HACKING ÉTICO

Detecte las vulnerabilidades a las que están expuestas las redes, sistemas y aplicaciones de su empresa

La seguridad informática continúa creciendo debido a que los intentos de vulnerar activos informáticos también siguen al alza. Las redes y aplicaciones son vulneradas para ser aprovechadas por terceros para robar información crítica, cobrar recompensas o simplemente difamar el objetivo, obligando a las empresas a incurrir en costos enormes tanto en su reputación como monetarios luego de que se concreta un ataque por parte de terceros.

La forma más efectiva para conocer las vulnerabilidades y mitigar los accesos no autorizados es ejecutar Hacking Ético sobre activos informáticos que tienen algún nivel de exposición.

Este servicio simula un ataque informático sobre activos individualizados estableciendo las vulnerabilidades presentes en las redes, sistemas o aplicaciones definidas. Durante el ataque se usan herramientas utilizadas por hackers para conocer las vulnerabilidades y explotar las mismas hasta obtener acceso. El tipo de ataque, junto con la profundidad de éste se acuerdan con anterioridad de tal forma de mitigar o eliminar las vulnerabilidades encontradas.

El servicio entregará un reporte que le permitirá al cliente conocer las vulnerabilidades y corregir los problemas encontrados.

Proceso

IIA adhiere a procesos conocidos en la Industria de servicios de seguridad que permiten a nuestros clientes obtener lo que necesitan de acuerdo a normas predefinidas que se ajustan a un marco de trabajo que permita analizar los resultados por etapas.

1. Planificación

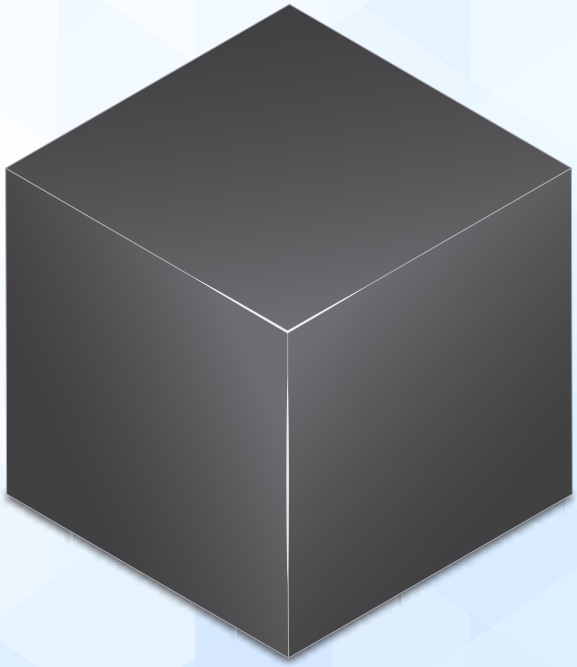
En la etapa de planificación se acuerdan los plazos y objetivos de la actividad afinando los detalles del tipo de reconocimiento, scan y acceso que el cliente desea. Como parte de esta etapa se firma un acuerdo de confidencialidad que establece las autorizaciones y responsabilidades adecuadas y permitirán el desarrollo de la actividad de forma segura para todas las partes.

2. Reconocimiento

La etapa de reconocimiento considera buscar y obtener información del objeto destino que está disponible libremente y que puede apoyar en el hackeo que se desea realizar. Puede incluir técnicas de ingeniería social, uso de medios de comunicación establecidos. En la mayoría de los casos el mismo proceso entrega información para abordar la manera de intentar hackear el objeto.

3. Scan

Esta etapa se refiere a descubrir las vulnerabilidades que pueden estar presentes. Se realiza usando herramientas manuales y automatizadas. El tipo de scan a ejecutar puede ser de dos tipos:



Blackbox

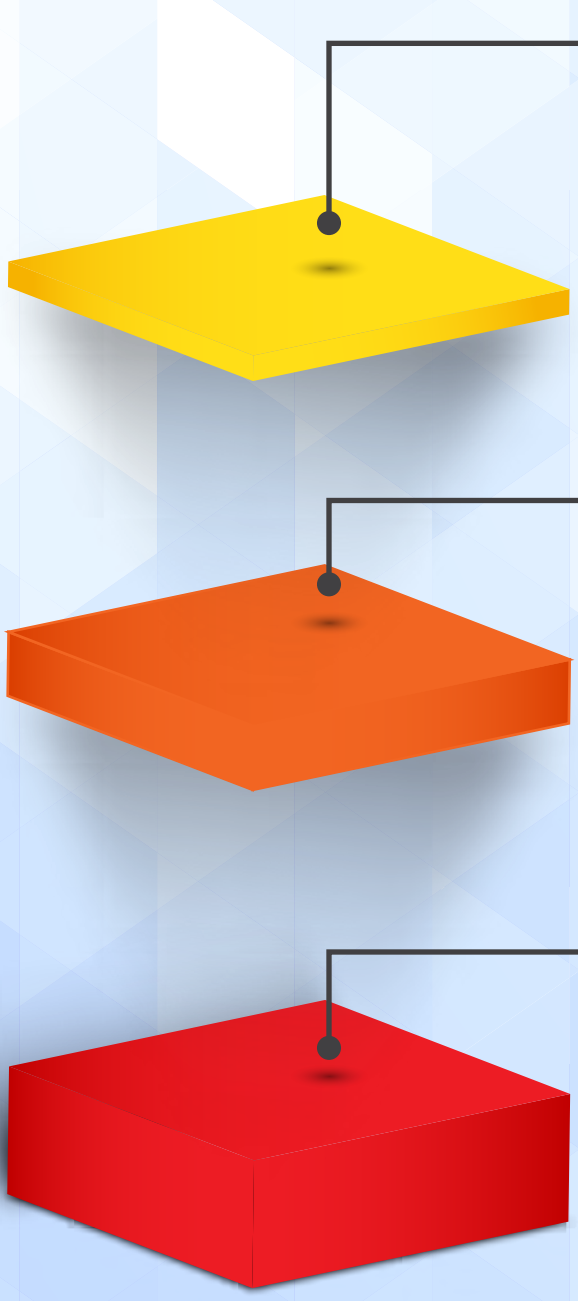
El scan se realiza sin tener información previa del objetivo. Sólo se cuenta con las fuentes conocidas públicamente o en herramientas expuestas al público, además de los métodos usados en la etapa de reconocimiento. Se usa cuando el contratante desea probar las medidas de seguridad existentes que protegen tanto la arquitectura del objetivo como la información.

Whitebox

El contratante provee información formal acerca del objetivo. Normalmente se realiza cuando se desea evaluar partes específicas de una red o aplicación o simular un intento de vulneración por parte de agentes internos. Puede ser un nombre de usuario para acceder a una red o aplicación que permita un acceso inicial mayor al que tiene un agente externo a la organización.

4. Acceso

Luego de obtener información del objetivo y los servicios o vulnerabilidades disponibles, se intenta usar las vulnerabilidades encontradas para forzar el acceso a los objetivos descubiertos. Este acceso puede realizarse siguiendo los siguientes lineamientos: Pasivo, Activo no invasivo, Activo invasivo.



Pasivo

Este intento de acceso es el que requiere menos esfuerzo y tiene como objetivo establecer si es posible explotar las vulnerabilidades encontradas sin llegar a concretar un acceso más allá de los objetivos establecidos.

Activo no invasivo

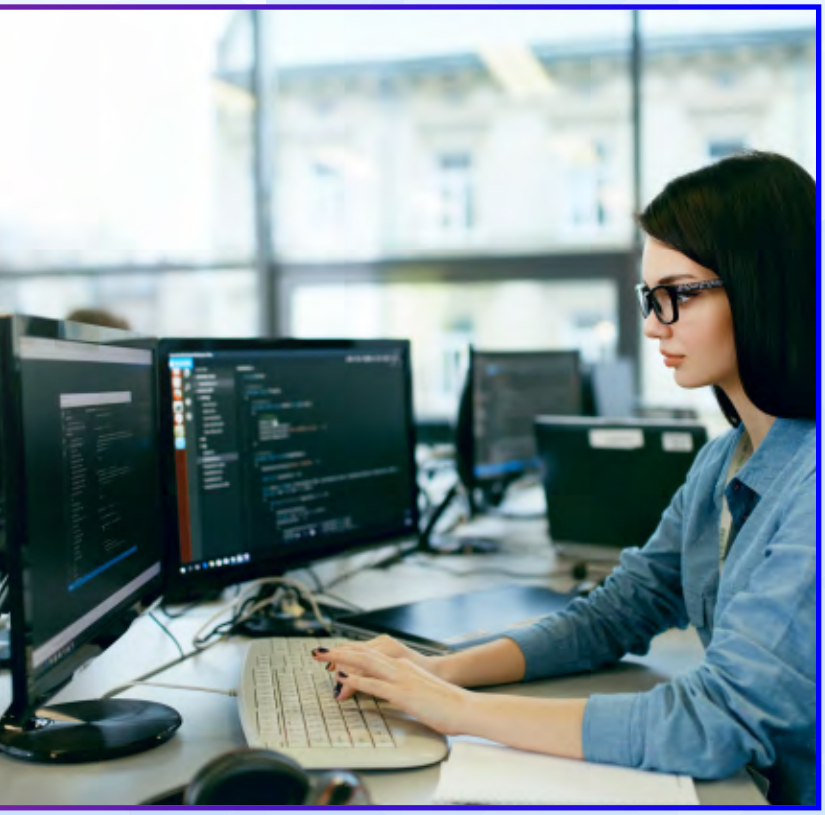
En esta metodología se intenta explotar las vulnerabilidades presentes en los sistemas llegando a ingresar a los objetivos y mantener cierto nivel de acceso que permita acceder a otros niveles de la infraestructura vulnerada.

Activo invasivo

La tercera opción es explotar las vulnerabilidades de tal forma de encontrar formas de obtener información sensible y control de sistemas que permitan establecer los límites a los que podrían llegar intentos de hackeo maliciosos.

5. Reporte

La etapa final del proceso se refiere a documentar los descubrimientos obtenidos en cada etapa del proceso de tal forma que el cliente pueda usar la información para revisar sus procedimientos y sistemas de seguridad presentes. El reporte incluye también recomendaciones de acuerdo a las vulnerabilidades encontradas, de tal forma que el cliente pueda tomar medidas de mitigación adecuadas que eviten que las vulnerabilidades sean explotadas.



6. Scan Final

Luego de que el cliente aplique las recomendaciones y resuelva los problemas expuestos, se realiza un nuevo escaneo de vulnerabilidades para determinar si las acciones tuvieron el efecto deseado para evitar posibles ataques. Este escaneo se realiza apuntando específicamente a los problemas encontrados y no buscando nuevas posibilidades de acceso.

Comparativo

Item	Scan	Acceso			Informe	Scan Final
	Reconocimiento		Pasivo	Activo no invasivo	Activo invasivo		
Hacking Ético Pasivo	✓	✓	✓			✓	✓
Hacking Ético Activo No Invasivo	✓	✓		✓		✓	✓
Hacking Ético Activo Invasivo	✓	✓			✓	✓	✓

CONTÁCTENOS

Para más información 228401000 - División Internet

30 AÑOS | Generando soluciones TI integrales para su empresa