Basque CyberSecurity Centre

nessus cheat sheet

Es una **herramienta de análisis de vulnerabilidades**, con una gran base de usuarios establecida y que se usa para identificar amenazas y poder responder de forma rápida a las mismas.

1. Nessus Instalación y uso

- Instalación
  apt-get install nessus
- Agregar administrador para la aplicación
  nessus-adduser
- Actualizar componentes
  nessus-update-plugins
- Iniciar nessus
  /etc/init.d/nessusd start
- Comprobar el puerto de nessus
  netstat -luntp or # netstat –landtp

2. Nessuscli

- Mostrar ayuda
  nessus –h
- Ejecutar en modo por lotes
  nessus –q
- Enumerar las directivas incluidas en el archivo de configuración .nessus
  nessus --list-policies
- Enumerar los nombres de informe incluidos en el archivo de configuración .nessus
  nessus --list-reports
- Lista de plugins disponibles en el servidor
  nessus –p
- Especificar la directiva que se utilizará cuando se inicie un análisis en la línea de comandos
  nessus --policy-name (nombre de directiva)
- Especificar el formato del informe de salida (html, text, nbe, nessus)
  nessus -T
- Utilizar los destinos de análisis especificados en el archivo en lugar del archivo .nessus predeterminado
  nessus --target-file (nombre del archivo)
- No comprueba si hay certificados SSL
  nessus –x

3. Comandos de Nessus Server

- Solo escuchar la dirección IP especificada
  nessus-service -a (dirección ip)
- Establecer para usar el archivo de configuración del lado del servidor en lugar del archivo de configuración predeterminado
  nessus-service -c (Nombre del archivo de configuración)
- Establecer el modo de servidor en ejecución en segundo plano
  nessus-service -D
- Lista de comandos nessus
  nessus-service -h
- Escucha solo IPV4
  nessus-service --ipv4-only
- Escucha solo IPV6
  nessus-service --ipv6-only
- Configurar la contraseña maestra para el escáner nessus
  nessus-service -K
- Configurar el servidor para que escuche el puerto especificado por el cliente en lugar del puerto predeterminado 1241
  nessus-service -p
- Ejecutar en modo silencioso
  nessus-service -q