7(E) Protect Web Servers Using Security Tools

7(E)(i) ID Server

Aim

To protect a web server using ID Server.

Tools Used

• ID Server
• Windows Operating System

Theory

ID Server is an intrusion detection tool that monitors server activities and generates alerts for suspicious access attempts.

Steps / Procedure

1. Install ID Server on the web server.
2. Configure intrusion detection rules.
3. Start monitoring server activity.
4. Detect unauthorized access attempts.
5. Generate alerts for security violations.

Result

ID Server successfully detected intrusion attempts on the web server.

7(E)(ii) Microsoft Baseline Security Analyzer (MBSA)

Aim

To analyze system security using Microsoft Baseline Security Analyzer.

Tools Used

• Microsoft Baseline Security Analyzer
• Windows Operating System

Theory

MBSA scans systems for missing updates, weak passwords, and security misconfigurations.

Steps / Procedure

1. Download and install MBSA.
2. Launch the MBSA tool.
3. Select **Scan a Computer**.
4. Start the security scan.
5. Identify missing updates and vulnerabilities.
6. Generate security report.

Result

System security vulnerabilities were successfully identified using MBSA.

7(E)(iii) Syhunt Hybrid

Aim

To perform web server vulnerability scanning using Syhunt Hybrid.

Tools Used

• Syhunt Hybrid
• Windows Operating System

Theory

Syhunt Hybrid is a security scanning tool used to detect web vulnerabilities such as SQL Injection, XSS, and server misconfigurations.

Steps / Procedure

1. Install Syhunt Hybrid.
2. Launch the application.
3. Enter the target web server URL.
4. Configure scan options.
5. Start the vulnerability scan.
6. Analyze the generated report.

Result

Web server vulnerabilities were successfully detected using Syhunt Hybrid.

Final Conclusion

Practical No. 7 successfully demonstrated web security scanning, session hijacking, firewall protection, honeypot monitoring, and web server security tools.