Systems and Network Security Midterm Exam

Date	**: 24.06.2008**
Duration	: 120 Mins.

Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Total
15	10	10	15	25	10	10	5	15	10	125 pts

Questions

1) **`″Security assurance is what the business pays for and security controls are what it gets.″`**

Please explain the statement above. Where do you see the problem/gap in corporate IT security? **(15 Pt.)**

2) During an incident, you notice that an attacker gained access to one of your servers. You notice these two entries in **`.bash_history`** file of a user:

```
find / -perm -04000 -print
find / -perm -02000 -print
```

a. What is the purpose of these commands? What is the attacker trying to achieve? **(5 Pt.)** (**hint:** -04000 : suid)

b. What actions do you expect him to take afterwards, depending on the result of the commands? **(5 Pt.)**

3) Why does a rootkit modify Import Address Table of a process? Does this affect behavior of other processes? Why/Why not? **(10 Pt.)**

4) Can security controls be security vulnerabilities? Why/Why not? Please use examples to support your arguments. **(15 Pt.)**

5) Company X develops a secure file server solution: "**`Fserver`**". It provides content filtering against data leaks. Fserver allows users to create as many files as necessary but a file can be opened only by one person at a time for business requirements. All read, write etc. requests from another party is denied when file is already opened by someone else. All file modifications are logged and audited.

Fserver uses its own networking protocol. Fserver has successfully gone through a security testing, which involved network attacks, buffer/heap overflows.

The clients are not connected to the Internet. They connect via vpn connections to the file server. There isn’t any network connectivity between any clients.

a. Assuming attacker has installed applications in both workstations previously, how can he/she create a covert channel between Client A and B to exchange data that Fserver doesn’t permit? **(10 Pt.)**

b. Can it be detected with FServer’s built-in security controls? Why/Why not?

(Note: Detectable solutions get 5 Pt. Undetectable solutions get 15 Pt. Wrong claims lose the points from a.)

6) Why do vendors publish MD5/SHA1 hash values when they provide software patches for their customers to download from the Internet? Which part of CIA is this related to? **(10 Pt.)**

7) Why are enterprises, which have proper patch management, still vulnerable against public exploits? **(10 Pt.)**

8) Why should a forensic examiner inspect slack space on disks? **(5 Pt.)**

9) Company Y has its web application and database servers placed in a DMZ, protected by a network firewall. Each packet sent/received from Internet to/from DMZ is filtered by the firewall according the following ruleset:

Order	**Protocol**	**Source Host**	**Source Port**	**Destination Host**	**Destination Port**	**Permit/Deny**
1	TCP	Any	Any	Webserver1	Http	Permit
2	Any	Webserver1	Any	Any	Any	Permit
3	UDP	Any	Any	Any	Any	Permit
4	Any	Any	Any	Any	Any	Deny

Rules are processed from top to bottom. When a match occurs rest of the rules are discarded.

a. What are the current security risks of the servers in this DMZ taking the ruleset into account? **(5 Pt.)**

b. How could you eliminate these risks? **(10 Pt.)**

10) What is ARP spoofing? How can you detect it? **(10 Pt.)**

Good Luck!
Ertunga Arsal