COOKIES

Las cookies son archivos de texto que se colocan
en el ordenador de un cliente para almacenar informacion
sobre los habitos de navegacion de usuario
Se utilizan para la autentificacion , seguimiento de sesiones
carritos de compras se deben bloquear el
almacenamiento de cookies
cookies de rastreo = suele ser utilizada por
programas espias para recopilar informacion
cookies de sesion = se utilizan para realizar un seguimiento
de los usuarios

---

control de cuentas de usuario

---

mantiene a todos los usuarios ademas
de sus cuenta de admin real en un modo de usuario
estandar de esta forma cuando intentes ejecutar
un programa te va a preguntar si quieres que
se ejecute como adm tendras que poner las
credenciales de admin

Backdoors :: Puerta traseras son codigo colocado
en un programa informatico para eludir
nuestra autentificacion normal
Directorio Transversal::va a explotar app
y servidores web codificados de forma segura
es un metodo para acceder a directorios
no autorizados moviendose atraves de la estructura
de directorios de un servidor remoto
Buffer Overflows ;; desbordamiento del bufer
se produce cuando un proceso de un programa
almacena datos fuera del rango de memoria
asignado , un bufer es un area de almacenamiento
temporal que un programa utiliza para guardar
sus datos
Cross-site scripting : cuando se incrusta un comando
de scripting malicioso en un sitio web
SQL Inyection : inyeccion de una consulta sql atraves
de un formulario de entrada de datos que el cliente
envia a la app web
XML Vulnerabilities :: lenguaje de marcado extensible
lo utilizan la app web para la auenticacion

Firewall : se utilizan para separar y proteger una red de otra hay 3 tipos los basados en software, hardware e integrados o embedded

firewall de software =se ejecutan como una pieza de sofware en un host o servidor

firewall de hardware = son dispositivos independientes que se instalan en la red

firewall : filtran los paquetes y lo acepta o rechaza segun las reglas que se hayan dado , existen dos tipos de filtrados de paquetes sin estado y con estado

sin estado simplemente va aceptar o rechazar paquetes basados en la ip y el numero de puerto solicitado

el filtrado con estado va a realizar un seguimiento de las solicitudes que salen atraves del firewall

filtrado NAT: filtra segun su puerto TCP O UDP

SERVIDOR PROXY: es un dispositivo que actua como intermediario para sus clientes

proxy ip : se utiliza para proteger una red manteniendo el anonimato de las maquinas que se encuentran detras

proxy de Cache = los proxys de almacenamiento

en cache se utilizan para intentar atender las peticiones de los clientes sin conectarse al servidor remoto
PAC = archivo de configuracion automatica de proxy para que el host se conecte al servidor proxy .
PAC = son mejores y se configuran manualmente pueden tener una politica global o GPO
filtro de contenidos de internet: se utilizan en las organizaciones para evitar que los usuarios no accedan a determinadas web
HONEYPOTS Y HONEYNETS: se utilizan para atraer y atrapar posibles atacantes con el fin de contrarrestar intentos de acceso no autorizado
---
CI/CD: integracion continua , entrega continua y despliegue continuo .
integracion continua : metodo de desarrollo de software en el que las actualizaciones de software se prueban y se envian a un servidor de desarrollo o repositorio de codigo
entrega contunia : estamos contantemente tomando

nuestro codigo estamos probando , los requisitos
de la app y la plataforma se prueban y se validan con
frecuencia para su disponibilidad inmediata
despliegue continua: contamos con un modelo de
desarrollo de software en el que las actualizaciones
de las app se envian rapidamente a produccion
mediante la automatizacion.

Puertos : es un punto final logico de comunicacion
entre un ordenador o un servidor
Puerto de entrada ; se utiliza cuando tu pc o servidor
esta en escucha de una conexion
puerto de salida ; lo abre una pc cuando quiere conectarse
a un servidor
puertos del 0 al 1023: puertos bien conocidos
puertos del 1024 al 49151 :son puertos registrados
puertos dinamicos o privados del 49152 al 65535
puerto 21 TCP = protocolo de transferencia de archivos
puerto 22 ssh = para administrar remotamente atraves de
tcp/udp
estan tambien compredidos SFTP Y FTP
puerto 23 telnet = administra remotamente los dispositivos

pero no tiene seguridad debemos desactivarlo de la red
utiliza tcp/udp
puerto 25 smtp = de simple transferencia de correo
se utiliza para enviar correos electronicos atraves de internet
puerto 53 dns = servicio de nombres de dominio , se utiliza para resolver nombres de host , ip en nombres de host
puerto 69 tftp = version simplificada de ftp para poner un archivo en un host remoto y obtener ese archivo
puerto 80 http = protocolo de transferencia de hipertexto transmite datos de website para el cliente atraves de una conexion no cifrada
puerto 88 kerberos = se utiliza para la autentificacion en red mediante sistema de tickets dentro de un dominio windows
puerto 110 pop3 = protocolo de oficina de correos para recibir correos
puerto 119 nntp = protocolo de transferencia de noticias en red, transporta articulos de usenet a un cliente
puerto 135 rpc= remote procedure call se utiliza
para localizar puertos dcom para solicitar un servicio

de un programa en otro equipo a traves de la red
puerto 137-138-139 netbios = se utiliza pra realizar consultas de
nombres
puerto 143 imap = protocolo de acceso de mensajes de internet
se utiliza para recibir correo electronico
puerto 161 udp = protocolo de simple gestion de redes
se utiliza para monitorizar remotamente dispositivos
de red mediante conexion udp
puerto 389 ldap = protocolo ligero de acceso a directorios
puerto 443 https :protocolo de hipertexto seguro
atraves de una conexion cifrada ssl/tls por un tunel encriptado
puerto 445 smb = bloque de mensajes de servidor ,
proporciona acceso compartido a archivos
puertos 465/587 : con ssl /tls envio de correo electronico
por un tunel cifrado
puerto 514 syslog = se utiliza para llevar a cabo
el registro de mensajes informaticos para router
y registro de contafuegos