EJERCICIO 1

Un desarrollador de una aplicación web debe diseñar y programar el módulo de autenticación de un sistema de control de reactores nucleares. Se ve frente a las siguientes opciones para almacenar las contraseñas en una base de datos:

- En texto claro
- Cifradas con AES y una clave fija
- "Hasheadas" con SHA-1

Explique cuáles son los problemas con cada uno de los métodos anteriores y los posibles ataques, si es que los hubiere. De haberlos, explique el diseño de un algoritmo que no presente las mismas debilidades ni sea vulnerable a los mismos ataques.

EJERCICIO 2

Las bases de datos Oracle soportan un mecanismo de autenticación llamado "remote OS authentication" que permite delegar la autenticación del usuario a un sistema operativo remoto. Es decir, permite que el usuario Pompin autenticado en un sistema operativo remoto se conecte a través de la red a la base de datos sin proveer credenciales (asumiendo que el usuario Pompin existe en la base de datos y está configurada su cuenta para autenticación remota).

¿Cuál es el problema de seguridad que presenta este mecanismo? Si tuviese un aplicativo que no funciona si no se habilita este mecanismo de autenticación para un usuario particular en la base de datos, ¿cómo haría para proteger esta cuenta?

EJERCICIO 3

Los servicios/comandos "r" utilizan el servicio Identd (TCP/113) para autenticar al usuario. ¿Qué mecanismo de seguridad del sistema operativo es el que impide que un atacante, con acceso como usuario no privilegiado a un servidor con relación de confianza con otro servidor, ejecute un demonio Identd que falsifique las respuestas para obtener acceso al servidor con el cual existe la relación de confianza? ¿Cómo podría un atacante falsificar la respuesta del demonio Identd?

Ejercicio 4

Intente romper los siguientes hashes para recuperar las contraseñas. Puede usar john the ripper o hashcat. Analice el tiempo que lleva, según el tipo de función de hash utilizada.

```
$1$qGEreJi2$39ObxEF4LYTCAXoiTyDRm0
$1$VdFKGU2S$fnuxigiQSL5TbiAwZkWnZ/
$1$uyaHqCxf$Pv6s3HlUJUhSxx8VrTdNL1
$1$lo6ivJ3m$mneUFEef7VRsR7fh2nv7..
$1$IHTGnm3.$TlbBtLyiwZrIlsNduffXO.
$1$LCs.Vq2.$T/qDNkeKq5bQofv2Rq0eL0
$1$dCnByexu$oi0F4kI19cW9/3wcTBVmR.
```

```
$6$MPEeVP.VQ73onVLN$IzbQHcH7KmeHZmLMpUXq293ore4sAfDRRhVXQ
B.5Nxdhn141.VFWpjhPf6uG4Zyld.K9CqOMgwLajpG0dH0on1
$6$XdO9dFHoVEupc8iZ$7Kao9/4M2MUYImrNIn38uI9tQvDdQIbuDIhEJ
RV.AK6GZ1V6k9OMvlv6xxu6vQ7vasPOXNMs/AD2UNldMDdC9.
$6$rounds=100000$PmAi1QqBOoY4PEWI$RpB2UpZMQM2jMP.JZ8PIsuR
n1qtA/Z55fsQRLZ94Eba7zXthNpIASOMfHCTe7ExZChIfsi6Mi.LR8q0P
IIeYF0
```

EJERCICIO 5

Dado que existe el protocolo SSL y es ampliamente utilizado para proteger conexiones HTTP en Internet, ¿se lo podría utilizar para proteger los correos electrónicos cifrando las comunicaciones entre los servidores SMTP? ¿Sería suficiente o sería necesario cifrar las comunicaciones entre los clientes y los servidores POP/IMAP? ¿Garantizaría la integridad de la autoría del correo electrónico? ¿Proveería la propiedad de no repudio?

EJERCICIO 6

Una empresa implementa una aplicación cliente-servidor, y luego de un análisis de riesgo decide que no es necesario cifrar toda la comunicación sino que únicamente desea cifrar la contraseña del usuario para protegerse de un ataque de "eavesdropping". El protocolo que implementan es el siguiente: la contraseña del usuario se cifra utilizando un algoritmo de cifrado de flujo (simétrico) y se envía. Por simplicidad no utiliza un vector de inicialización.
¿Cuál o cuáles son los problemas con este esquema? ¿Cómo podría hacer un atacante con acceso al cliente para descifrar una captura de autenticación exitosa que obtuvo al "sniffear" la red? ¿Necesita el atacante acceso al cliente?

EJERCICIO 7

Una empresa desarrolla un sistema ERP escalable. Su arquitectura consiste de uno o más servidores de presentación a los cuáles se conectan los clientes (que tienen la lista de servidores de presentación configurada), un Gateway de aplicación y uno o más servidores de aplicación. Cabe resaltar que todos los servidores se encuentran en el mismo segmento de red.

Los servidores de aplicación se registran con el Gateway al igual que los servidores de presentación. Las tareas son ejecutadas por los servidores de aplicación, la interacción con los clientes por los servidores de presentación, y el balance de la carga entre los servidores de aplicación por el Gateway.

Supongamos que el mecanismo de registración con el Gateway no posee ningún mecanismo de control de acceso y, por simplicidad, que existe un único servidor de aplicación y un único servidor de presentación. ¿Cómo podría un atacante realizar un ataque de Man-in-the-middle a las conexiones entre el servidor principal y el servidor de aplicación? ¿Es necesario que el atacante se encuentre en el mismo segmento de red que los servidores? Sin cambiar la arquitectura ni los (no)mecanismos de autenticación, ¿cómo se podría proteger al sistema de éste ataque? ¿Serviría un IDS/IPS para éste propósito? ¿Y una VPN? Justifique su respuesta.

EJERCICIO 8

¿Cómo se podría detectar que un firewall implementa stateful packet inspection? ¿Podría un IDS detectar este ataque? ¿Podría prevenirlo un IPS? Justifique su respuesta.

EJERCICIO 9

Supongamos que para acceder a un determinado servidor Web, se debe primero establecer una VPN contra un concentrador. Si al conectarme al servidor Web que utiliza SSL me da un error de certificado porque no tengo instalado el certificado de la autoridad certificante que emitió el certificado utilizado por el servidor Web, ¿puedo confiar en que me estoy conectando al servidor Web real ya que estoy utilizando una VPN para acceder al segmento de red dónde está conectado el servidor? ¿Y si en lugar de un servidor Web fuese un servidor SSH que no tengo almacenado en el archivo de hosts conocidos? Justifique su respuesta.

EJERCICIO 10

En la captura x-forwarded-for-filtered.pcap vemos un pedido HTTP al sitio del DC. ¿Qué datos se pueden deducir del cliente realizando la petición? ¿El cliente se encuentra utilizando un proxy? Justifique su respuesta.

EJERCICIO 11

En la captura dns-spoofing.pcap vemos dos peticiones DNS por el nombre www.dc.uba.ar. ¿Qué diferencias encuentra entre las peticiones y respuestas de DNS? ¿Se puede tratar de un ataque? En caso afirmativo, ¿cuál y por qué? Justifique su respuesta.

EJERCICIO 12

Analice la captura de tráfico contenida en el archivo smtp-auth-cram-md5.pcap
Extraiga la información relacionado con el login, y consiga el usuario y la contraseña en texto claro.

EJERCICIO 13

La captura de tráfico del archivo ojo_malware.pcap contiene un ejemplo de una máquina que fue atacada, y el cliente automáticamente descargó un binario y lo ejecutó. Obtenga con cuidado el binario de la captura, y analícelo a través del sitio virustotal.com. ¿Qué otras cosas ve en la captura?