Consolidación y utilización de sistemas comprometidos (Hacking ético)

Administración de sistemas de manera remota

Una operación de administración remota puede ser cualquier tarea que se realice en un sistema operativo como por ejemplo agregar y eliminar software, actualizar el sistema operativo, controlar procesos y servicios, crear tareas programadas, control de usuarios, encender y apagar equipos, etc.

Se puede administrar de manera remota mediante terminales en modo texto y también gráficas, el acceso remoto consiste en la comunicación entre servidor y clientes, al servidor se conectan los clientes. Para conectar un cliente con un servidor lo único que necesita es conocer el puerto y el nombre del equipo o la dirección IP. El acceso de los cliente se hace utilizando usuarios por lo tanto es necesario que el usuario tenga permiso para acceder al servidor.

Ataques y auditorías de contraseñas

Mediante una serie de pruebas se comprueba la fortaleza del sistema de contraseñas que se utilizan en los equipos de la red.

Más información

- https://www.jesusninoc.com/contrasenas-seguras-con-power

shell/

Pivotaje en la red

Consiste en realizar conexiones dentro de la red, de esa forma desde un equipo se puede acceder a cualquier otro de la red.

Instalación de puertas traseras con troyanos (RAT, Remote Access Trojan)

Una puerta trasera es una secuencia especial o un término trasero dentro del código de programación o script, mediante la cual se pueden evitar los sistemas de seguridad del algoritmo para acceder al sistema.