

Seguridad

Unidad V – Redes II

APU- UNJu

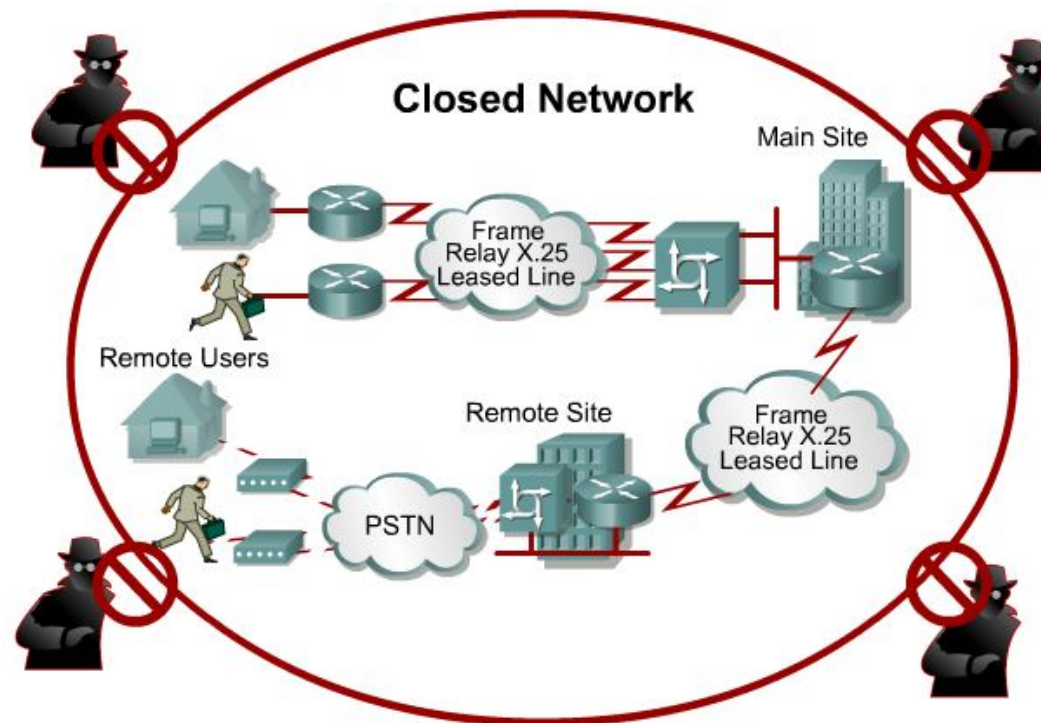
Ing. Consuelo Gómez



Amenazas de Seguridad en Las Redes Modernas

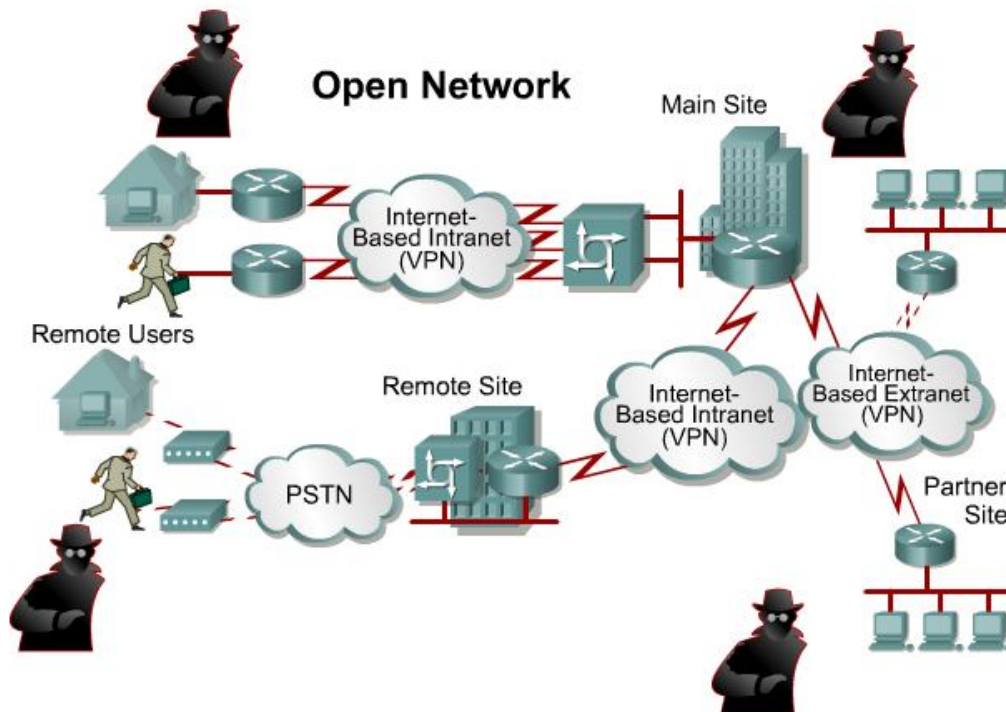
Propósito de la Seguridad

- ¡Para proteger los bienes!
- Históricamente hace a través de la seguridad física y redes cerradas.



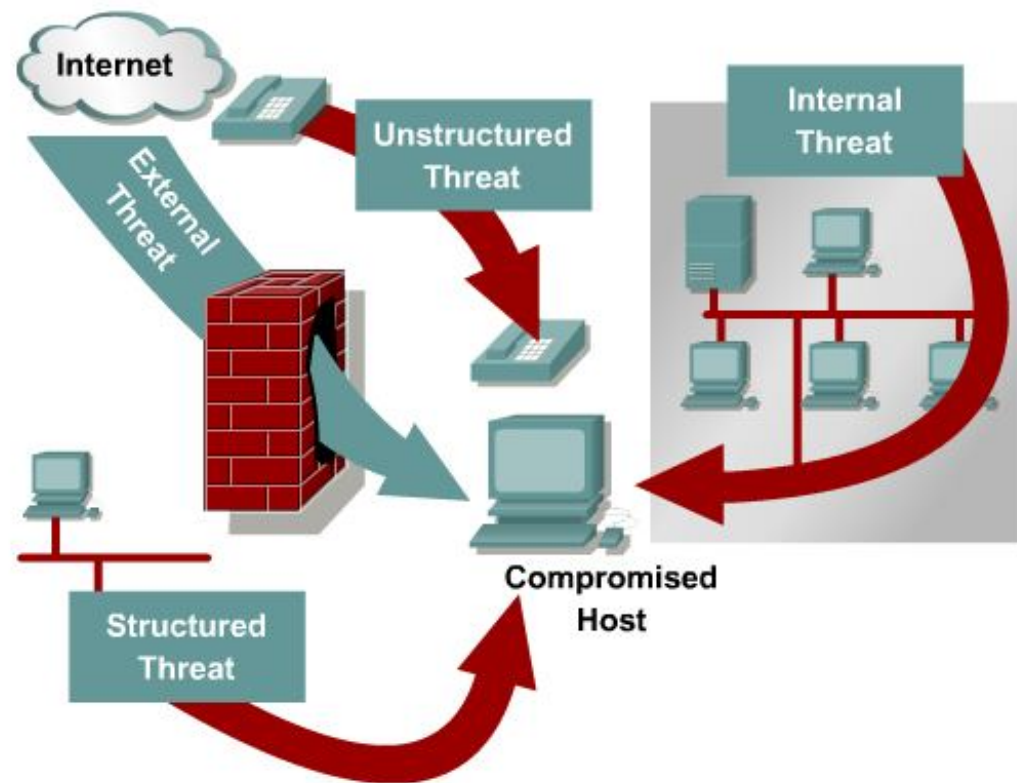
La Red Hoy

- Con el arribo de las computadoras personales, las redes de área local y el mundo totalmente abierto a Internet, las redes de hoy en día están más abiertas. ¡Menos seguras!



Amenazas

- Hay cuatro clases principales de amenazas a la seguridad de la red:
 - Amenazas no estructuradas
 - Amenazas estructuradas
 - Las amenazas externas
 - Las amenazas internas





Restrictive

Open



Closed

Security Policy



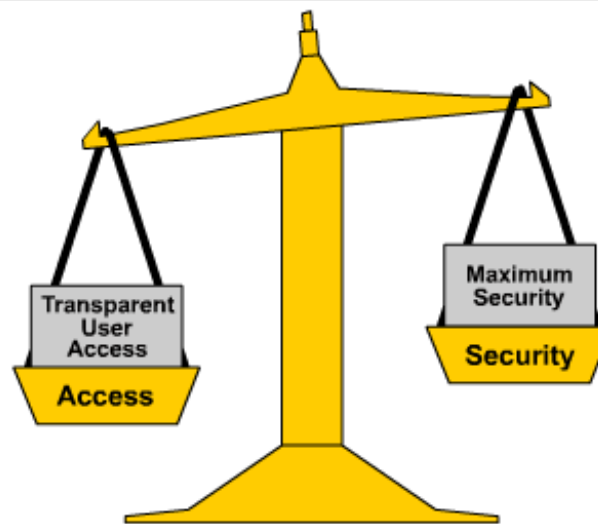
**Enterprise
Network
Security**



**Application
Security**

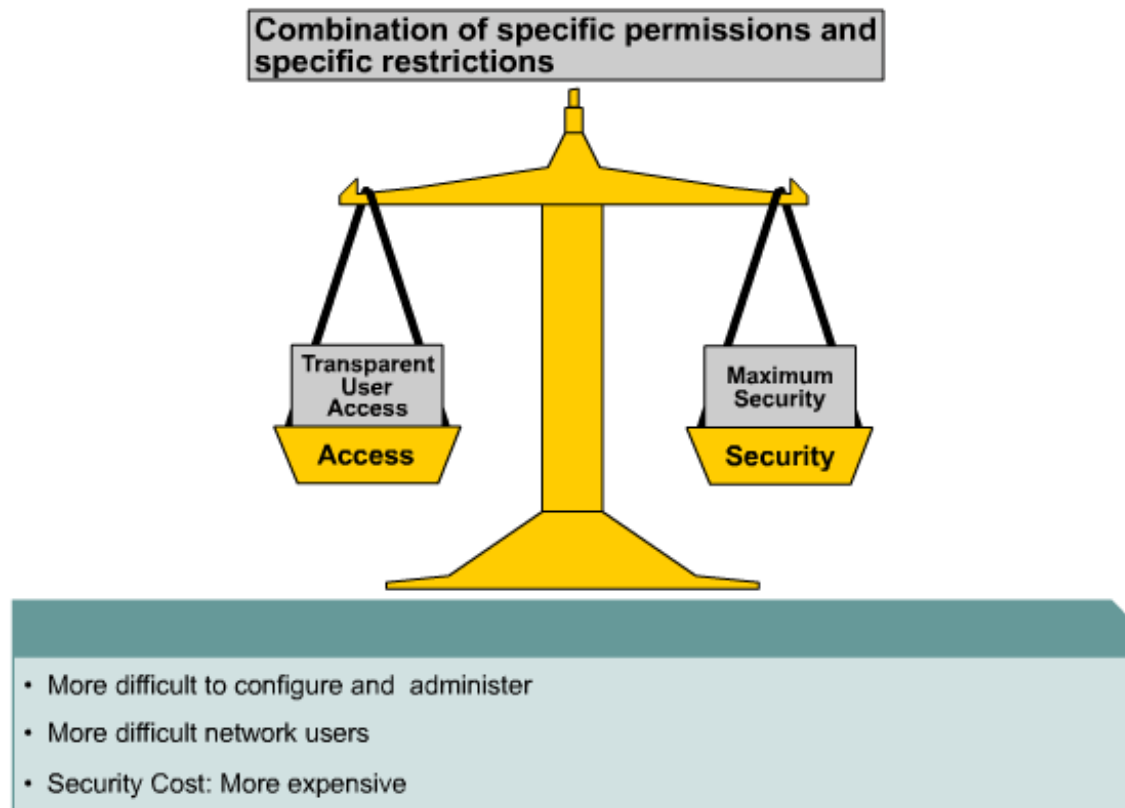
Modelos de seguridad Abierta

Permit everything that is not explicitly denied



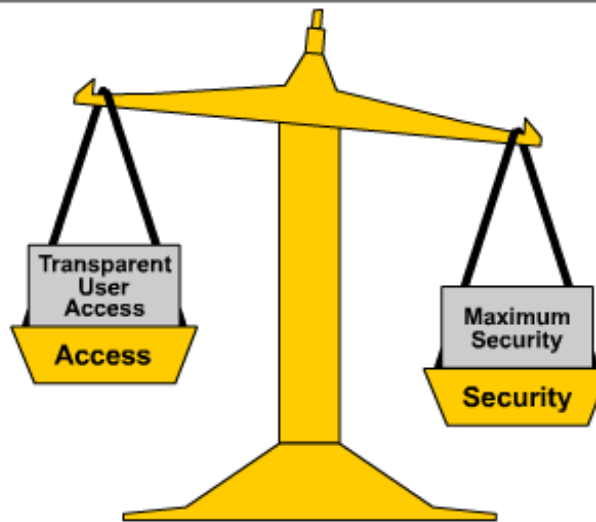
- Easy to configure and administer
- Easy for network users
- Security Costs: Least expensive

Modelo de seguridad Restrictivo



Modelos de seguridad Cerrada

That which is not explicitly permitted is denied



- Most difficult to configure and administer
- Most difficult network users
- Security Cost: Most expensive



Controladores para Seguridad de Redes



Hacker

- La palabra hacker tiene una variedad de significados. Para muchos, esto se relaciona a programadores de Internet que tratan de ganar el acceso no autorizado a dispositivos en el Internet.
- También se utiliza para referirse a las personas que ejecutan programas para prevenir o reducir el acceso de red a un número grande de usuarios, o corromper o borrar datos en los servidores.
- Pero para algunos, el término hacker tiene una interpretación positiva, como un profesional de red que usa sus habilidades de programación sofisticada de Internet para garantizar que las redes no son vulnerables a ataques. Buena o malo, la piratería es una fuerza impulsora en la seguridad de la red.

Tipos de Hackers



- Phreaker

- Un individuo que manipula la red de telefonía con el fin de hacer que se realice una función que normalmente no se permite, como para hacer llamadas de larga distancia.
- Captain Crunch (John Drapper)

- Spammer

- Individuo que envía grandes cantidades de mensajes de correo electrónico no solicitados.
- Los spammers a menudo utilizan los virus para tomar el control de los ordenadores para enviar sus mensajes a granel.

- Phisher

- Un individuo que usa email u otros medios, en un intento de engañar a los demás para que proporcione información confidencial, como números de tarjetas de crédito o contraseñas.





Evolución del Hacking

- 1960s - Phone Freaks (Phreaks)
- 1980s - Wardialing (WarGames)
- 1988 - Internet Worm
- 1993 - First def Con hacking conference held
- 1995 - First 5 year federal prison sentence for hacking
- 1997 - Nmap released
- 1997 - First malicious scripts used by script kiddies
- 2002 - Melissa virus creator gets 20 months in jail

Primicias de seguridad ...



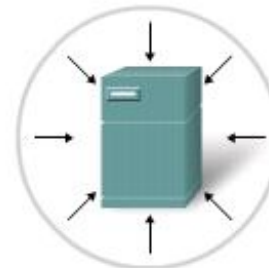
First Virus



First Worm



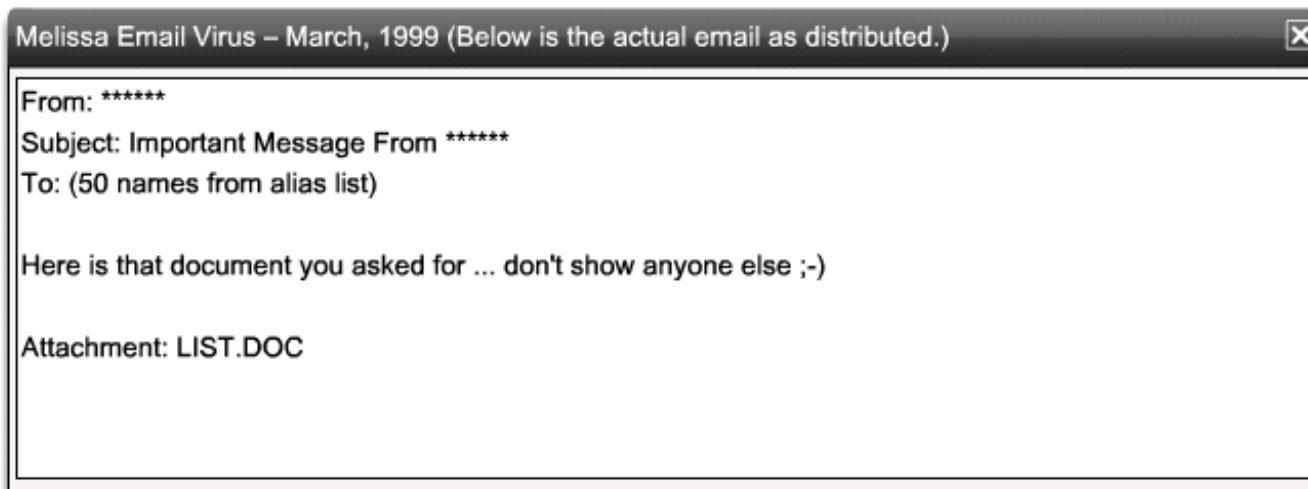
First Spam



First DoS Attack

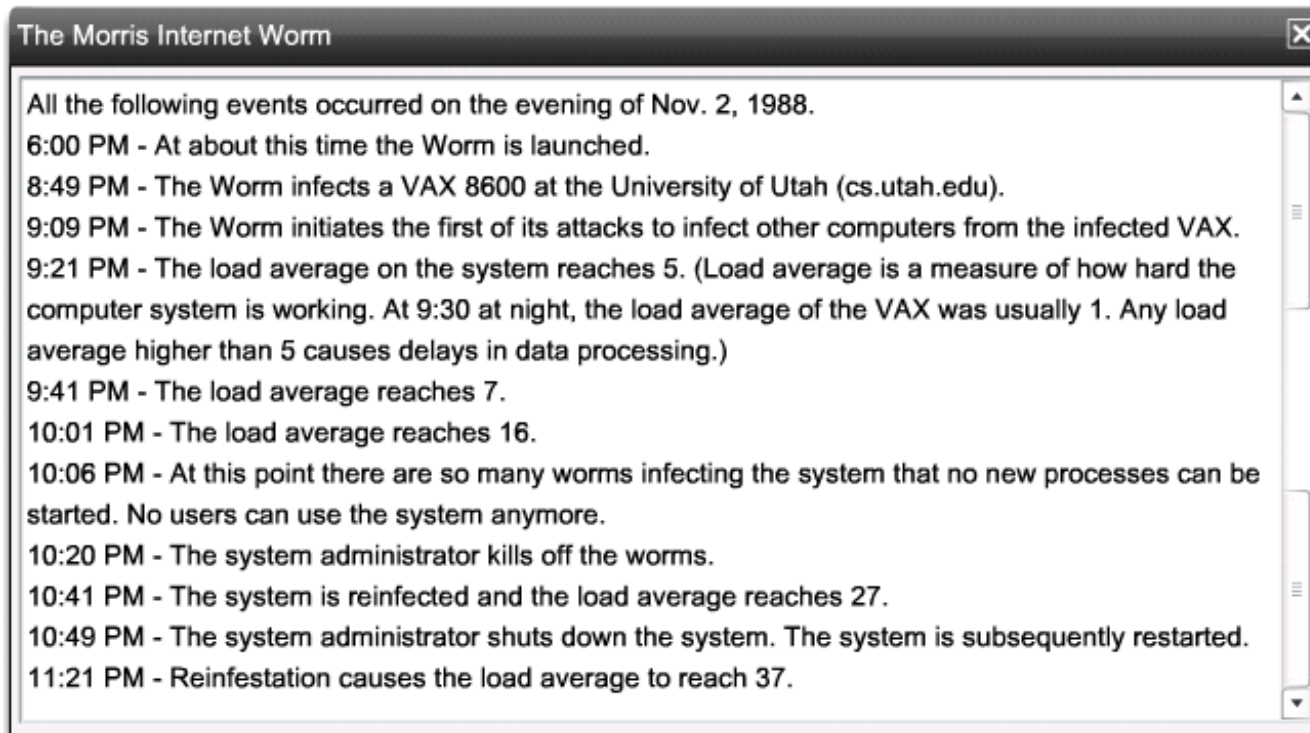
El primer Virus por Email

- El virus Melissa, fue escrito por David Smith y dio lugar a desbordamientos de memoria en los servidores de correo de Internet.
- David Smith fue sentenciado a 20 meses de cárcel en la Prisión Federal y una multa de U.S. \$5.000.

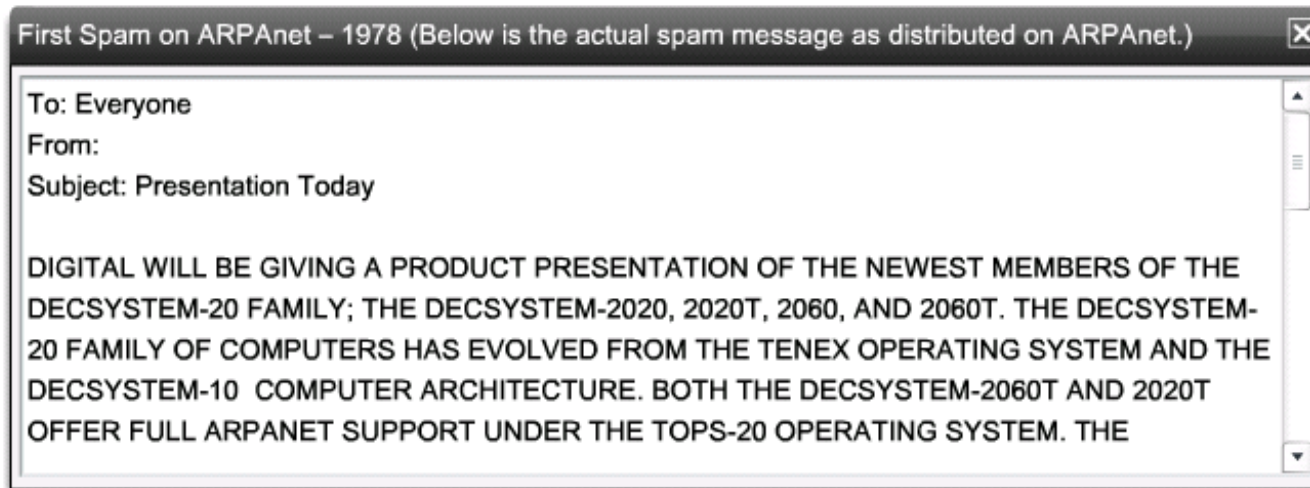


El primer Gusano

- Robert Morris creó el primer gusano de Internet con 99 líneas de código.
 - Cuando el gusano de Morris fue liberado, el 10% de los sistemas de Internet llegaron a un punto muerto.

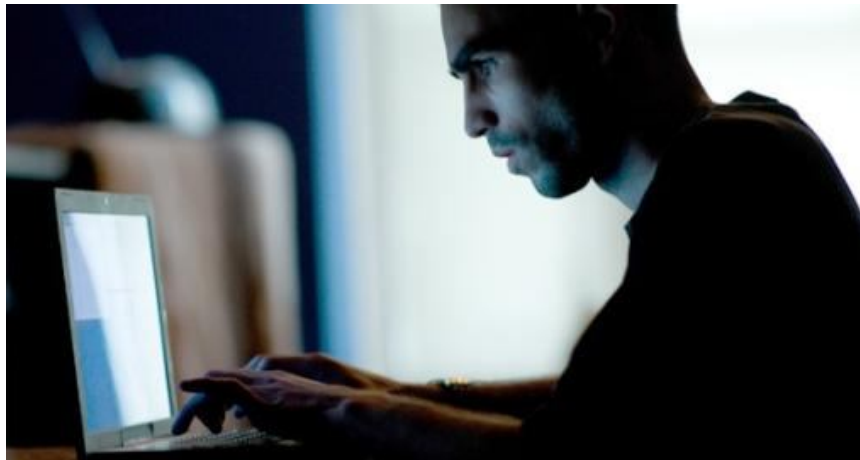


El primer SPAM



Primer Ataque de DoS

- MafiaBoy era el alias de Internet de Michael Calce, de 15 años, estudiante de la escuela secundaria de Montreal, Canadá.
- Lanzó ataques DoS muy publicitados en Feb 2000 hacia Yahoo!, Amazon.com, Dell, Inc., E*TRADE, eBay y CNN.



Tendencias que marcan la Seguridad de la Red

- El aumento de los ataques de red
- El aumento de la sofisticación de los ataques
- La mayor dependencia de la red
- El acceso inalámbrico
- La falta de personal capacitado
- La falta de conciencia
- La falta de políticas de seguridad
- Legislación
- Demandas



Malware / Malicious Code



Tipos de ataques

- Existen cuatro categorías de ataques:
 - Código malicioso: Virus, Gusanos y Caballos de Troya
 - Ataques de Reconocimiento
 - Ataques de Acceso
 - Ataques de Denegación de Servicios.

Let's focus on Malicious Code

Malware

- “Software Malicious” es un software diseñado para infiltrarse en un ordenador sin el consentimiento del propietario.
- Malware incluye:
 - Los virus informáticos
 - Gusanos
 - Caballos de Troya
 - Rootkits
 - Backdoors (método para evitar la autenticación de los procedimientos normales y generalmente se instala usando troyanos o gusanos.)
 - Con fines de lucro (Spyware, botnets, capturadores de teclado y dialers)





Spyware

- Spyware es una categoría estrictamente con fines de lucro de malware diseñado para :
 - Supervisar la navegación web de los usuarios.
 - Mostrar anuncios no solicitados.
 - Redirigir los ingresos de marketing de afiliación al creador del spyware.
- Los programas de spyware se instalan generalmente por los agujeros de seguridad o programas de Caballo de Troya, como la mayoría de los peer-to-peer.

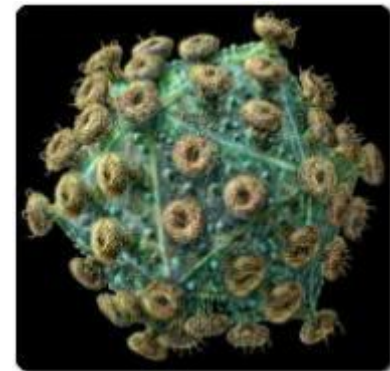


Virus, Caballos de Troya y Gusanos

- Un **virus** es un software malicioso que se adjunta a otro programa para ejecutar una función determinada no deseado en la estación de trabajo del usuario.
- Un **gusano** ejecuta código arbitrario e instala copias de sí mismo en la memoria de la computadora infectada, que infecta a otros hosts.
- Un **Caballo de Troya** es diferente sólo en que toda la aplicación fue escrita para que parezca otra cosa, cuando en realidad se trata de una herramienta de ataque.

Virus

- Un virus informático es un programa informático malicioso (archivo ejecutable), que puede copiarse a sí mismo e infectar un ordenador sin el permiso o conocimiento del usuario.
- Un virus sólo puede propagarse de un ordenador a otro por:
 - Enviarlos a través de una red como un archivo o como una carga de correo electrónico.
 - Llevándolo en un medio removible.
- Los virus necesitan la INTERVENCIÓN DEL USUARIO para propagarse ...



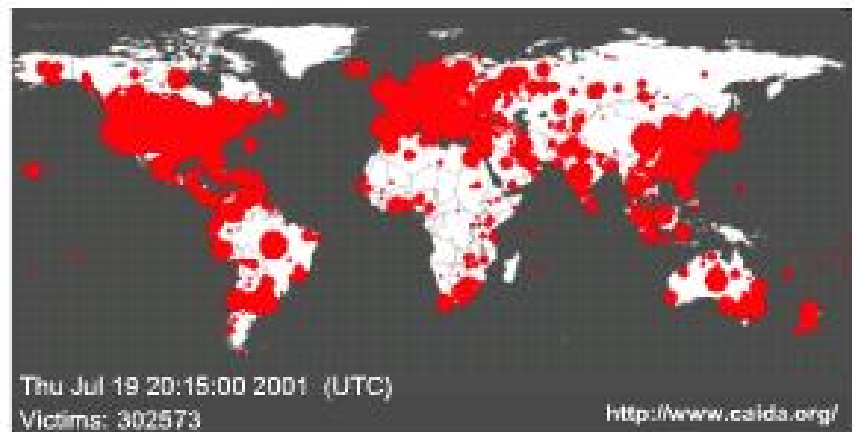
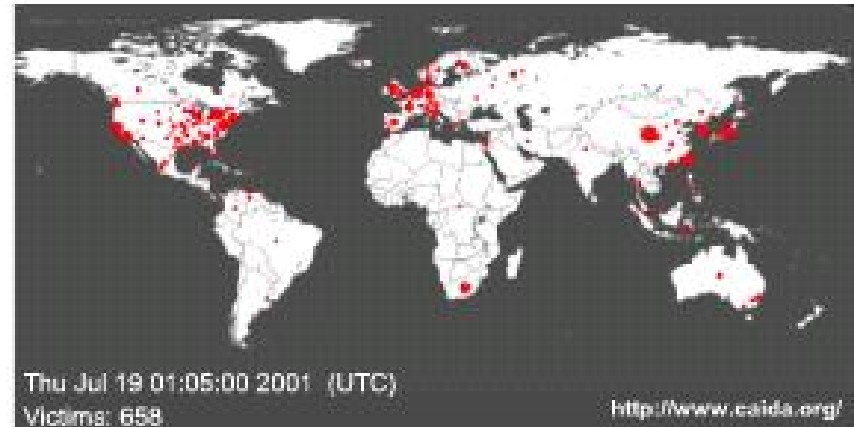


Gusanos

- Los gusanos son un tipo particularmente peligroso de código hostil.
 - Ellos se reproducen de forma independiente explotando de vulnerabilidades de las redes.
 - Los gusanos suelen ralentizar redes.
- Los Gusanos ¡NO NECESITAN LA INTERVENCION DEL USUARIO!
 - Gusanos no requieren la participación del usuario y se pueden propagar extremadamente rápida en la red.

Gusano SQL Slammer

- En Enero de 2001, el Gusano SQL Slammer ralentizo el tráfico global de Internet como resultado de DoS.
- Mas de 250.000 hosts fueron afectados en 30 minutos de su lanzamiento.
- El gusano explota un error de desbordamiento de búfer en SQL Server de Microsoft.
 - Un parche para esta vulnerabilidad fue lanzado a mediados de 2002, por lo que los servidores en los que se vieron afectados fueron aquellos que no tienen el parche de actualización aplicado.





Caballos de Troya



El software de hackeo mas vendido en el año 2009

- *“Kits que tienen por nombres como ‘T-IFramer,’ ‘Liberty Exploit Systems’ y ‘Elenore’ todos aumentaron la venta en mercados clandestinos con una venta entre \$ 300 a \$ 500, según Kandek, permite al atacante instalar un programa troyano listo para descargar, a los deseos de los cibercriminales, desde spyware a software, haciendo simplemente un click. Estos tres kits explotaban 45 bugs únicos de Adobe Reader, junto con un menor número de errores en Internet Explorer, Microsoft Office, Firefox e incluso Quicktime.”*

Articulo completo:

<http://www.cbc.ca/technology/story/2009/12/16/f-forbes-adobe-hacked-software.html>

Caballo de Troya

- Un caballo de Troya es un programa que aparece, para el usuario, para realizar una función deseable pero, de hecho, facilita el acceso no autorizado al sistema informático del usuario..
- Los troyanos pueden parecer programas útiles o interesantes, o por lo menos inofensivo a un usuario desprevenido, pero en realidad son dañinos cuando se ejecutan.
- Los troyanos no se auto-repican esto los distingue de los virus y gusanos.



Clasificación de un Troyano



- Troyano de Acceso Remoto
 - Permite el acceso remoto no autorizado
- Troyano para envío de Datos
 - Proporciona el atacante datos confidenciales.
- Troyano Destructivo
 - Corrompe o borra archivos
- Troyano Proxy
 - El PC del usuario funciona como un servidor proxy.
- Troyano FTP (abre el puerto 21)
 - Deshabilita software de seguridad (detiene los programas antivirus o firewalls en funcionamiento)
- Troyano de Denegación de Servicios (retarda o detiene la actividad de red)

Cómo mitigar Virus y Gusanos?

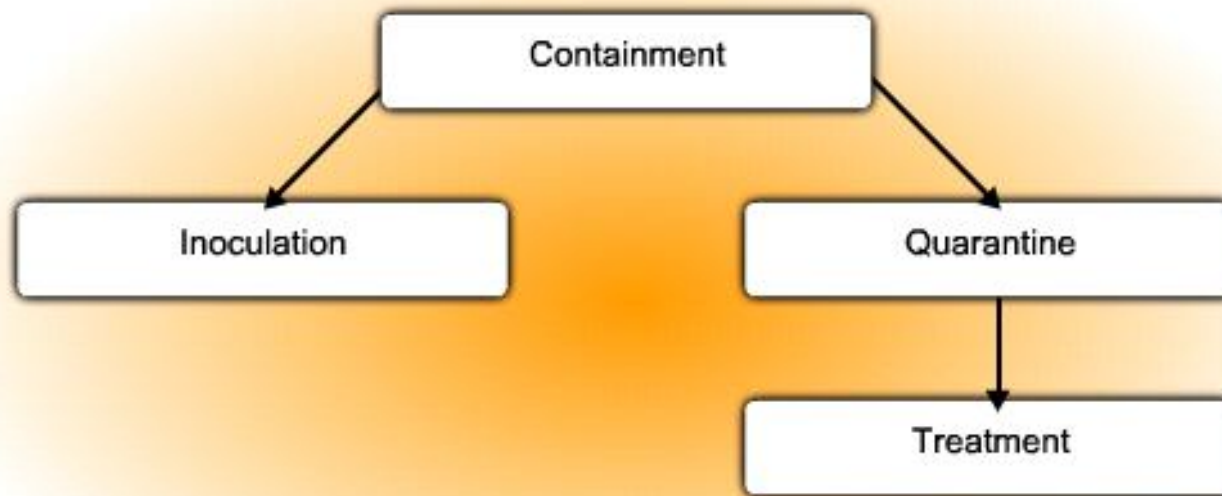


Virus y Troyanos - Mitigación

- El principal medio de mitigar el virus y los ataques de caballo de Troya es un software antivirus.
 - Para una total protección, los sistemas de prevención de intrusos basados en hosts (HIPS), tal como el Cisco Security Agent debe ser implementado.
 - HIPS protege el kernel del SO.
- El Anti-virus ayuda a evitar que los equipos se infecten y difundir código malicioso.
 - De todas formas, el antivirus debe ser usado de forma apropiada.
 - Siempre debe estar actualizado con el .dat mas reciente y las ultimas versiones de las aplicaciones.
 - Considere la posibilidad de que requiere mucho más tiempo para limpiar ordenadores infectados que lo hace para mantener al día el antivirus y las definiciones de antivirus en las máquinas.

Mitigación de una Gusano Activo

- El ataque de mitigación del Gusano requiere diligencia por parte del personal de la administración del sistema y de la red.
- Las cuatro fases para mitigar los ataques de un gusano activo, son:



Mitigación de un Gusano

- Contención:
 - Limitar la propagación de la infección del gusano de las áreas de la red que ya están afectados.
 - Segmentar la red para reducir la velocidad o detener el gusano para evitar que los host infectados afecten a otros sistemas.
 - Use ACL de entrada y salida en los routers y firewalls en los puntos de control dentro de la red.
- Inoculación:
 - Corre paralela a o con posterioridad a la fase de contención.
 - Todos los sistemas infectados están parchadas con el parche del proveedor adecuado para la vulnerabilidad.
 - El proceso de inoculación además priva al gusano de cualquier blanco disponible.

Mitigación de un Gusano

- **Cuarentena:**

- Sigue la pista e identifica las máquinas infectadas dentro de las áreas contenidas las mismas se deben desconectar, bloquear, o eliminar.
- Esto aísla estos sistemas apropiadamente para la fase de tratamiento..

- **Tratamiento:**

- Activamente los sistemas infectados se desinfectan del gusano.
- Terminar el proceso del gusano, eliminar archivos modificados o configuraciones del sistema que el gusano haya introducido y parchear la vulnerabilidad que el gusano utiliza para explotar el sistema.
- En casos más severos, completamente volver a instalar el sistema para asegurarse de que el gusano y sus derivados son eliminados



Ataques de Reconocimiento

Tipos de Ataques

- Los ataques se clasifican en cuatro categorías:
 - Código Malicioso: Virus, Gusanos y Troyanos
 - Ataques de Reconocimiento
 - Ataques de Acceso
 - Ataques de Denegación de Servicios (DoS)

Let's focus on Reconnaissance attacks

Reconocimiento

- Es la recopilación de información mediante el descubrimiento no autorizado y la cartografía de los sistemas, servicios o vulnerabilidades en los mismos.
 - En muchos casos precede a un ataque de DoS.
- Los ataques de Reconocimiento consisten en:
 - Consultas de información de Internet. (**whois**, **nslookup**)
 - Barridos de ping
 - Exploracion de puertos
 - Sniffers de paquetes



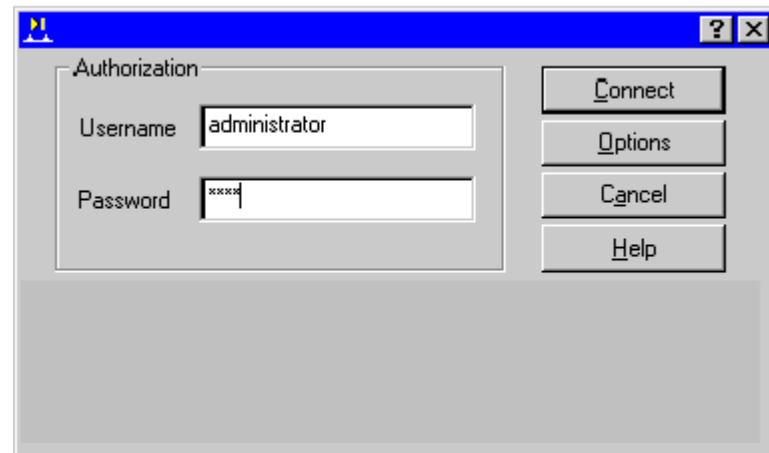
Ataques de Acesso

Ataques de Acceso

- Explotan vulnerabilidades conocidas en los servicios de autenticación, servicios de FTP y servicios web para poder entrar a cuentas web, bases de datos confidenciales y otra información sensible, por estas razones:
 - Recuperar datos
 - Obtener acceso
 - Elevar sus privilegios de acceso
- Técnicas de Ataques de Acceso
 - Ataques de contraseña
 - Explotación de Confianza
 - Redirección de Puertos
 - Man-in-the-middle
 - Desbordamiento de búfer

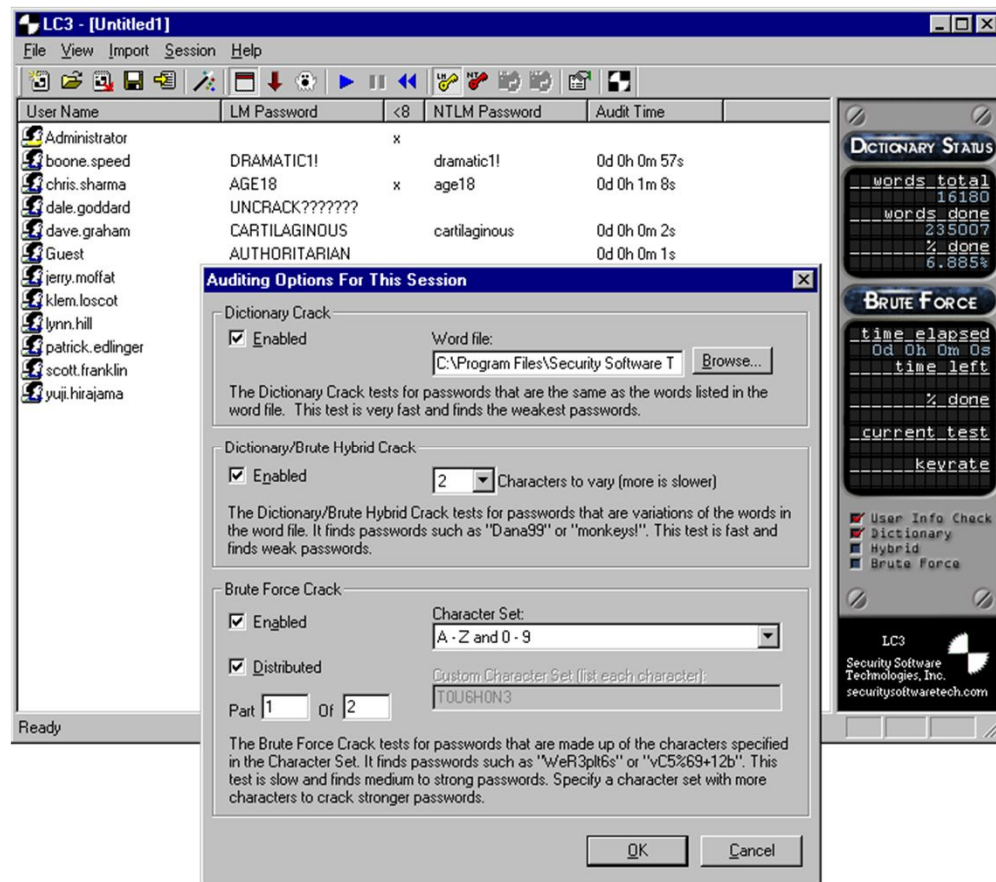
Ataques de Contraseña

- Los hackers ejecutan ataques de contraseña utilizando el siguiente:
 - Ataques de Fuerza Bruta
 - Troyanos
 - Suplantación de IP
 - Sniffers de Paquetes



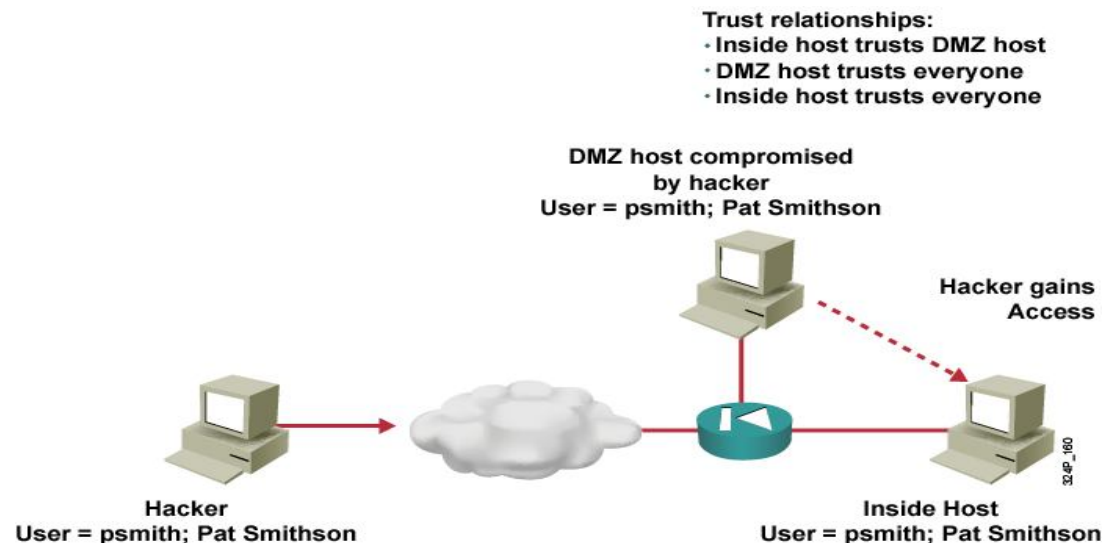
Password Attack Example

- L0phtCrack (“loft-crack”) takes the hashes of passwords and generates the plaintext passwords from them.
- Passwords are compromised using one of two methods:
 - Dictionary cracking
 - Brute-force computation

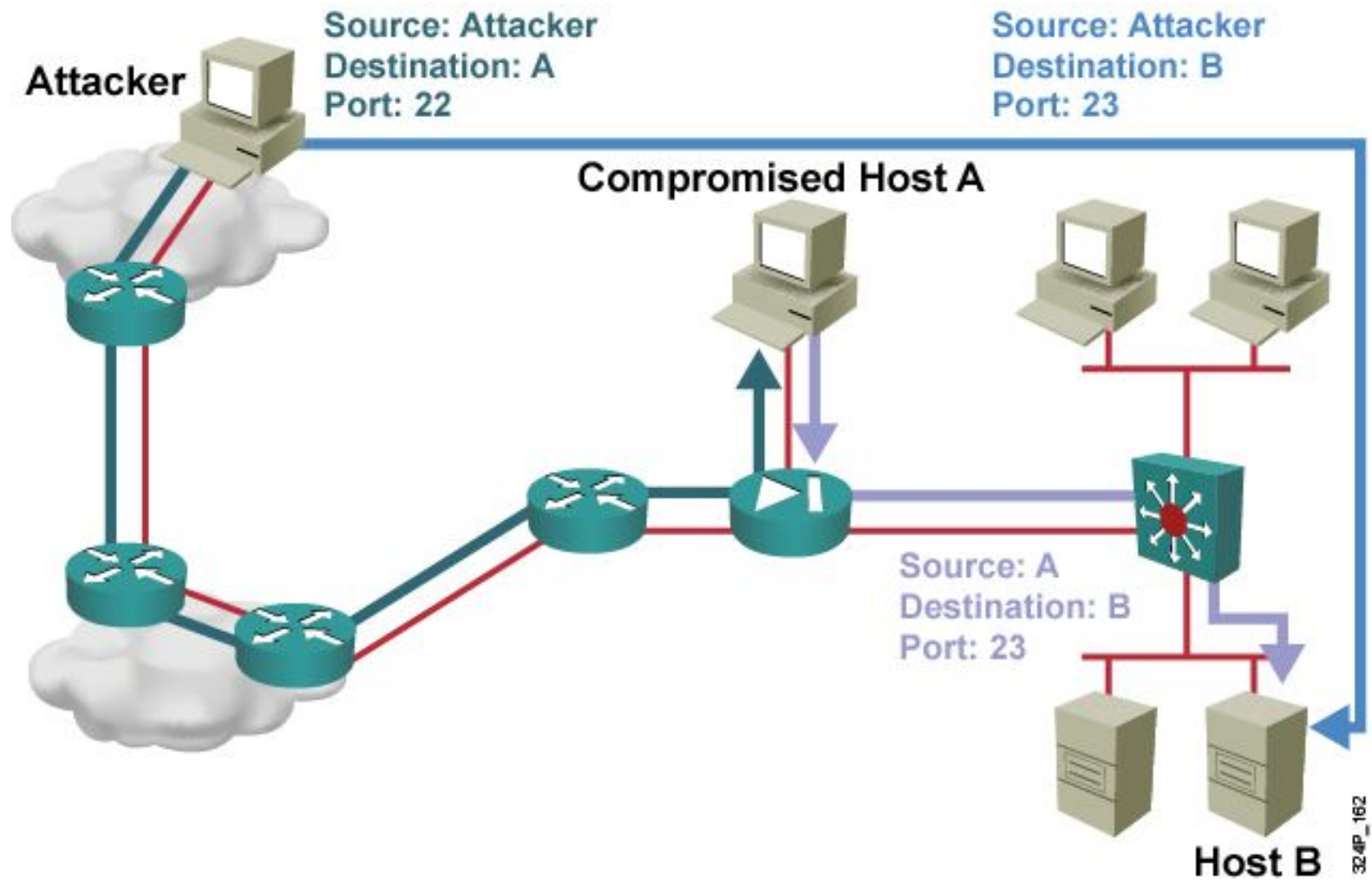


Explotación de Confianza

- Un ejemplo de un ataque de explotación de confianza es cuando una red perimetral está conectada a una red corporativa.
 - Estos segmentos de red suelen contener DNS, SMTP y HTTP.
 - Debido a que estos servidores residen todas en el mismo segmento, un compromiso de un sistema puede llevar al compromiso de otros sistemas si esos otros sistemas también confían en los sistemas que están conectados a la misma red.



Redirección de Puertos



Ataque “Man-in-the-Middle”

- Los propósitos de este ataques son:
 - El robo de información
 - Secuestro de una sesión en curso para obtener acceso a los recursos de la red interna
 - El análisis de tráfico para obtener información sobre la red y los usuarios de la misma
 - DoS
 - La corrupción de los datos transmitidos
 - La introducción de la nueva información en sesiones de red
- Un ejemplo es cuando alguien que trabaja para el ISP, obtiene acceso a todos los paquetes de red y la transferencia entre la red y cualquier otra red.



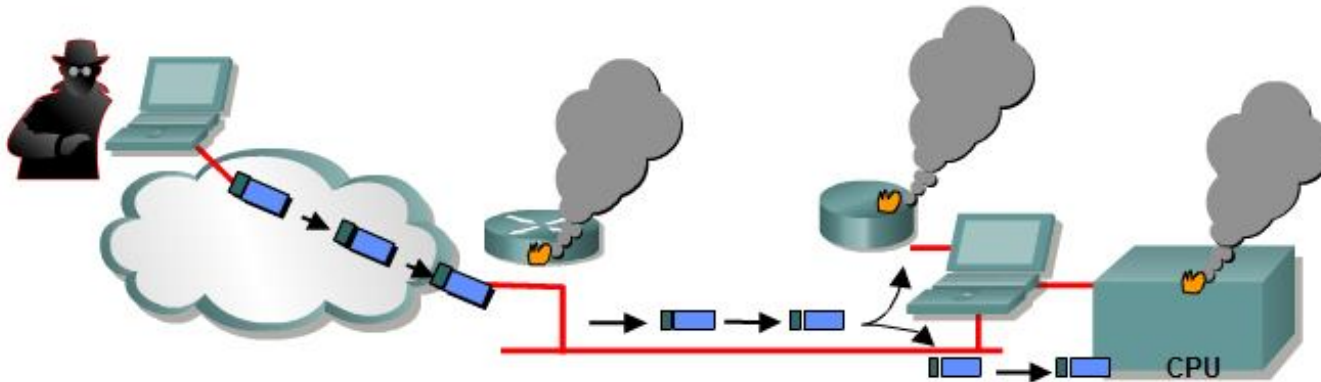
Ataques de DoS

Denial of Service Attack (DoS)

- Tipos de ataques de DoS:
 - Ping de la muerte
 - Ataque Smurf
 - Ataque de Inundación TCP SYN
- Otros incluyen la fragmentación de paquetes y reensamblaje, bombas de E-mail, CPU hogging, Aplicaciones Maliciosas, routers mal configurados, el ataque chargen, ataques out-of-band tales como WinNuke, Land.c, Teardrop.c y Targa.c.

DoS Attacks

DoS attacks prevent authorized people from using a service by using up system resources.



Resource overloads

- Disk space, bandwidth, buffers, and so on.
- Ping floods: smurf, and so on.
- Packet storms: UDP bombs, fraggle, and so on.

Malformed data

- Oversized packets: ping of death, and so on.
- Overlapping packets: winuke, and so on.
- Un-handled data: teardrop, and so on.

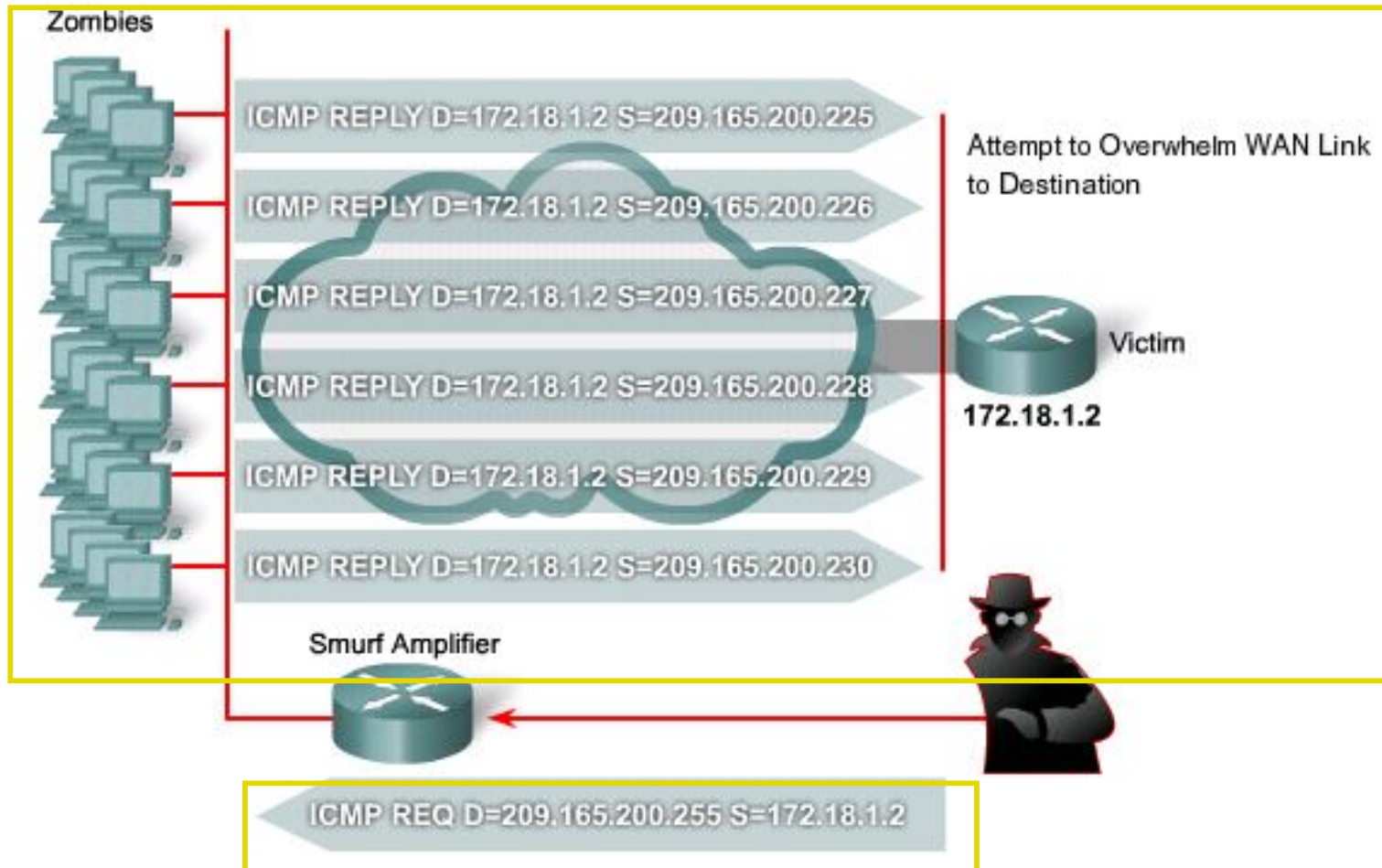


Ping de la Muerte

- Ataque legendario que envía una petición de eco en un paquete IP más grande que el tamaño máximo de paquete de 65.535 bytes.
- Una variante de este ataque es el envío de fragmentos ICMP, que llenan los buffers de reensamblaje del equipo objetivo.

Ataque Smurf

- Este ataque envía un gran número de peticiones ICMP a las direcciones de broadcast, todas ellas con direcciones de origen falsas en el mismo segmento de red.





Ataque de Inundacion TCP SYN

- Este ataque se envían gran cantidad paquetes con una dirección IP origen falsa.
 - Cada paquete se maneja como una solicitud de conexión, haciendo que el servidor genere un medio de apertura (conexión embrionaria) enviando de vuelta un TCP SYN-ACK y esperando una respuesta de paquete de la dirección origen.
 - Sin embargo, debido a que la dirección origen es falso, la respuesta nunca llega.
 - Estas conexiones medio abiertas saturar el número de conexiones disponibles que el servidor es capaz de hacer, evitando responder a las peticiones legítimas.



DDoS

Ejemplo de ataque de DDoS

1. Scan for systems to hack.

Client System

2. Install software to scan, compromise, and infect agents.

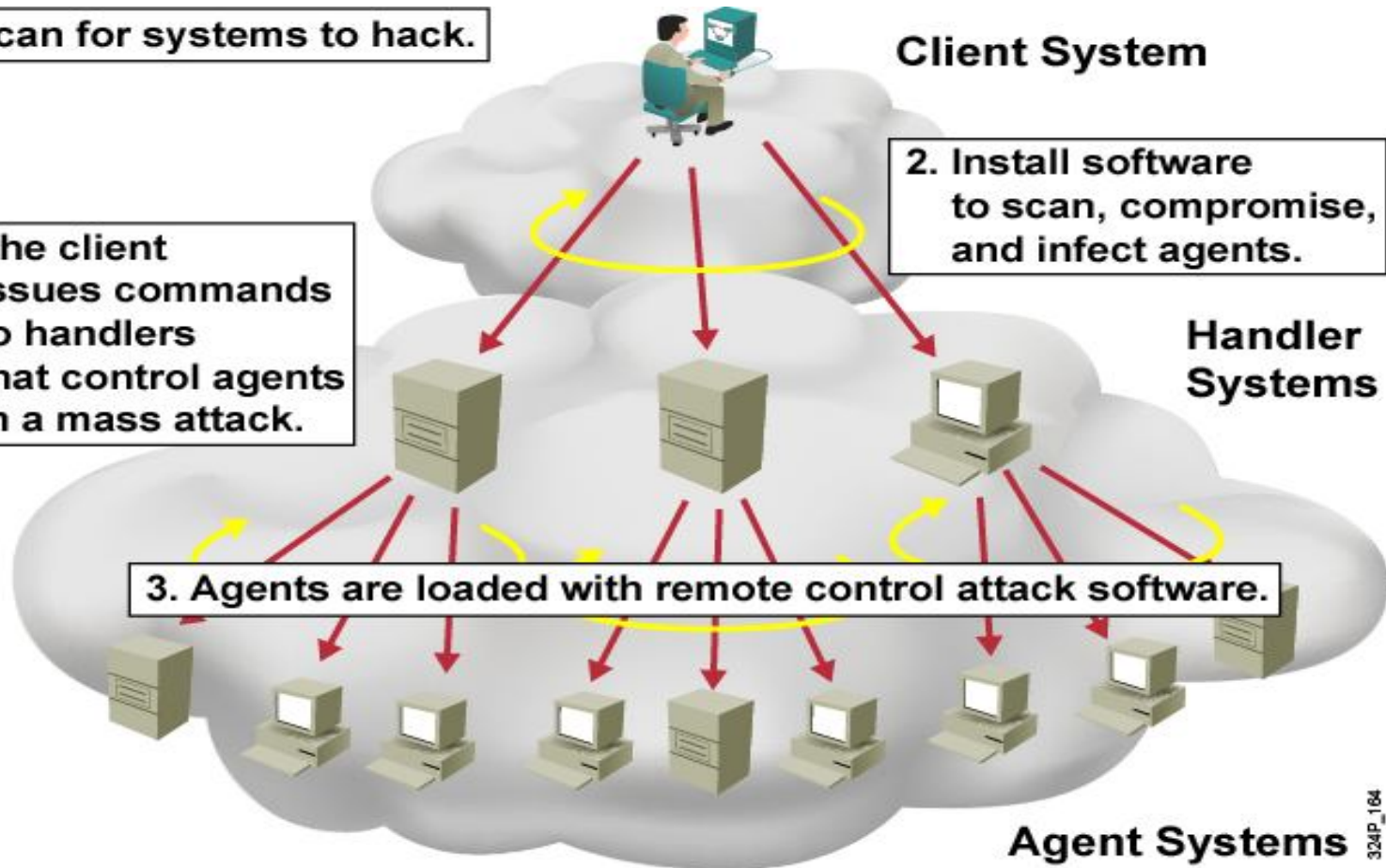
Handler Systems

4. The client issues commands to handlers that control agents in a mass attack.

3. Agents are loaded with remote control attack software.

Agent Systems

324P_164





Mitigación de los Ataques



Ataques de Reconocimiento

- La implementación y aplicación de una política que prohíbe el uso de protocolos con susceptibilidades conocidas a escuchas.
- El uso de encriptación que satisface las necesidades de seguridad de datos de la organización, sin imponer una carga excesiva sobre los recursos del sistema o los usuarios.
- Utilizar redes conmutadas.

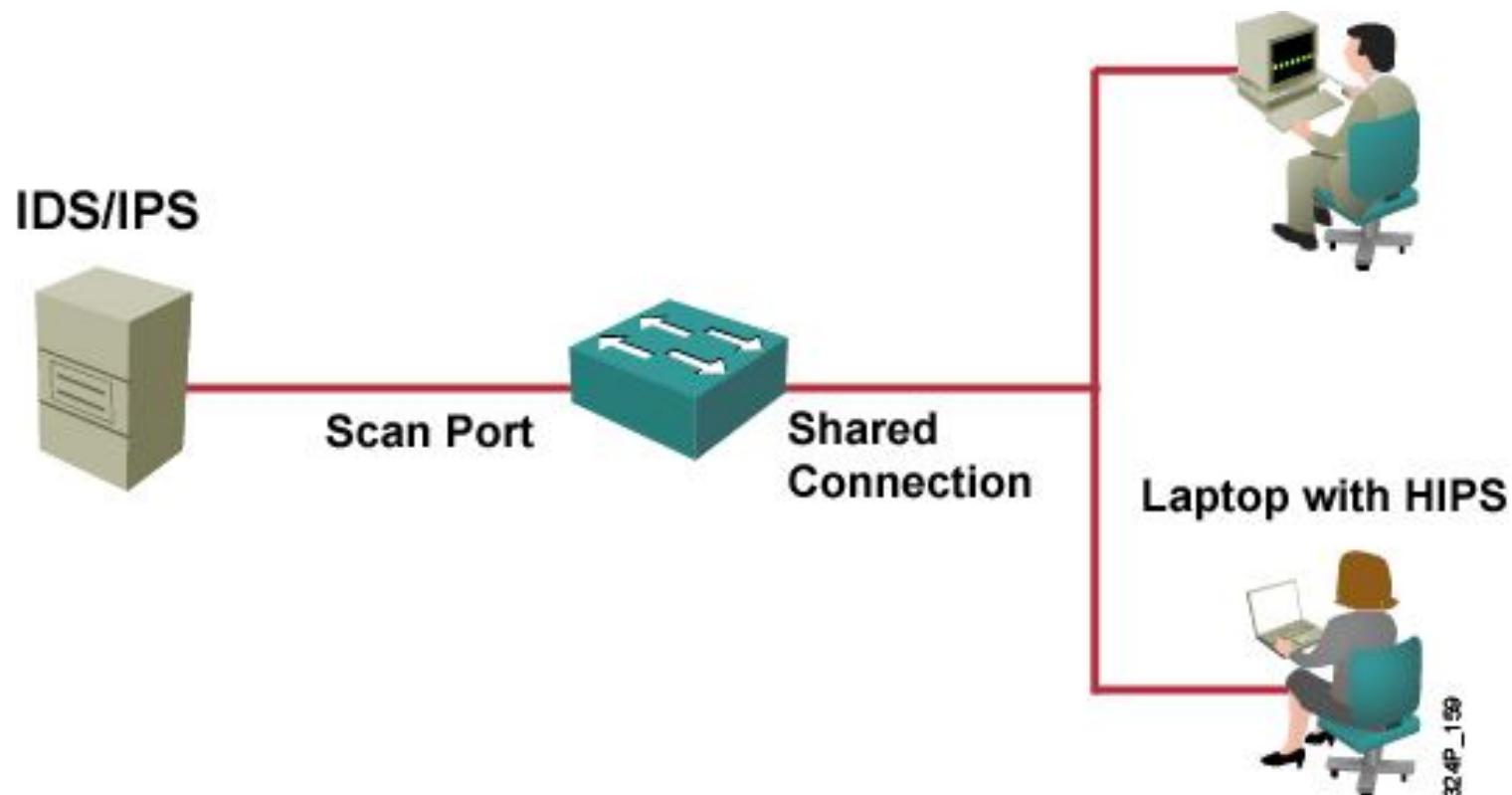


Mitigación del escaneo de Puertos y Barrido de Pings

- El escaneo de puertos y barrido ping no es un delito y no hay manera de detener estas exploraciones y barridos cuando un equipo está conectado a Internet.
- Los barridos de ping se puede detener si el echo de ICMP y la respuesta de eco-están deshabilitados en los routers de borde.

Mitigación del escaneo de Puertos y Barrido de Pings

- No se puede evitar sin comprometer las capacidades de red.
 - Sin embargo, el daño puede ser mitigado mediante sistemas de prevención de intrusiones (IPS) en los niveles de red y host.



Mitigacion de un Sniffer de Paquetes

- Autenticación
- Criptografía
- Herramientas Anti-sniffer
- Infraestructura Conmutada

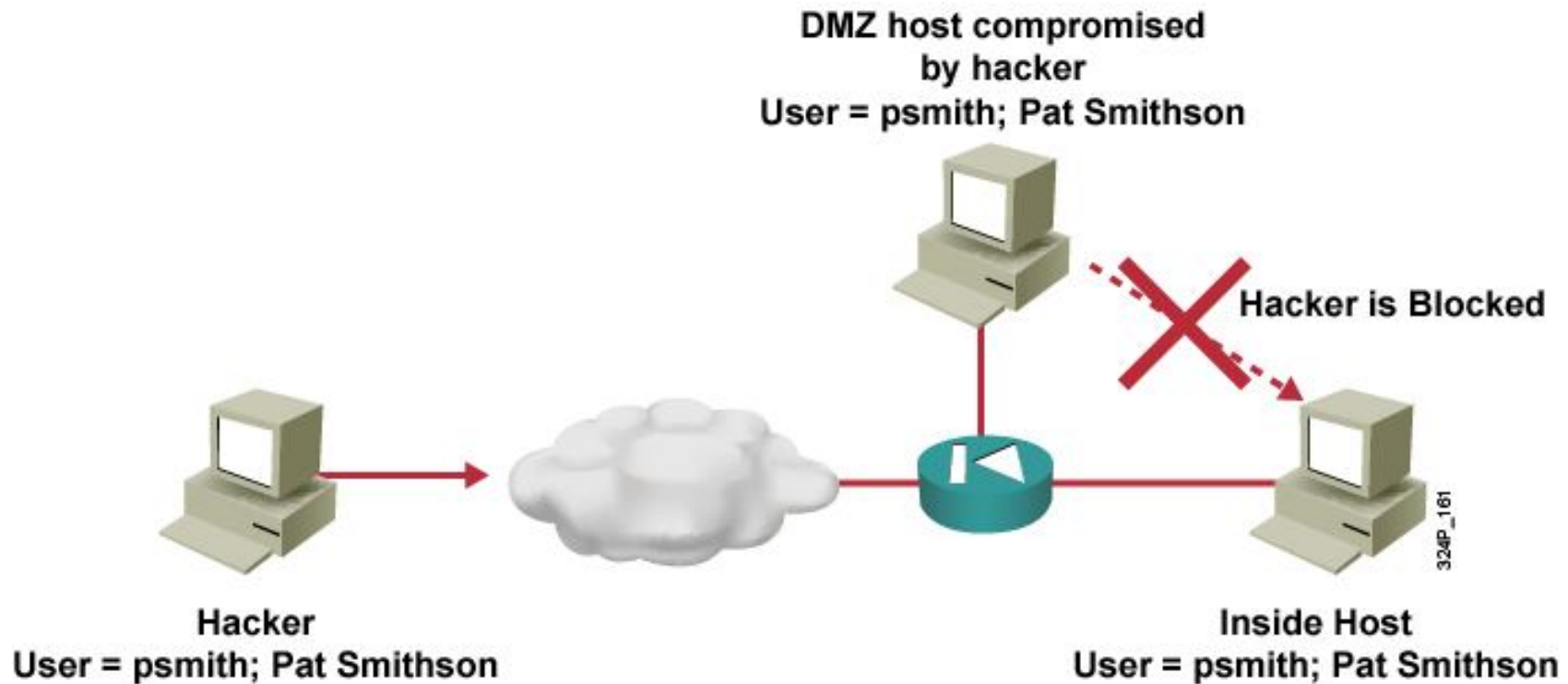


Mitigación de ataques de Contraseñas

- No permita que los usuarios utilicen la misma contraseña en varios sistemas.
- Deshabilitar la cuenta tras un cierto número de intentos de conexión fallidos.
- Use OTP o una contraseña criptográfico.
- Utilice contraseñas "fuertes" que son al menos ocho caracteres y contener letras mayúsculas, minúsculas, números y caracteres especiales.
- No use contraseñas en texto plano

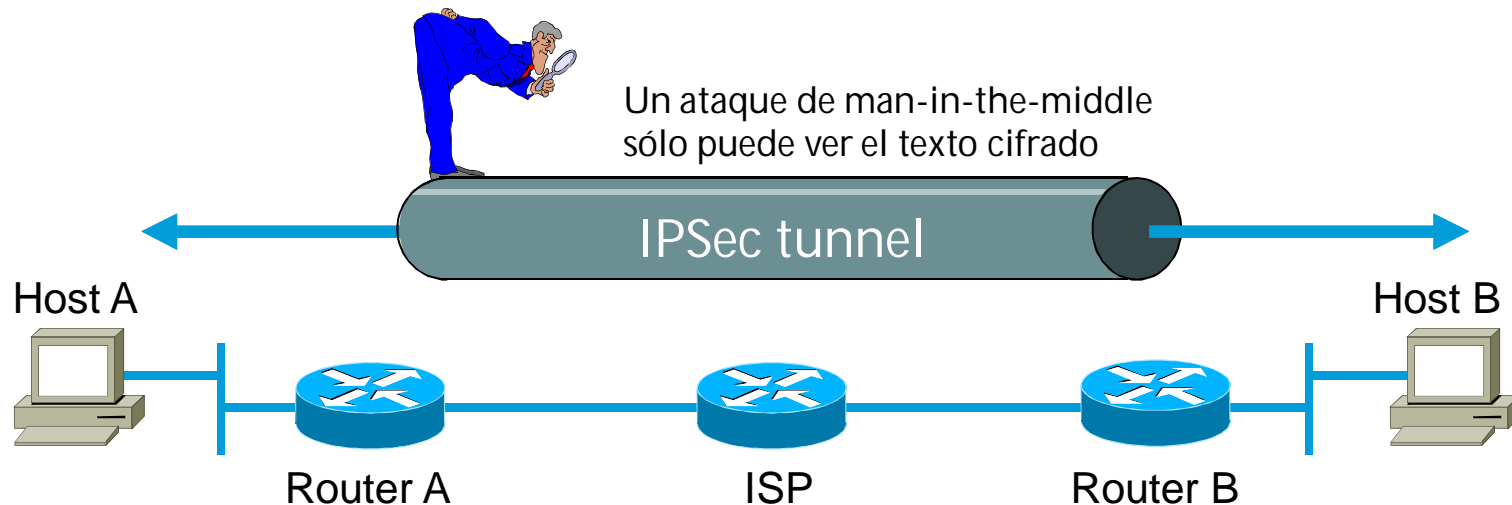
Mitigación de Ataque de Explotación de Confianza

- Los niveles de confianza dentro de una red deben estar bien sujetos garantizando que los sistemas dentro de un firewall pueda confiar absolutamente en los sistemas fuera de él.



Mitigación del Man-in-the-Middle

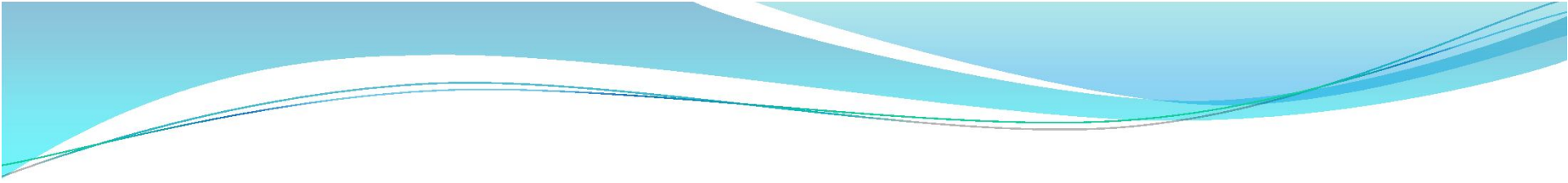
- Puede ser eficazmente mitigada sólo a través del uso de la criptografía (cifrado).





10 Mejores Prácticas

1. Mantener los parches hasta la fecha mediante la instalación de todas las semanas o todos los días, si es posible, para evitar desbordamiento de búfer y ataques de escalación de privilegios.
2. Deshabilitar los servicios innecesarios y puertos.
3. Utilice contraseñas seguras y cambiarlas con frecuencia.
4. Controlar el acceso físico a los sistemas.
5. Evite entradas innecesarias a páginas web.
6. Realizar copias de seguridad y probar los archivos de copia de seguridad en una base regular.
7. Educar a los empleados sobre los riesgos de la ingeniería social, y desarrollar estrategias para validar las identidades a través del teléfono, por correo electrónico o en persona.
8. Encriptar y proteger con contraseña los datos sensibles.
9. Implementar hardware y software de seguridad tales como firewalls, IPS, VPNs, anti-virus y filtrado de contenidos.
10. Desarrollar una política de seguridad para la empresa.



Cisco Network Foundation Protection (NFP)

Cisco Network Foundation Protection (NFP)

- NFP divide lógicamente routers y switches en tres áreas funcionales:
 - **Plano de Control** - Responsable del enrutamiento de datos correctamente. Consta de paquetes generados por el dispositivo necesarios para el funcionamiento de la red, tales como los mensajes ARP o anuncios de enrutamiento OSPF.
 - **Plano de Gestión** - Responsable de la gestión de elementos de red. Generado por cualquiera de los dos dispositivos de red o estaciones de administración que utilizan procesos y protocolos como Telnet, SSH, TFTP, FTP, NTP, AAA, SNMP, syslog, TACACS +, RADIUS y NetFlow.
 - **Plano de Datos** - Responsable de la transmisión de los datos. Consiste en paquetes generados por los usuarios que se reenvían entre las estaciones finales. La mayoría del tráfico viaja a través del router o switch, a través del plano de datos.



Asegurando el Plano de Control

- Cisco AutoSecure proporciona un bloqueo de un solo paso para los planos de control, gestión y datos.
- Protocolo de autenticación de Enrutamiento impide que el router acepte actualizaciones fraudulentas de enrutamiento.
- Políticas del Plano de Control o CoPP evita que el tráfico innecesario sobrecargue el procesador. CoPP trata el plano de control como una entidad separada y aplica reglas para la entrada y salida de las interfaces.



Asegurando el Plano de Gestión

- Implementar una política de inicio de sesión y contraseña para restringir el acceso a dispositivo.
- Notificación legal actual desarrollado por el asesor legal de una corporación.
- Garantizar la confidencialidad de los datos mediante el uso de protocolos de gestión de autenticación fuerte.
- Utilice un papel de control de acceso basado en roles (RBAC) para asegurarse de que el acceso se concede sólo a los usuarios autenticados, grupos y servicios.
- Restringir las acciones y puntos de vista que son permitidos por ningún usuario en particular del grupo, o servicio.
- Habilitar el registro de acceso de administración y dar cuentas de todos los accesos.

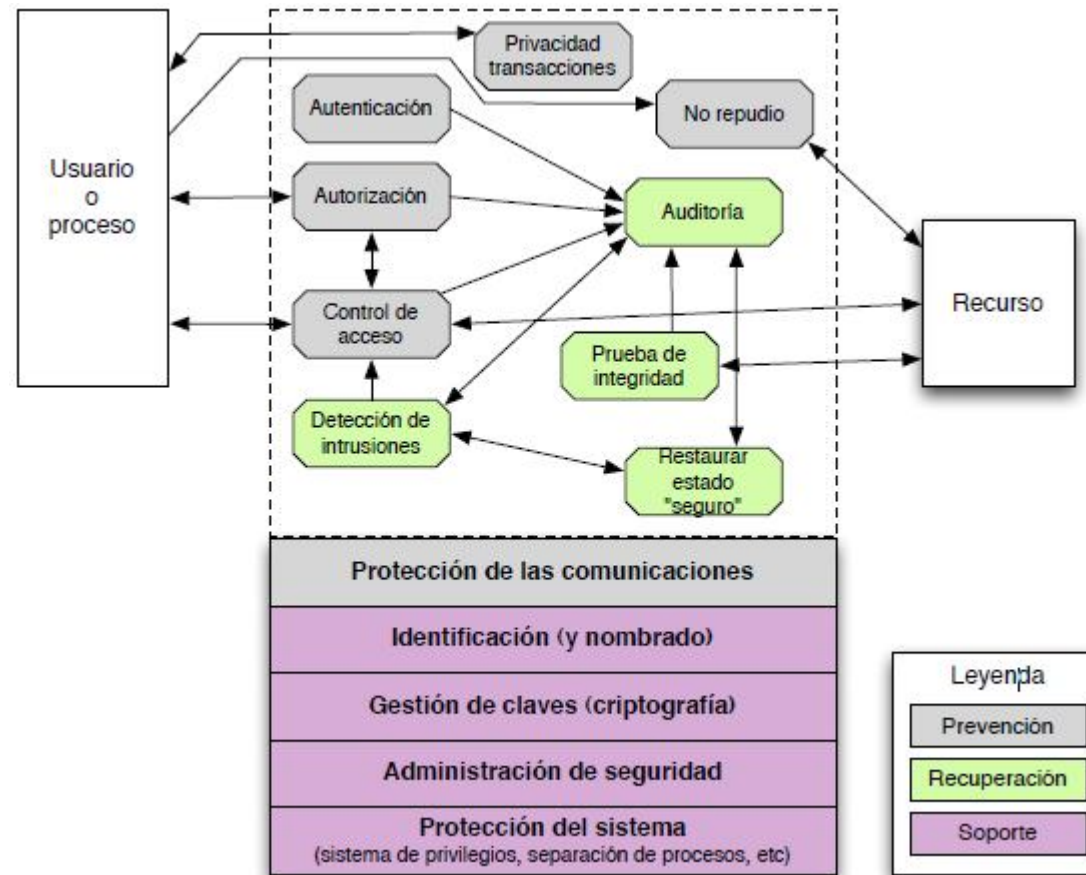
Asegurando el Plano de Datos

- Use ACLs para el filtrado de paquetes, así como también:
 - Bloquear el tráfico no deseado o usuarios.
 - Reducir el impacto de un ataque DoS.
 - Mitigar los ataques de suplantación de identidad.
 - Proporcionar control de ancho de banda.
 - Clasificar el tráfico para proteger a los planos de control y gestión.
- Implementar seguridad de Capa 2:
 - Port security
 - DHCP snooping
 - Dynamic ARP Inspection (DAI)
 - IP Source Guard

Mecanismos de seguridad(i) X.800

- **Mecanismos de seguridad específicos: para incorporar sobre la capa de seguridad OSI correspondiente.**
 - Cifrado
 - Firma digital
 - Control de acceso
 - Integridad
 - Mecanismos de autenticación
 - Tráfico de relleno
 - Control de enrutamiento
 - Mecanismos de notario
- **Mecanismos de seguridad omnipresentes: no específicos de ninguna capa OSI concreta.**
 - Mecanismos de confianza
 - Etiquetas de seguridad
 - Detección de eventos
 - Auditorías de seguridad
 - Mecanismos de recuperación

Un modelo de seguridad en redes



Fuente: Security Services Model, NIST Special Publication 800-33, December 2001, Underlying Technical Models

Estándares SGSI

- **SGSI (ISMS):** Sistemas de **G**estión de la **S**eguridad de la **I**nformación (Information Security Management System)
- **Información** conjunto de datos organizados que pueden poseer valor para la entidad que los posea
- **Normativa ISO 27000**
 - Seguridad de la información: preservación de su confidencialidad, integridad y disponibilidad.
 - También se contempla la seguridad de los sistemas implicados en el tratamiento de la información dentro de la organización.
 - Propone hacer uso de procesos sistemáticos, documentados y conocidos por toda la organización.



Certificaciones

- Empresas certifican (mediante exámenes) los conocimientos sobre seguridad informática o sobre cómo utilizar sus propios productos en seguridad informática.
- Pueden ser requisito para ciertos proyectos de implantación y para cumplir con normativas de seguridad.
- La mayoría de las certificaciones debe ser renovadas después de unos años (por lo general, no más de 5 años)



¿Preguntas?