# Final Exam Paper

## CIS 5650 Cybersecurity Essentials

Department of Computer and Information Sciences, Fordham University

Total Score 20 points

### A. Select appropriate answer(s) (10 points)

1. What is the detection method for eavesdropping attack?
    a) Network analysis
    b) Network forensic analysis
    c) Strong cryptography
    d) None of them

2. Select the layer(s) that include the network level firewall
    a) Application layer
    b) IP layer
    c) TCP layer
    d) Network layer

3. Which one of the following offers the facility of application whitelisting?
    a) Antivirus
    b) Antimalware
    c) Codeshield
    d) Previx1

4. Which one is the part of the network intrusion detection systems?
    a) Packet sniffing
    b) Inspecting network traffic
    c) Deploying network firewall
    d) Trust management

5. Select suitable countermeasures for cyber defense.
    a) Demilitarized zone
    b) IDS
    c) IPS
    d) Self-defending networks

6.

7.

8.

9.

10.

## B. Select True or False for the following statements (5 points)

1. IPS cannot recognize unknown anomalies.
2. Keeping monitoring logs is a method to defend the logic bomb attack.
3. More than 75% of vulnerabilities are due to buffer overflow.
4. Inherent risk and residual risk are almost the same, just differ in terms of risk tolerance.
5. Having secret cooperation with outsiders is collusion attack.

## C. Matching Questions (5 points)

### Determine which is the best match for each problem/statement.

| | | | |
|---|---|---|---|
| Trust management | IPS | vulnerability scanner | Defense in Depth |
| 0-Day to patch Availability | DPI | Patching | Firewalls |
| Vulnerability Signature | IDS | Packet filter | Access Controls |

1. A countermeasure that picks an appropriate reputation estimation model for a given application.
2. The Trojan horse would automatically be downloaded and executed on an unsuspecting victim's system only when specific code embedded in a banner ad was accessed with Internet Explorer.
3. A computing activity in which usernames and info on groups, shares, and services of networked computers are retrieved.
4. A software or program that can be designed to assess network systems, computer systems, network applications for potential weaknesses.
5. A software that includes all the abilities of an intrusion detection systems and can also attempt to stop possible cyber incidents.