Inycom

CONSULTORÍA DE HACKING ÉTICO

Sistemas y Comunicaciones
www.inycom.es
info@inycom.es
902 511 004

Descubra y ponga remedio a los riesgos de seguridad y vulnerabilidades de sus sistemas informáticos

QUÉ ES HACKING ÉTICO

Consiste en la penetración en los sistemas informáticos de una organización, de la misma forma que lo haría un hacker o pirata informático, aunque de forma autorizada y controlada. El resultado es un informe donde se identifican los sistemas en los que se ha logrado acceder y la información confidencial y/o secreta conseguida.

Cada proyecto se estudia individualmente y se realiza una propuesta de servicios que puede combinar diversos ámbitos de auditoría (interna, externa, de sistemas, de aplicaciones web, etc) en función de las necesidades específicas de cada cliente.

METODOLOGÍA, ESTÁNDARES Y HERRAMIENTAS

La metodología utilizada es la provista por EC-Council en su certificación C|EH (Certified Ethical Hacker).

- **Reconocimiento.**

  Recopilación inicial de toda la información posible acerca del objetivo, con la intención de identificar posibles vectores de ataque.

- **Escaneo.**

  Identificación de equipamiento, servicios y puertos en la red objetivo y sus posibles vulnerabilidades. Extracción de nombres de usuarios, contraseñas, nombres de máquinas, recursos compartidos y servicios del sistema en un entorno de intranet.

- **Obtención de acceso.**

  Entrada en el sistema utilizando diversas tecnologías ofensivas (virus, troyanos, exploits, servicios configurados con valores de fábrica, etc) y a través de los vectores de ataque recopilados anteriormente. Una vez dentro de la red, escalada de privilegios hasta alcanzar los permisos más elevados.

- **Mantenimiento del acceso.**

  Instalación de rootkits, troyanos, backdoors, keyloggers, etc. que permitan mantener el acceso fácil y continuado a la red.

- **Borrado de evidencias.**

  Eliminación de cualquier rastro del ataque mediante la manipulación de los logs, entre otros.

Metodología EC-Council · Certificación C|EH

Sistemas y Comunicaciones
www.inycom.es
info@inycom.es
902 511 004

SERVICIOS DE HACKING ÉTICO

1.

HACKING ÉTICO EXTERNO CAJA BLANCA

- Información facilitada por el cliente para realizar la intrusión.
- Análisis en profundidad de las brechas de seguridad de los sistemas sometidos a estudio.
- Informe amplio y detallado de las vulnerabilidades y recomendaciones para solventarlas.

2.

HACKING ÉTICO EXTERNO CAJA NEGRA

- Información para realizar la intrusión no facilitada por el cliente.
- Análisis en profundidad y extensión de todas las brechas de seguridad de los sistemas sometidos a estudio.
- Informe amplio y detallado de las vulnerabilidades y recomendaciones para solventarlas.

3.

HACKING ÉTICO INTERNO

- Auditoría acotada a la red interna de la empresa.
- Necesaria la presencia de los especialistas de Inycom en las instalaciones de la empresa a auditar.
- Informe amplio y detallado de las vulnerabilidades de la red interna y recomendaciones para solventarlas.

4.

HACKING ÉTICO DE APLICACIONES WEB

- Simulación de ataques reales contra las vulnerabilidades de una o varias aplicaciones (ej. correo electrónico, bases de datos, etc.).
- No es necesaria la entrega del código fuente de la aplicación.
- Informe amplio y detallado de las vulnerabilidades y recomendaciones para solventarlas.
- Análisis OWASP Top Ten.

5.

HACKING ÉTICO DE SISTEMAS DE COMUNICACIONES

- Análisis de la seguridad de las comunicaciones (redes de datos, hardware de red, comunicaciones de voz, fraude en telecomunicaciones, etc.)
- Informe amplio y detallado de las vulnerabilidades y recomendaciones para solventarlas.

6.

HACKING ÉTICO VOIP

- Identificación de los puntos débiles en una infraestructura de comunicaciones para minimizar riesgos como robo de servicio, interceptación de comunicaciones, denegación de comunicaciones telefónicas, etc.
- Identificación de posibles nuevas vías de ataque en las redes de datos, con motivo de su modificación para permitir el uso de VoIP.

7.

TEST DE DENEGACIÓN DE SERVICIO (DOS)

- Test que refleja el grado de solidez o resistencia de un servicio ante la agresión de un atacante (local o remoto) que intente deshabilitarlo.
- Informe detallado de los resultados obtenidos incluyendo, en su caso, la descripción de las situaciones específicas en las que se ha conseguido la denegación del servicio.

Rev. 001 febrero 2012