Herramientas análisis vulnerabilidades

Roberto Gómez Cárdenas
rogomez@itesm.mx
http://webdia.cem.itesm.mx/dia/ac/rogomez

Lámina 1 Dr. Roberto Gómez Cárdenas

Los escaner de vulnerabilidades

- Es un programa/herramienta que detecta automáticamente vulnerabilidades y/o debilidades ya sea de un host local ó de un host remoto.
- ¿Cómo funcionan?
  - interrogan puertos TCP/IP primordialmente y analizan las respuestas.

Lámina 2 Dr. Roberto Gómez Cárdenas

¿Cuándo se deben usar?

- Monitoreo es un proceso continuo.
- Problemas seguridad pueden presentarse cada vez que los recursos son
  - actualizados,
  - reconfigurados,
  - nuevos recursos son comprados,
  - antiguos recursos son removidos.

Lámina 3 Dr. Roberto Gómez Cárdenas

Límites de las herramientas

- Las herramientas no son un sustituto para:
  - el sentido común.
  - La responsabilidad del usuario, operador o administrador.
- No son un corrector o reparador de los problemas que ha detectado.
  - es el administrador el que debe hacerlo
- No previenen/detectan ataques de ingenieria social

Lámina 4 Dr. Roberto Gómez Cárdenas

¿Qué información aporta un scanner?

- Servicios que ofrece el host
- Que usuarios son dueños de dichos servicios
- Logins anónimos
- Si ciertos servicios de red permiten autentificación anónima.
- Arquitectura de Hardware
- Sistema Operativo
- Versiones de software

Lámina 5 Dr. Roberto Gómez Cárdenas

Importancia de los scanners

- Revelan al administrador posibles vulnerabilidades y/o debilidades de sus sistemas.
  - posible que un atacante tambien la use
- Son herramientas indispensables en la auditoría de sistemas.
- ¿Qué servicios se abren cuando realizo la instalación de un nuevo programa?
  - por ejemplo Web server, NIS, NFS, samba server, hotfix, parche, actualización de versión (NT 4.0 – 2000)?
- Permiten conocer la configuración de un sistema operativo en instalaciones iniciales (por omisión).

Lámina 6 Dr. Roberto Gómez Cárdenas

Algunas herramientas

- nmap
- Nessus
- Saint
- Satan
- Cops
- ISS

Lámina 7 Dr. Roberto Gómez Cárdenas

Nessus

Scanner vulnerabilidades de software libre

Lámina 8 Dr. Roberto Gómez Cárdenas

NESSUS

- Escáner remoto de vulnerabilidades y debilidades de sistemas.
- Escrito por Renaud Deraison (a los 18 años, París),
  - comenta que conoció Linux a los 16 años y desde entonces se ha dedicado a cuestiones de seguridad de sistemas (específicamente hacking).
  - hoy tiene 23 años, deraison@cvs.nessus.org.
- Se puede obtener de
  - http://www.nessus.org
  - http://www.nessus.com

Lámina 9 Dr. Roberto Gómez Cárdenas

Puntos significativos Nessus

- Actualizado
- Incorpora ataques basados en Web
- Gratis
  - distribuido bajo la licencia GNU, Free Software Foundation
- Open Source
  - elimina el riesgo de que ejecute código malicioso.
- Cuenta con su propio lenguaje de programación
  - NASL, Nessus Atack Scripting Language
  - optimizado para pruebas de seguridad
- Fácil instalación y uso

Lámina 10 Dr. Roberto Gómez Cárdenas

Puntos significativos Nessus

- Arquitectura de “Plug-ins”
  - cada plug-in es una prueba de seguridad
- Arquitectura cliente/servidor.
  - Nessus está compuesto por un servidor (nessusd) el cual realiza las pruebas y un cliente (nessus) el cual es el entorno gráfico donde se presentan los resultados.
  - Hasta hoy, existen versiones de servidor para Unix, y clientes tanto Unix com Win32.
- Puede probar varios hosts a la vez, depende de la fortaleza del equipo donde se ejecuta el demonio y la velocidad de la red.

Lámina 11 Dr. Roberto Gómez Cárdenas

Puntos significativos Nessus

- Reconocimiento inteligente de servicios
  - Smart service recognition
  - no se da por hecho que el target-host sigue la norma de puertos IANA (Internet Assigned Number Authority).
  - Nessus identificará un ftp-server en el puerto XXXX, o un web-server en el puerto YYYY.
  - *“Never trust the version number, never trust that a given service is listenning on the good port”*
- Genera reportes en diferentes formatos de salida

Lámina 12 Dr. Roberto Gómez Cárdenas

Plugins de Nessus

Más de 900 plug-ins en la base de datos.

http://cgi.nessus.org/plugins/

- Backdoors
- CGI abuses
- Denial of Service
- Finger abuses
- Firewalls
- FTP
- Gain a shell remotely
- Gain root remotely
- General
- Misc.
- NIS
- Port Scanners
- Remote file access
- RPC
- SMTP problems
- SNMP
- Useless services
- Windows

Lámina 13 Dr. Roberto Gómez Cárdenas

Nessus y NASL

- NASL (Nessus Attack Scripting Language)
- Permite que cualquiera escriba sus propias pruebas de seguridad
- Permite que dichas pruebas sean compartidas sin importar el sistema operativo
- Garantiza que solo se hará la prueba al target-host, a ningún otro

Lámina 14 Dr. Roberto Gómez Cárdenas

Ejemplo NASL

```
#
# Check for ssh
#
if(description)
{
 script_name(english:"Ensure the presence of ssh");
 script_description(english:"This script makes sure that ssh is running");
 script_summary(english:"connects on remote tcp port 22");
 script_category(ACT_GATHER_INFO);
 script_family(english:"Administration toolbox");
 script_copyright(english:"This script was written by Joe U.");
 script_dependencies("find_service.nes");
 exit(0);
}
```

Lámina 15 Dr. Roberto Gómez Cárdenas

Ejemplo NASL

```
#
# First, ssh may run on another port.
# That's why we rely on the plugin
#'find_service'

port = get_kb_item("Services/ssh");
if(!port)port = 22;

}
```

Lámina 16 Dr. Roberto Gómez Cárdenas

Ejemplo NASL

```
#declare that ssh is not installed yet
ok = 0;
if(get_port_state(port))
{
   soc = open_sock_tcp(port);
   if(soc)
   {
        #Check that ssh is not tcpwrapped. And that it's really  SSH
      data = recv(socket:soc, length:200);
      if("SSH" >< data)ok = 1;
   }
   close(soc);
}
```


Ejemplo NASL

```
#
#Only warn the user that SSH is NOT
#installed
#

if(!ok)
{
  report = "SSH is not running on this host !";
  security_warning(port:22, data:report);
```

Usando Nessus

- Instalarlo
- Crear cuenta nessusd
- Configurar demonio
- Actualizar plugins
- Activar servidor
- Lanzar cliente
- Configurar scaneo
- Verificar resultados

Lámina 19 Dr. Roberto Gómez Cárdenas

1er. paso: instalación

- Requisitos:
  - GTK (gimp toolkit) ftp://ftp.gimp.org/pub/gtk
  - nmap http://www.insecure.org/nmap
- La forma más fácil y menos peligrosa
  - Nessus está disponible como un paquete de autoinstalación.
  - Para usarlo se baja el escript nessus-installer.sh bajo el directorios nessus-installer/ y se teclea el siguiente comando

    #sh nessus-installer.sh

  - No se necesita ningún otro paquete que el instalador

Lámina 20 Dr. Roberto Gómez Cárdenas

Otra forma de instalación

- La forma más común
  - Bajar y compilar los siguientes paquetes en el órden indicado (./configure, make, make install).

nessus-libraries-x.x.tar.gz
libnasl-x.x.tar.gz
nessus-core.x.x.tar.gz
nessus-plugins.x.x.tar.gz

Lámina 21 Dr. Roberto Gómez Cárdenas

2do. paso: crear cuenta

- El servidor nessusd tiene propia base de datos de usuarios, donde cada usuario cuenta con un conjunto de restricciones
- Lo anterior permite compartir un servidor nessusd para toda una red con diferentes administradores que probaran su parte de la red
- Se puede usar la utilería *nessus-adduser* para crear una nueva cuenta

Lámina 22 Dr. Roberto Gómez Cárdenas

Ejemplo uso nessus-adduser

```
toto@maquina:34> nessus-adduser
        Addition of a new nessusd user
        ------------------------------
        Login : renaud
        Password : secret
        Authentification type (cipher or plaintext) [cipher] : cipher
        Now enter the rules for this user, and hit ctrl-D once you are done :
        (the user can have an empty rule set)
        ^D
        Login          : renaud
        Pssword        : secret
        Authentification : cipher
        Rules          :

        Is that ok (y/n) ? [y] y

        user added.
toto@maquina:35>
```

Lámina 23 Dr. Roberto Gómez Cárdenas

Continuando ...

- Tercer paso: configurar el demonio nessus
  - en el archivo /usr/local/etc/nessus/nessusd.conf, se pueden definir diferentes opciones para nessusd
  - se le puede indicar a nessus que use un determinado idioma
  - el archivo configuración estándar tiene inglés como idioma
- Cuarto paso: actualizar los plug-ins (/usr/local/sbin)

```
toto@maquina:35> nessusd -update
```

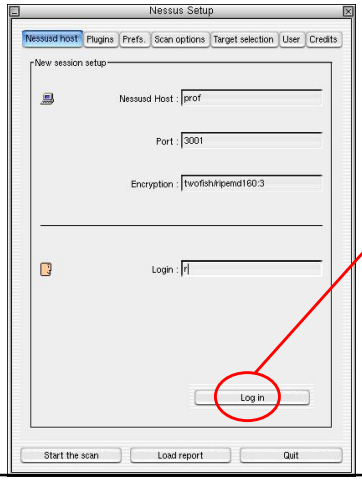
- Quinto paso: arrancar nessusd
  - una vez realizado lo anterior, es posible arrancar el servidor nessusd (se requieren permisos de root):

```
toto@maquina:36> nessusd -D
```

Lámina 24 Dr. Roberto Gómez Cárdenas

Configurando el cliente

- Lo anterior se hizo como root, ahora se conecta como usuario normal y se lanza nessus

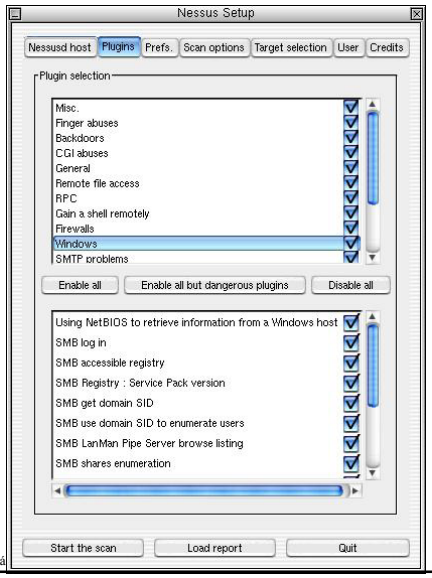


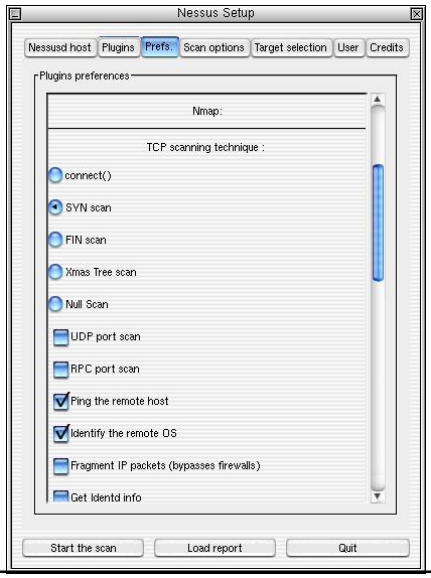
primera vez, por lo que solicita login y password, la próxima vez solo con la llave pública será suficiente

una vez conectado, boton Log in cambia a Log out y aparece etiqueta Connected

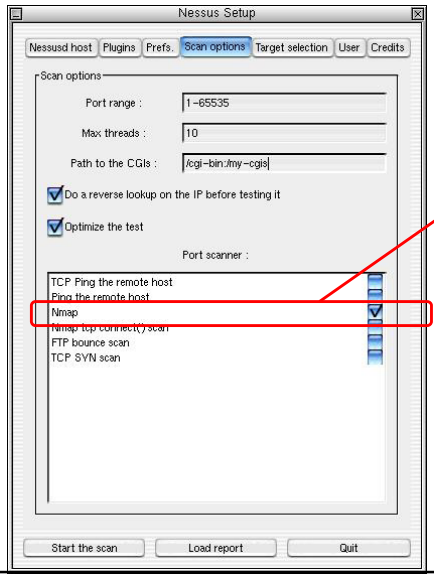
Lámina 25 Dr. Roberto Gómez Cárdenas

Configuración del chequeo a realizar





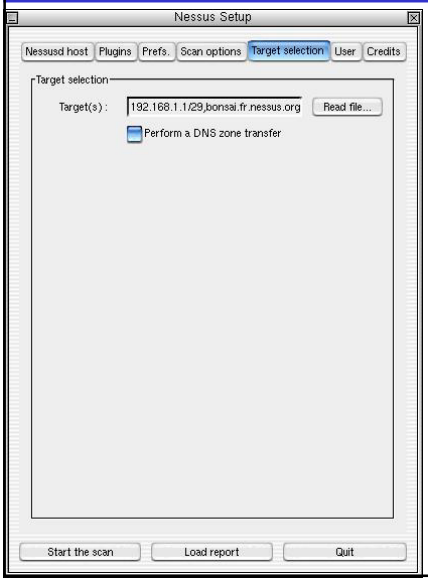
Opciones de scaneo



se elige nmap como herramienta de scaneo de puertos, ya que es rápido

Lámina 27 Dr. Roberto Gómez Cárdenas

Definiendo el objetivo



Posible usar cualquiera siguientes opciones:

192.168.1.1
una sola dirección IP

192.168.1.1-7
un rango de direcciones IP

192.168.2.1-192.168.2.50
otro rango de direcciones IP
Another range of IP addresses.

192.168.1.1/29
otro rango de direcciones IP (not. CIDR)

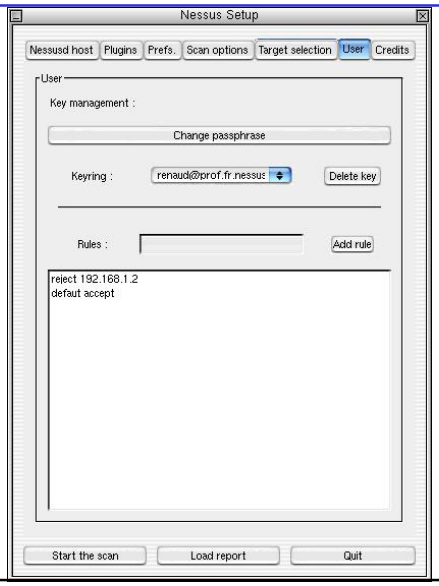
prof.fr.nessus.org
un hostname (Full Qualifie Domain Name).

prof
un hostname (si puede "resolverlo" el servidor)

prof, 192.168.1.1/29, ...
cualquier combinación separada por una coma

Dr. Roberto Gómez Cárdenas

La sección de reglas



Se desea probar 192.168.1.0/29, excepto 192.168.1.2

Lámina 29 Dr. Roberto Gómez Cárdenas

Empieza el scanneo

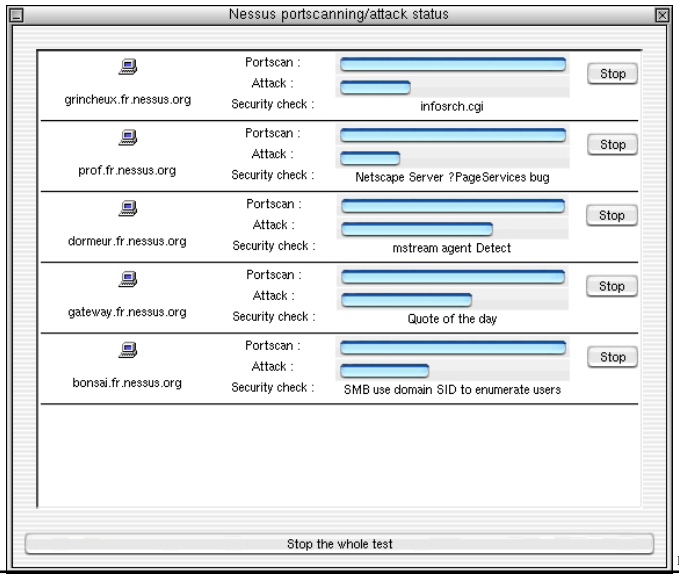


Lámina 30 Roberto Gómez Cárdenas

El reporte otorgado

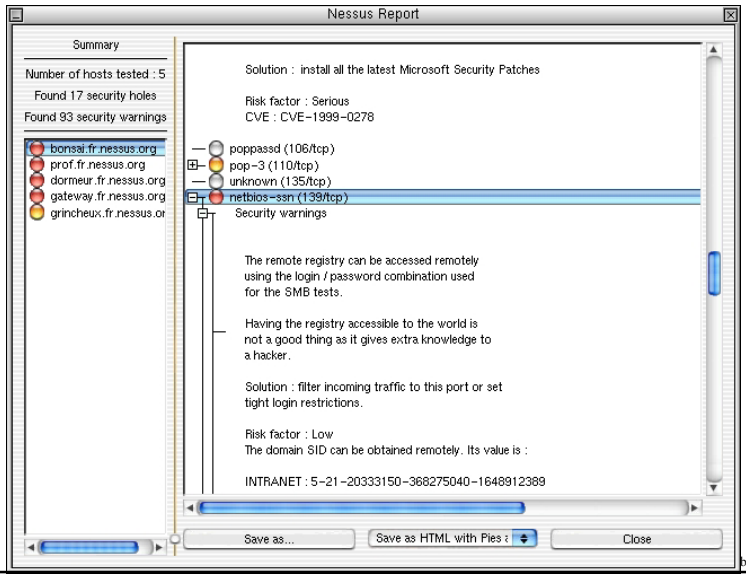


Lámina 31 berto Gómez Cárdenas

Opciones reporte

- Posible obtener reporte en diferentes formatos
  - en formato .NSR, que puede ser leído por el cliente unix y NessusJ
  - en formato spiffy HTML, con gráficas y pasteles
  - en formato HTML
  - en formato texto
  - en formato LaTex

Lámina 32 Dr. Roberto Gómez Cárdenas