Universidad del Valle de Guatemala
Departamento de Ciencias de la Computación
Ingeniería de Software 2
Carlos Alburez- 231311

Tarea 6: Identificación y corrección de vulnerabilidades comunes

Chapter 5: The Robin Hood Hacker

Descripción del caso:

El capítulo 5, denominado “Robin Hood Hacker” cuenta el caso de un intruso que solía ingresar y penetrar sistemas y sitios corporativos y gubernamentales con el propósito de exponer las fallas de seguridad. Siendo raro, ya que por lo general los hackers tradicionales tienen el propósito de buscar dinero o malicia, pero él lo que hacía era infiltrarse en redes, documentaba meticulosamente las vulnerabilidades que explotaba y luego él mismo enviaba reportes detallados explicando exactamente cómo había logrado dicho acceso. Su modus operandi incluía reconocimiento exhaustivo de los sistemas objetivo, explotación de configuraciones débiles, y uso de ingeniería social. Además, combinaba OSINT con malas configuraciones internas de las compañías, aprovechando que muchas compañías dejaban servidores de prueba, contraseñas por defecto o accesos internos mal resguardados.

Uno de los casos más sonados fue contra el New York Times, logrando acceder a la intranet interna del periódico, donde encontró no solo correos de empleados sino también información personal de más de 3,000 colaboradores externos, incluyendo números de seguridad social. Así mismo, también irrumpió en los sistemas de MCI/WorldCom y en Microsoft. Específicamente en el caso de Microsoft, según el relato del libro, logró entrar a servidores internos y ver partes del código fuente de sus productos. Y en todos los casos, después de lograr acceso, avisaba a la empresa para que corrigiera los fallos.

Vulnerabilidad principal identificada:

La vulnerabilidad principal siento que es organizacional en lugar de ser técnica, ya que hubo gestiones inadecuadas de la seguridad y falta de auditorías proactivas de seguridad. Las organizaciones víctimas tenían configuraciones por defecto sin cambiar, políticas de contraseñas débiles, falta de monitoreo de logs y ausencia de evaluaciones regulares de vulnerabilidades. Además de servicios internos accesibles desde internet y falta de segmentación de redes.

Propuesta de solución:

- Desactivar servicios innecesarios, aplicar actualizaciones de software de manera sistemática y establecer contraseñas fuertes y no reutilizables

- Separa la red interna de la externa mediante firewalls, definir roles y permisos mínimos necesarios para cada usuario (principio de mínimo privilegio)
- Instalar IDS/IPS para detectar patrones de tráfico sospechoso y analizar logs de acceso en tiempo real
- Realizar evaluaciones periódicas por parte de consultores certificados para identificar vulnerabilidades antes que los atacantes.