Universidad del valle de Guatemala

Erick Guerra

Tarea 6. Desarrollo Seguro Parte 1

Capítulo 4: “Cops and Robbers”

Descripción:

Listo, big papi. Dos estudiantes hacían wardialing hasta toparse con un módem del U.S. District Court que aceptaba el acceso con las credenciales por defecto “public/public”. De apoyo fueron encadenando accesos, primero al entorno del tribunal y luego, aprovechando confianza entre sistemas y contraseñas débiles, pivotaron hacia la red de Boeing. Ya dentro, ejecutaron herramientas de cracking de contraseñas, ganaron más privilegios y se movieron lateralmente por cientos de equipos, llegando incluso a un Cray usado en colaboración con NASA. En paralelo, ocultaban directorios y actividad para persistir sin levantar sospechas.

Vulnerabilidad explotada:

Creo que fue una combinación de autenticación débil por cuentas “public/public” y contraseñas triviales, exposición de módems dial-up accesibles desde la PSTN, y confianza/segmentación deficiente que permitió encadenar saltos desde el tribunal hacia el perímetro de Boeing y, de ahí, a otros sistemas internos y externos, ya dentro, ejecutaron Crack y ocultaron directorios para persistencia.

Propuestas de solución:

- Identificar vulnerabilidades explotadas en sistemas informáticos a partir de casos reales.
- Eliminar cuentas por defecto y política de contraseñas en todo acceso remoto para retirar o aislar módems.
- Detección de ejecutables como Crack, carpetas ocultas y uso inusual de CPU logging centralizado y alertas.