มหาวิทยาลัยสงขลานครินทร์

คณะวิศวกรรมศาสตร์ ภาควิชาวิศวกรรมคอมพิวเตอร์

การสอบไล่ปลายภาคการศึกษาที่ 2 **ประจำปีการศึกษา 2546**

วันที่ 21 กุมภาพันธ์ 2547 **เวลา 9.00-12.00 น**

วิชา 240-425 Computer Security **ห้องสอบ R200**

ไม่อนุญาตให้นำเอกสารเข้าในห้องสอบ

1. Managed Security Services(MSS) for security improvement(14 marks)
1.1.Explain the following security services given by providers at a client's site as Managed Security Services(MSS) for security improvement:

- Security Policies, Procedures, and Regulations
- Contingency Planning; Operational and Disaster Recovery
- Authentication and Authorization
- Access Control
- Software Integrity
- Monitoring and Auditing
- Incident Management

1.2.Describe risks in engaging an MSS provider for the following issues:

-Trust
-Dependence
-Ownership
-Partnership Failure
-Hidden Costs and Impacts
-Legal Issues

2.Explain the following network boundary protection as Managed Security Services:(16 marks)
2.1.A managed firewall service

-Bandwidth/Throughput
-Rules Management
-Firewall Visibility
-Monitoring (Proactive)
-Stateful Packet Filtering
-Network Address Translation (NAT)
-Firewall System Reports

2.2.A managed Intrusion Detection System(IDS) service
-Multiple Network Sensors and Sensor Locations
-Host-Based and Network-Based
-Signature-Based and Anomaly-Based
-IDS Visibility
-Monitoring (Proactive)
-Throughput
-IDS Reports

2.3.A managed Virtual Private Network(VPN) service
-Bandwidth/Throughput
-Authentication Alternatives
-Encryption
-Use Statistics

3. Securing desktop workstations for security improvement. (14 marks)
3.1.Describe actions for securing desktop workstations for security improvement for the following categories:
-Planning deployment
-Configuring workstations
-Maintaining workstation integrity
-Improving user awareness

3.2.Explain the following detailed actions needed for securing desktop workstations by configuring computers for user authentication.
-Configure the system to use available authentication capabilities.
-Remove unneeded default accounts and groups.
-Change default passwords.
-Create the user groups for the particular computer.
-Create the user accounts for the particular computer.
-Ensure users follow your password policy.
-Configure computers to require reauthentication after idle periods.
-Configure computers to deny login after a small number of failed attempts.
-Install and configure other authentication mechanisms as required by your organization's security plan and policies.

4. Securing Public Web Servers (14 marks)
4.1.Describe actions for securing public web servers for security improvement with the following categories:
-Configuring server technology
-Maintaining server integrity

4.2.Explain the following detailed actions needed for securing public Web servers by configuring the Web server with appropriate object, device, and file access controls:

-Configure the Web server to execute only under a unique individual user and group identity.
-Identify the protection needed for files, devices, and objects specific to the Web server.
-Limit the use of resources by the Web server host operating system to mitigate the effects of DoS attacks.
-Configure time-outs and other controls to mitigate the effects of DoS attacks.
-Configure the public Web server so it cannot serve files that are outside of the specified file directory tree for public Web content.
-Configure Web server software access controls.
-Disable the serving of Web server file directory listings.

5. Responding to intrusions (14 marks)
5.1. Describe actions needed for responding to intrusions for security improvement with the following categories:
-Preparation.
-Handling of intrusions.
-Follow up.

5.2.What are detailed actions needed for responding to intrusions by collecting and protecting information associated with an intrusion.
-Collect all information related to an intrusion.
-Collect and preserve evidence.
-Ensure evidence is captured and preserved securely.
-Preserve the chain of custody for all evidence
-Contact law enforcement immediately if you decide to pursue and prosecute an intruder.

6. Deploying firewalls (14 marks)
6.1 Describe actions needed for deploying firewalls for security improvement with the following categories:
-Preparation.
-Configuring of firewalls.
-Testing.
-Deployment.
6.2.Describe detailed actions needed for deploying Firewalls by configuring firewall logging and alert mechanisms.
-Design the logging environment

-Select logging options for packet filter rules
-Design the alert mechanism configuration
-Acquire or develop supporting tools

7. Firewalls functions and topologies. (14 marks)
7.1.Explain the following firewall functions
-Packet filtering
-Application proxies
-Stateful inspection or dynamic packet filtering

7.2. Explain the following firewall topologies with the help of diagrams.
-Basic border firewall
-Untrustworthy host
-DMZ network
-Dual firewall