Especificaciones Técnicas para Ethical Hacking

OBJETIVO PRINCIPAL

El BANCO DEL ESTADO, requiere efectuar un estudio de Ethical Hacking sobre su infraestructura", que permita identificar y corregir las vulnerabilidades existentes en las configuraciones de los equipos y sistemas que conforman la plataforma tecnológica.

El Banco del Estado tiene como plataforma a nivel de software los siguientes productos: Microsoft Windows 2008 R2 Server, Windows 7 y XP profesional, Microsoft Isa Server 2006, Exchange Server 2010 y en su infraestructura de hardware cuenta con un firewall Fortinet Cisco. .Por lo que es importante que la empresa que participe en este concurso disponga de técnicos especializados en la mencionada infraestructura y cumplan con las siguientes competencias:

1. Advanced Infrastructure Solutions
2. Networking Infrastructure Solutions
3. Security Solutions
4. Development solutions.

Como requerimiento para la empresa adjudicada se ha establecido:

El desarrollo de la consultoría deberá estar enmarcado en los lineamientos, metodologías y estándares internacionales OSSTMM, NIST 800-115, ISSAF, y OWASP para lo cual en el cronograma detallado de ejecución se deberá establecer la aplicabilidad de los mismos. Este cronograma deberá ser presentado por el proveedor para la aprobación de Banco del Estado antes del inicio de cualquier actividad.

El líder del proyecto deberá tener al menos tres certificaciónes internacionales en temas de Ethical Hacking, entre los cuales pueden ser: CISSP, CEH, GPEN, GWAPT, LPT, CHFI, ECSA), las cuales deben estar vigentes y validadas por su emisor, o deben indicar el link de validación de las mismas.. Los títulos universitarios obtenidos por el líder del proyecto deberán ser emitidos por universidades nacionales y registrados en el Senescyt. En caso de títulos emitidos por universidades extranjeras, éstos deberán ser reconocidos e inscritos por el Senescyt.

Deberán asignarse además al menos un consultor senior al proyecto el cual con el líder del proyecto debe disponer al menos dos de las siguientes certificaciones: CEH, GPEN, GWAPT, LPT, CHFI, ECSA,), las cuales deben estar vigentes y validadas por su emisor, o deben indicar el link de validación de las mismas.

La empresa oferente deberá demostrar experiencia de por lo menos dos proyectos de ethical hacking o penetration testing en los dos últimos años, dentro o fuera del país.

Conocimiento sobre normativa de seguridad informática vigente para el sistema financiero e instituciones públicas del Ecuador

La empresa deberá tener oficina local y deberá estar domiciliada en el Ecuador.

La omisión de cualquiera de los requerimientos o documentación podrá ser motivo de descalificación del proponente de esta Selección de Cotizaciones.

El plazo de ejecución del contrato será de cuarenta y cinco (45) días laborables, contados a partir de la fecha de inicio de ejecución señalada por EL BANCO DEL ESTADO, el lugar de ejecución será en las oficinas de la Matriz del BANCO DEL ESTADO en la ciudad de Quito y en la Sucursal del Banco en la ciudad de Portoviejo.

OBJETIVOS ESPECIFICOS.

El contratista deberá ejecutar como mínimo la siguiente lista de Pruebas de Ethical Hacking, si el contratista considera que hay pruebas adicionales que se deban hacer debe incluirlas en su oferta y detallarlas.

- Escaneo y análisis de puertos;
- Escaneo y análisis de vulnerabilidades
- Escaneo de vulnerabilidades de Base de Datos y servicio de correo
- Identificar el estado actual de los parches instalados en los sistemas operativos, servidores y base de datos.
- Evaluación de las seguridades tecnológicas implementadas en el servicio de acceso a Internet
- Evaluación de los niveles de control de accesos lógicos a la infraestructura de servidores, redes y comunicaciones
- Evaluación de configuración de seguridad establecida en la red inalámbrica.
- Evaluación de la configuración y diseño de las conexiones VPN.
- Desbordamiento de buffer;
- Fuerza bruta sobre el servicio de acceso remoto;
- Fuerza bruta sobre el servicio de autenticación de las Aplicaciones
- Google Hacking;
- Ataque de aplicaciones web
- Inyección de SQL, SSI, LDAP;
- Travesía de Trayectoria (Path Traversal);
- Inyección de comandos del sistema operativo;
- XSS Secuencias de Comandos entre sitios (Cross Site Scripting);
- Falsificación de petición en sitios cruzados (Cross Site Request Forgeries);
- Control de autorización erróneo sobre aplicaciones del sitio Web;
- Análisis de direcciones IPs públicas para identificar vulnerabilidades;
- Explotar vulnerabilidades de los servidores Web con el uso de programas exploit;
- Análisis y aprovechamiento de vulnerabilidades de los servidores, mediante el uso de programas exploit;
- Ataques de denegación de servicio para la red Ethernet e inalámbrica;
- Ataques de vulnerabilidades;
- Ataques de autenticación;
- Escalamiento de privilegios;
- Suplantación de credenciales;
- Usuarios o Claves en aplicaciones en texto plano.
- Manejo de sesiones
- Análisis de la topología de los equipos de seguridad perimetral
- Backdoors "Puerta trasera"
- CGI Abuses. "Common Gateway Interface"
- Finger Abuses
- FTP. "Pruebas de configuración y debilidades en versiones especificas"
- Gain a Shell Remotely "Ejecución de comandos en el servidor"
- Gain Root Remotely "Obtener cuenta administrador remotamente"
- NIS "Network Information Systems"
- Remote File Access "Posibilidad de re-escribir archivos del servidor utilizando puertos conocidos"

Las pruebas internas de tipo graybox, se las realizara a los servidores de red con los siguientes servicios: IIS, Motor de Base de Datos, Correo Electrónico, Share Point, Directorio Activo, Servidor de aplicación financiera, un grupo de computadoras de escritorio, aplicaciones de datos tanto desde la red Lan como desde la red Wan. los equipos a ser verificados y su ubicación son:

- Directorio Activo 3, 2 en Quito y 1 en Portoviejo

- Base de datos SQL 1en Quito,
- Intranet 1, en Quito
- Extranet 1, en Quito
- Correo Exchange 1en Quito.
- Correo SMTP 1, en Quito
- Switch 2, en Quito
- Router 3, 2 en Quito y 1 en Portoviejo
- Firewall 1 en Quito
- Proxy 1, en Quito
- Web 1, en Quito
- Computadores de escritorio 15, 10 en Quito y 5 en Portoviejo.
- Computadoras portables 5, en Quito

El proveedor deberá utilizar al menos una herramienta de software comercial de escaneo de vulnerabilidades y otra de explotación presentes en el cuadrante de Gartner y/o Forrester.
Las herramientas de escaneo de vulnerabilidades y explotación deben incluir Bases de Datos aActualizadas a la fecha de realización de la consultoría.

El proveedor deberá realizar al menos dos pruebas de ingeniería social, aprobadas previamente por Banco del Estado

FASES DE EJECUCIÓN

1.1.1 Capacitación

La empresa adjudicada realizará una capacitación de al menos 45 horas para 5 funcionarios de la Gerencia de Informática sobre seguridad informática considerando los siguientes puntos:

La capacitación deberá ser al menos un 90% práctico
Inlcuir temas de:

- Introducción al Ethical Hacking
- Footprinting y reconocimiento
- Escaneo de redes
- Enumeracion
- Hacking de sistemas
- Troyanos y backdoors
- Virus y gusanos
- Sniffers
- Ingeniería social
- Denegación de servicio
- Secuestro de sesiones
- Hackeo de servidores web
- Hackeo de aplicaciones web
- Inyección SQL
- Hackeo de redes inalámbricas
- Evasión de IDS, firewalls y honeypots
- Desbordamiento de bufer
- Criptografía
- Penetration Testing

Deberían generar una charla de concientización, de por lo menos 3 horas, para todo el personal del Banco del Estado en la Ciudad de Quito

- Responsabilidad sobre la información.
- Fugas de información.

- Análisis de Riesgos.
- Normativa legal sobre seguridad informática para instituciones financieras y sector público.

1.1.2 Etapa de Análisis.

Etapa en la que se realizará el análisis de la infraestructura y sus configuraciones de acuerdo al alcance establecido en el punto "Objetivos específicos" del presente documento.
Se deberá contemplar también el análisis de resultados del último ethical hacking realizado.

1.1.3 Plan de Acción.

La empresa consultora adjudicada establecerá una metodología y cronograma para la ejecución del estudio. El contratista deberá proponer un plan de ejecución del servicio de Ethical Hacking, el que será aprobado por la Gerencia de Informática.
El plan de acción deberá contemplar la evaluación de resultados del último estudio de ethical hacking realizado versus los resultados obtenidos, como medio de control.

1.1.4 Ejecución del Servicio

La empresa adjudicada realizará el estudio de ethical hacking de acuerdo al cronograma aprobado, en la ejecución de las pruebas intervendrán funcionarios de la Dirección de Sistemas de Información~~Gerencia de Informática~~.

RESPONSABILIDAD Y CONFIDENCIALIDAD

La empresa adjudicada asume la responsabilidad sobre el manejo de la información, debiendo garantizar la integridad y disponibilidad de la misma durante la ejecución de las pruebas, además mantendrá la información tanto institucional como del resultado de las pruebas bajo estricta confidencialidad; pudiendo el Banco del Estado realizar las verificaciones necesarias en cualquier momento.

Para tales efectos se tendrá como confidencial cualquier información no divulgada que posea legítimamente su titular que pueda usarse en alguna actividad productiva, industrial o comercial, y que sea susceptible de transmitirse a un tercero, en la medida en que dicha información sea secreta, en el sentido que como conjunto o en la configuración y reunión precisa de sus componentes no sea generalmente conocida ni fácilmente accesible a quienes se encuentran en los círculos que en forma usual manejan la información respectiva, tenga un valor comercial por ser secreta, y haya sido objeto de medidas razonables tomadas por su legítimo poseedor para mantenerla secreta.

La obligación de reserva consiste en abstenerse de usar, facilitar, divulgar o revelar, sin causa justificada y sin consentimiento del titular, la información sobre cuya confidencialidad se la haya prevenido en forma verbal o escrita; dicha obligación subsistirá durante la vigencia del contrato, y luego de su terminación mientras subsistan las características para considerarla como información confidencial.

ENTREGABLES.

La empresa adjudicada deberá entregar:

- Informes tanto técnicos, como ejecutivos especificando las vulnerabilidades encontradas, nivel de riesgo, y las recomendaciones y/o posibles soluciones a dichas vulnerabilidades.
- Informe con los resultados de todas las pruebas realizadas.
- Plan de remediación para eliminar vulnerabilidades encontradas.
- Certificados de asistencia de las capacitaciones brindadas
- Matriz de control y seguimiento de los resultados del ethical hacking versus los resultados obtenidos en el último ethical hacking