Comptia Security A+ parte 4

wp2 = se basa en el estandar de cifrado avanzado AES

Tarjeta SIM = son las siglas de modulo de identidad del abonado

es un circuito integrado que almacena la identidad del abonado

su numero IMSI

La clonacion de SIM , permite que dos telefonos

utilizen el mismo servicio

Ataques a Bluetooth

Bluejacking = consiste en enviar mensajes no solicitados

a dispositivos con bluetooth, debemos configurar

la clave de emparejamiento que suele ser 0000 o 1234

Bluesnarfing= se trata de un acceso no autorizado a la informacion

Navegacion por los buscadores

navegar por sitios seguros https:// esto garantiza que se ha creado
un tunel TLS entre el telefono y el servidor
TLS = Transport Layer Security pondra una capa
de cifrado y un tunel entre tu dispositivo y el servidor
evitando asi los ataques man-in-the-middle
Las mejores formas de proteger tu dispositivo movil

1-actualiza a la ultima version
2-instala un antivirus y antimalware
3-solo instalar app de las tiendas oficiales appStore , GooglePlay
4-descativar las funciones innecesarias
5-activar la encryptacion para voz y datos
6-utilizar contraseñas seguras y datos biometricos
para el inicio de sesion huellas dactilares , escaneres faciales

7-habilitar buscar mi telefono
8-habilitar el bloqueo remoto
9-habilutar las funciones de borrado remoto

Hardeling

El endurecimiento es un acto de configurar un sistema
de forma segura , actualizandolo, creando politicas y reglas
para gobernarlo y eliminado aplicaciones y servicios innecesarios
Cada app que se instala ocupa espacio de disco , posee codigo adicional
Los Administradores ponen en practica
La funcionalidad minima en el proceso de configurar
que solo proporcione app y servicios esenciales
Para crear un entorno de minima funcionalidad se

deben restringir las app, servicios , puertos y protocolos
innecesarios .
Podemos al panel de control -programas y vemos los que
estan instalados
Debemos crear una imagen del sistema segura para
todas las estaciones de trabajo
Restriccion de aplicaciones : solo las app que estan en la lista
de aprobadas pueden descargarse y ejecutarse para
las demas se bloquea atraves de Microsoft Active Directory
ejemplo: servicios - msc -windows update-stop -disable y
este servicio no funcionara
podemos hacerlo en el cmd :
sc stop wuauserv
otra forma

net stop wuauserv

Parche: Es una pieza de softaware diseñada para solucionar
un problema del sistema operativo o app

podemos ver el estado en Microsoft Baseline Security Analizer
o MBSA

Politicas de Grupos : conjunto de reclas o politicas que
que se aplican a un conjunto de usuarios o cuentas dentro de un
sistema operativo para acceder en el cmd :
gpedit

simbolo del sistema :
gpedit
windows settings
security settings
application control policies
appLocker
executable rules

click con el boton derecho para crear las reglas
podemos allow -permitir o deny -denegar
hacemos deny
everyone
path
browser folders(buscamos el archivo)
vamos hacer que nadie pueda ejecutar ningun archivo
windows
temp (lo selecciono)
esto es que cualquier cosa que se intente ser ejecutada
desde el directorio temporal no se permitira
dado que muchos malware intentan salir de la carpeta Temp

Windows utiliza sistema de archivos NTFS:sistema de
archvios de nueva tecnologia , es el forma prederterminado

es mas seguro que /FAT32

desde el cmd podemos covertirlo al FAT32 A NTFS

cmd :

/FS:NTFS + ENTER

Otra cosa que debemos hacer es hacer la desfragmentacion de la unidad de disco periodicamente y hacer una copia de seguridad de los datos

entender como restaurar el sistema desde una copia de seguridad