Jayabheri apartments,Kukatpally
TESTING 2, TAVVA
E-mail: tavvaforu@gmail.com
Phone: 98098909033
Fax: 5678909487

Estimation #5048

To: Serge Software

Hyderabad,
Kondapur,500072,
P: 890987678,
E-mail: tavvaforu@gmail.com

Estimation Date: Nov 15, 2016

Description	Total
Vulnerability Assessment	$5,200.00
Network Penetration Testing	$5,200.00

Sub - Total amount: $10,400.00

Grand Total: $10,400.00

SERGE TECHNOLOGIES Service Overview

We are proud to submit the following quote in support of our client's efforts to assess and improve the maturity of their information security program. We are a leading provider of information security testing and consulting services, partnering with our customers to improve the safety and security of their employees

The proposed services in this Statement of Work are:

1. Vulnerability Management
2. Network Penetration Testing (external, internal or both)
3. Web/Mobile Application Security Assessment
4. Email Phishing Campaign

The following sections provide additional details about each service including pricing and payment terms.

Selected Services Descriptions

Vulnerability Assessments & Management

A vulnerability assessment is the process of identifying and quantifying security vulnerabilities in an environment. It is an in-depth evaluation of your information security posture, indicating weaknesses as well as providing the appropriate mitigation procedures required to either eliminate those weaknesses or reduce them to an acceptable level of risk

Vulnerability assessments consist of:

1. Defining and classifying network or system resources
2. Assigning relative levels of importance to the resources
3. Identifying potential threats to each resource
4. Developing a strategy to deal with the most serious potential problems first
5. Defining and implementing ways to minimize the consequences if an attack occurs

The vulnerability management service offering is a complete solution for finding and tracking the remediation of vulnerabilities within the Client enterprise. Vulnerabilities are well-known flaws, usually a result of out-of- date software, missing patches or a misconfiguration that would enable an attacker to cause an unauthorized change to the way systems operate or process data.

Vulnerability Management Process

1. System and Service Discovery/Scoping
2. Vulnerability Identification & Manual Verification
3. Remediation Building Development
4. Reporting
5. Tracking of Findings
6. Testing to Confirm Remediation
7. Report & Presentation
8. Reassessment

Vulnerability management is a continuous testing cycle. New patches are always being issued, software and applications are reaching the end of support and system configurations are changed as new requirements are added.

Deliverables include detailed report of findings for the current cycle, trending information to show the progress of remediation for previous issues and vulnerability data in an easy-to- import format based on specific requirements. All final report materials will be provided in a generic format where you can add your corporate logo and contact information.

Network Penetration Testing (external, internal or both)

A network penetration test simulates the actions of an external and/or internal cyber attacker that aims to breach the information security of the organization. Using many tools and techniques, the penetration tester (ethical hacker) attempts to exploit critical systems and gain access to sensitive data.

A penetration test doesn’t stop at simply uncovering vulnerabilities: it goes the next step to actively exploit those vulnerabilities in order to prove (or disprove) a real-world attack would be successful and what systems and data that attacker could gain access to.

Our teams use the Penetration Testing Execution Standard (PTES) framework when conducting these types of assessments. Following this framework, we execute the following phases in our network penetration testing service:

Network Penetration Process

1. Goals and Rules Scoping
2. Intelligence Gathering – Recon and Mapping
3. Vulnerability Analysis and Identification
4. Exploitation
5. Post Exploitation
6. Remediation Exploration
7. Report and Presentation

8. Reassessment

Throughout the network penetration test, we will cycle through the phases, gathering intelligence and analyzing vulnerabilities the further into the network they reach. The final report includes a detailed write-up of findings, as well as a comprehensive list of testing activities red flags which enable full visibility into how well your security controls performed during the assessment. Findings can also be delivered in an easy-to- import format based on certain requirements. All final report materials will be provided in a generic format where you can add your corporate logo and contact information.

Vulnerability Assessments vs Network Penetration Testing

Simply said, a vulnerability assessment identifies vulnerabilities in an external (web facing) and internal network as well as instructions on how to fix these vulnerabilities. It would be like getting an opinion from your home security company on where a robber would potentially break in your home and how to secure it.

A penetration test is the next step after you have had a good vulnerability assessment(s). The penetration test finds any remaining external (web facing) and internal network vulnerabilities, but the test also exploits these vulnerabilities to access systems and data, which helps to display your actual risk. Using the home security example, it would then be like getting a “ethical robber” to try to break into your home and if a break in is successful, what the robber could destroy or steal…hence how much you would lose.

Assumptions

All service quotes above are based on information provided through our service provider online portal. This is only an initial security services quick quote. Once we execute a statement of work, we will verify all assumptions and if necessary, provide an amended statement of work.