2.1 Produce a project specification for a networking and cybersecurity project in line with requirements.

Project specification for a networking and cyber security project

1.Project overview

Title : Comprehensive Penetration Testing of Corporate Network Infrastructure

Start Date : 1 August 2024

End Date : 12 September 2024

Budget : £ 50,000 - £ 100,000

Stakeholders: Project sponsor, CISO, IT and security teams, Ethical Hacking team, Compliance and Legal team, Business Unit Leaders

2.Objectives/Goal

Identify vulnerabilities and weaknesses in the network

Evaluate the effectiveness of security measures

Exploit vulnerabilities and execute attacks

Enhance Incident Response Capabilities

Improve the overall cybersecurity posture of the organization

3.Scope

Target systems and Applications:

- Networks – Internal and external network infrastructure, routers, switches, firewalls, wireless networks.
- Servers – Web servers, database servers, file servers, application servers, mail servers.
- Applications – Web applications, mobile applications, software applications.
- End devices, IoT devices
- Cloud-based infrastructure and services

Testing techniques:

- External Penetration Testing
- Internal Penetration Testing

- Web Application Testing
- Social Engineering
- Wireless Network Testing
- Physical Security Testing

Methodologies and standards:

- OWASP for application testing
- Follow CREST standards
- CHECK Scheme
- OSSTMM for open source security testing
- NIST framework and CPNI guidelines

4.Deliverable

- Tested specific high vulnerabilities, weaknesses
- Risk Assessment
- Recommendation for addressing each issues
- Improve network infrastructure
- Enhance security measures

5.Project Plan

Week 1-2 : Planning, Scoping, and Reconnaissance

Week 3 : Vulnerability Analysis

Week 4 : Execute attacks and Exploitation network

Week 5 :Report and Recommendation

Week 6 : Clearing tracks of hacking activities

6.Risk and Mitigation

Potential Risks :

- Delays in hardware procurement
- Emerging cybersecurity threats
- Inaccurate test results
- Disruptions on network performance
- Legal and compliance issues
- Data Loss

Mitigation :

- Have spare hardware, establish strong relationships with multiple vendors
- Conduct regular updates, continuously monitor network activities
- Use multiple testing tools and techniques, perform by experienced and certified penetration tester
- Schedule penetration test during off-peak hours
- Obtain written consent, review legal and regulatory requirements, follow testing scope and methodologies
- Backup data and system before testing, implement data recovery and restoration backup procedures

7. Budget and resources

Budget:

- Project planning and scoping : £ 1,000 - £ 2,000
- Reconnaissance and Information gathering : £ 5,000 - £ 12,000
- Vulnerability Analysis : £ 10,000 - £ 22,000
- Exploitation : £ 10,000 - £ 28,000
- Post-Exploitation, Report and Recommendation - £ 10,000 - £ 25,000
- Retesting and Validation - £ 5,000 - £ 10,000

Resources:

- Project Manager
- Lead Ethical Hacker (Senior Penetration Tester)
- Ethical Hacker (Junior Penetration Tester)
- Security Analyst
- IT support staff
- Compliance officer

8. Communication Plan

- Meeting and updates by every three days for the progress reports
- After final report writing, present findings to Project sponsor, CISO, and stakeholders
- Conduct post-project review with ethical hacking team and stakeholders to review the project's success and challenges.

9. Compliance and Confidentiality

- Ensure all findings and reports are kept confidential and shared only with authorized personnel.