

Week 7 Tutorial: Security Technologies- IDS, IPS and Other Security Tools

Group Discussion and Analysis (60 minutes)

Groups discussion continues using the same scenarios and groups allocation as previous weeks.

Scenario topics:

1. An online holiday booking system.
2. A medium size school timetabling and attendance system
3. An estate agent web application
4. A restaurant self-service digital ordering system

IDS, IPS and Other Security Tools (1 hour)

Each group must:

a) Choose Suitable IDS and IPS Types

1. Evaluate different IDS and IPS types, such as:
 - Network-based IDS (NIDS)
 - Host-based IDS (HIDS)
 - Signature-based IDS/IPS
 - Anomaly-based IDS/IPS
 - Hybrid IDS/IPS
2. Determine the most appropriate IDS/IPS solution for your system, considering:
 - The nature and sensitivity of the data being protected
 - The level of threat intelligence required
 - System architecture (on-premises, cloud, hybrid)
 - Performance impact and false positive rates
3. Justify your choice of IDS/IPS, explaining why it best suits your security needs.
4. Research a specific IDS/IPS product that meets your selected type. Consider:
 - Vendor reputation and support
 - Features (e.g., real-time monitoring, automated response, integration with SIEM)
 - Cost and scalability
 - Compatibility with existing security infrastructure

b) Deploying Honeypots for Threat Analysis

1. Assess different types of honeypots, such as:
 - Low-interaction vs. High-interaction honeypots
 - Research honeypots vs. Production honeypots
 - Client honeypots vs. Server honeypots
2. Determine the most appropriate honeypot deployment for your system, considering:
 - The type of threats your organization faces
 - Whether you need to study attacker behaviour or divert attacks
 - System resources and risks associated with honeypot exposure
3. Justify the selection of the honeypot type, explaining how it enhances network security.
4. Research a honeypot solution that aligns with your choice. Consider:
 - Open-source vs. commercial solutions
 - Ease of deployment and maintenance
 - Logging and analysis capabilities

Presentation (10 minutes each)

Each group will present their findings, covering:

- Key network security requirements based on last week's risk assessment.
- Chosen IDS/IPS type and justification.
- Researched IDS/IPS product and why it meets the needs.
- Chosen honeypot type and justification.
- Implementation of IDS/IPS rules, honeypot deployment, and monitoring mechanisms.

Class Discussion (30 minutes)

The remaining of the session is focused on the assignment and how you should align this week activity with the assignment tasks.