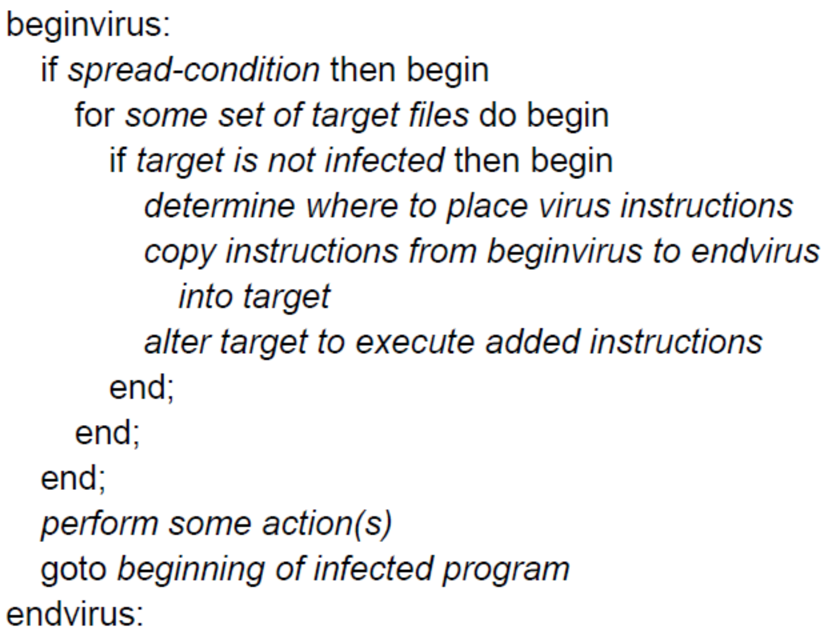
CS 485/585 – Computer Security
Exam 3
Fall 2021

Make sure there are 8 questions.

Name:___________________________

1. Briefly explain the two phases of a computer virus. Indicate the two phases. (You may mark on the following pseudocode). (12 points)



```
beginvirus:
   if spread-condition then begin
      for some set of target files do begin
         if target is not infected then begin
            determine where to place virus instructions
            copy instructions from beginvirus to endvirus
               into target
            alter target to execute added instructions
         end;
      end;
   end;
   perform some action(s)
   goto beginning of infected program
endvirus:
```

Insertion phase is inserting itself into file. (3 points)
Line 2-11 (3 points)

Execution phase is performing some (possibly null) action (3 points)
Line 13, “Perform some action(s) (3 points)

2. (14 points)
a) Explain the Thompson's Compiler. (8 points)

Modify the compiler so that when it compiles login, login accepts the user's correct password or a fixed password (the same one for all users).

Modify the compiler again, so when it compiles a new version of the compiler, the malicious code to do the first step is automatically inserted.

b) Why it was so difficult to ensure second version of the Thompson compiler never released. (6 points)

In this case, performing source code analysis would not be sufficient to detect the malicious code in the compiler and login programs.

3. (18 points)

a) Briefly describe the three models of intrusion detection systems. (6 points)

- Anomaly detection
  - What is usual, is known
  - What is unusual, is bad
- Misuse detection
  - What is bad, is known
  - What is not bad, is good
- Specification-based detection
  - What is good, is known
  - What is not good, is bad

b) (6 points)
Explain false positive and false negative in anomaly detection.

FP/false positives: identify non-anomalous data as anomalous
FN/false negatives: identify anomalous data as non-anomalous

c) Which one, false positive or false negative, is more dangerous in anomaly detection? Why? (6 points)

False negative because an undetected intrusion may cause damages for days or even months.

4. (12 points)
Describe the two purposes of a Trojan horse. Provide an example.

Overt purpose (known to user) and a covert purpose (unknown to user) (3 points each)

(3 points each) Example, Malware learning module, Slide 5
Overt purpose: list files in directory
Covert purpose: create setuid shell

5. (12 points). Determine whether the following statements are correct. Briefly explain your reason.

a). A tiger team (red team) often contributes the least in the flaw elimination stage compared other four stages in the Flaw Hypothesis Methodology.

True.

b) In a penetration testing, a team does not find any vulnerabilities/security flaws. That means that the software/system is therefore verified to satisfy the system constraints.

False. Penetration is not verification.

6. a) Explain Encrypted Viruses. (6 points)

A virus that has a small decryption routine. It makes the virus detection by signature much harder.

b) Compare the encryption/decryption operation in encrypted viruses to the RSA encryption or DES encryption in terms of efficient. (6 points)

The operation has much lower overhead, just one line of code to decipher: (*rC) = (*rC) xor rA xor rB;

7. (8 points)
Explain the difference between Secure Testing and Standard Testing.

Standard software testing focusses on software failure
Secure software testing adds an intelligent adversary

8. (12 points)
What are the three components in an auditing system? Briefly explain their functions.

Logger: records information, usually controlled by parameters
Analyzer: analyzes logged information looking for something
Notifier: reports results of analysis