Tema 4 – Seguridad y privacidad en aplicaciones telemáticas

1 Herramientas de seguridad Red Team

Consiste en un equipo especializado en realizar actividades ofensivas, buscando las vulnerabilidades de su propio sistema y reportándoselo al equipo Blue. Se diseñan los ataques de forma personalizada para la arquitectura del sistema, se identifican herramientas para explotar las debilidades y ejecutar los ataques.

1.1 Kali Linux

Es una distribución de Debian diseñada principalmente para la auditoría y seguridad informática.

1.2 Parrot Security OS

Diseñada para realizar pruebas de penetración, evaluación y análisis de vulnerabilidades.

1.3 Otras herramientas de seguridad

- Aircrack-ng - herramienta para descifrar claves 802.11 TPA-PSA y WEP
- Burpsuite - herramienta integrada para probar aplicaciones web
- **Hydra** – herramienta para derivar credenciales de seguridad e iniciar sesión
  - Permite crackear inicio de sesión por fuerza bruta
- John (the Ripper) - herramienta derivar contraseñas
- Maltego – herramienta de inteligencia y forense
- Metasploit framework – un suite de herramientas para realizar pruebas de seguridad extremadamente flexible
- **Nmap** - herramienta de mapeo de redes
  - Recopila información de puertos abiertos, rangos IP, información del sistema operativo.
- Owasp-ZAP - herramienta de prueba de aplicaciones web
- **Wireshark** - La principal herramienta de análisis de protocolos de red
  - Captura de tráfico red y sniffing
- Lego (la versión actualizada de Sparta) - herramienta de pruebas de penetración de la infraestructura de red
- **Scapy** – herramienta de manipulación de paquetes de red
  - Creación, modificación, captura y envío de paquetes.
- **Ettercap-graphical** - herramienta de ARP spoofing
  - Permite simular Man in the Middle.

Se recomienda revisar la página para tratar ataques de entre los disponibles.
https://attack.mitre.org/matrices/enterprise/

2 Herramientas de seguridad Blue Team

Consiste en un equipo especializado en realizar actividades defensivas tratando, evitando y mitigando vulnerabilidades.

2.1 SEGURIDAD EN EMAIL

2.1.1 PGP (Pretty Good Privacy)

Integra algoritmos criptográficos para proporcionar servicios de autenticidad y confidencialidad para aplicaciones de e-mail y de almacenamiento de ficheros. No permite el uso de certificado.

Por cada usuario almacena pares clave privada y pública (private-keyring) y la clave pública de los usuarios con los que se ha interactuado (public-key ring), es un modelo de PKI en malla.

2.1.2 S/MIME (Secure/Multipurpose Internet Mail Extension)

Sigue también el modelo de PKI híbrido, pero permite el uso de certificados.

Function	Requirement
Create a message digest to be used in forming a digital signature.	MUST support SHA-1. Receiver SHOULD support MD5 for backward compatibility.
Encrypt message digest to form a digital signature.	Sending and receiving agents MUST support DSS. Sending agents SHOULD support RSA encryption. Receiving agents SHOULD support verification of RSA signatures with key sizes 512 bits to 1024 bits.
Encrypt session key for transmission with a message.	Sending and receiving agents SHOULD support Diffie-Hellman. Sending and receiving agents MUST support RSA encryption with key sizes 512 bits to 1024 bits.
Encrypt message for transmission with a one-time session key.	Sending and receiving agents MUST support encryption with tripleDES. Sending agents SHOULD support encryption with AES. Sending agents SHOULD support encryption with RC2/40.
Create a message authentication code.	Receiving agents MUST support HMAC with SHA-1. Sending agents SHOULD support HMAC with SHA-1.

2.1.3 .zip

¿Qué pasa si enviamos un archivo .zip que realmente es un ejecutable? Se recomienda usar PGP y S/MIME para la compartición de archivos comprimidos.

2.2 SEGURIDAD DE OTROS PROTOCOLOS RED

Telnet (puerto 23) para el acceso remoto.

FTP (puerto 20/21) permite la transferencia de ficheros entre diferentes recursos.

SSH (Secure Shell, puerto 22) cifra transacción con criptografía pública. Se divide en tres capas de aplicación (autenticación), transporte (intercambio de claves) y capas de red (conexión directa). Se crean un proceso sin privilegios y otros con privilegios una vez confirmado. Mitiga spoofing de IP o DNS.

Existen clientes cmoo PuTTy y Open SSH.

SFTP usa como base SSH, para modos de autenticación.

FTPS se basa, no obstante, en **TLS**.

2.3 HERRAMIENTAS DE CIFRADO

- TrueCrypt
- DiskCryptor

- VeraCrypt, iterativa
- BitLocker, que permite cifrar datos de disco futo unidad de flash hace uso de Trusted Platform Module.

O de esteganografía como OpenStego y OpenPuff.

3 SEGURIDAD EN PAGOS ELECTRÓNICOS

Involucran a un comprador y a un vendedor, incluso con un mediador para resolver conflictos. Las clasificaciones de sistema dependen de:

- Cuándo el vendedor contacta con el banco para verificar el proceso:
  - Online
  - Offline, se realiza el contacto con el banco después del proceso de compra bena
- Cuándo el comprador procede con la transacción:
  - Pre-pago, antes de la compra. Ejemplo: monedero electrónico y tarjetas telefónicas.
  - Pago instantáneo, al aceptar la compra
  - Post pago, después de aceptar la compra
- La cantidad de dinero:
  - Micropagos
  - Pagos
  - Macropagos
    Normalmente, los pagos inferiores a 10 euros presentan el problema del coste de implementación.

3.1 PROBLEMAS DE SEGURIDAD

- Ataques de escucha
- Suplantación de identidad
- Generación de dato dalso
- Modificación del dato

Inicialmente se aplicaba el protocolo SSL (Secure Socket Layer), aunque no estaba pensada para pagos electrónicos, establecía un canal seguro. Por otra parte, solo protegía transacciones entre dos puntos, no protege al comprador frente al vendedor, no hay mecanismos de autenticación de tarjetas y de facturación.

3.2 SECURE ELECTRONIC TRANSACTIONS (SET)

Proporciona confidencialidad, autenticación con X.509, privacidad, integridad, no repudio y autorización de pago. Pasos del protocolo SET:

1. Petición del producto
2. Inicialización, envío de certificados
3. Información del pedido e instrucciones de pago, descripción de la compra
4. Petición de autorización vendedor-pasarela y pasarela-banco emisor
5. Aprobación de autorización, el banco emisor autoriza el pago
6. Finalización, compensación entre bancos

3.2.1 Firma dual

La información del pago (Payment Information - PI) al banco y la información del pedido al comerciante (Order Information - OI) al comerciante. Se cifra el hash de la combinación de los hashes del PI y OI, el resultado es la firma dual. Con esto se evitan problemas de privacidad al estar separados en hash y tener que cada entidad realice el hash sobre la parte que posea, y comparar el resultado.

La PKI tiene CA de comerciante, usuario y pago.

Si bien garantiza los servicios de autenticación, confidencialidad, integridad, no-repudio y privacidad; supone una dependencia con RSA/DES/SHA y no está adaptado a micropagos.

3.3 CYBERCASH

Usa una pasarela propia permitiendo el uso de cualquier tipo de tarjeta, también presenta el concepto de cyberwallet. No existe privacidad de la información del cliente en la pasarela "privada".

3.4 I-KEY (IKP)

iKP (i = 1, 2, 3), son protocolos desarrollados por IBM multiparte, donde la i corresponde a las entidades que necesitan el certificado.

3.5 MICROPAGOS

Debido a que la infraestructura y protocolos anteriores pueden suponer unos gastos exagerados para pagos pequeños, se tratan de solucionar los costes como servicios de prepago, autorizaciones off-line, agrupación de facturas para el micropago por lotes y soluciones online.

3.5.1 Milicent

Existe una figura del agente de negocios y una moneda electrónica, el scrip que se compran a través de un broker. Se consigue cierto anonimato por parte del comprador,

4 PRIVACIDAD DE LOS USUARIOS EN APLICACIONES

4.1 CONCEPTOS GENERALES

La **privacidad** puede definirse como el derecho de los individuos y entidades de proteger; salvaguardar y controlar el acceso, almacenamiento, distribución y uso de información sobre su propia persona.

- La confidencialidad es relativa a los datos, mientras que la privacidad, las personas.
- Todo lo que se sube a la red es público.
- El análisis de tráfico permite a observadores externos obtener información a través de la comunicación de un usuario.

Las propiedades de la privacidad son:

- No-vinculación: no se puede inducir información a través de dos mensajes
- No-observabilidad: imposibilita distinguir la referencia del mensaje
- Anonimato: el estado de no ser identificable entre un grupo de sujetos

Técnicas:

- **Pseudónimos**, aunque su uso continuado puede ser vinculante.
- **Anonimato rastreable**, en caso de necesidad se puede revelar la identidad; por ejemplo, vendedor con banco.
- **Anonimato no rastreable**, garantiza que la identidad de los usuarios no se va a revelar.
- **Anonimato no rastreable y no vinculante**, garantiza que la identidad no se puede revelar y no se pueden vincular las operaciones

4.2 Privacidad basada en esquemas avanzados

4.2.1 Firma digital

- **Firma ciega** (anonimato rastreable), firma desconociendo el contenido. Por ejemplo, el voto electrónico.
- **Firma de grupo** (anonimato rastreable), que cuenta con un administrador del grupo, miembros y un verificador (receptor). Se origina una clave pública de grupo, claves privadas individuales y una clave de administrador.
- **Firma de anillo** (anonimato no rastreable ni vinculante), cada miembro genera su clave privada y usa las públicas de los demás.

4.2.2 Protocolos criptográficos y de enrutado

- Uso de **proxy**, intermediario en la comunicación, aceptando conexiones del cliente, pudiendo proteger la dirección IP
- Uso de mezcladores (**mixer**), que cambia el orden de los paquetes
- Conocimiento parcial de la ruta
    - **Onion Routing**: el onion proxy crea un paquete cifrado en capas (cebollas) que se va descifrando según pasa por los routers onion.
    - **TOR**: es la segunda generación que permite navegar a través de una ruta privada de la red, crea de manera aleatoria. Se configura una red con un entry guard, middle relay y exit relay, que devuelve al destino el paquete sin cifrar. Cada 10 minutos se renueva la red.
- Creación de grupos
    - **Crowds**: consiste en la agrupación de multitudes donde cada nodo solo conoce el destino y el nodo desde el que recibe el paquete
    - **Hordes**: a diferencia del crowd, se hace un broadcast de la respuesta desde el router a todos los miembros.

Test

1 "Eks(Zip(M)) || Kpubb(Ks)" es una operación específica de:

a) PGP
b) SFTP
c) SMIME
d) FTPS

2 ¿Cómo hay que almacenar las contraseñas de nuestros usuarios?

a) Protegidas con sal y hasheadas
b) Protegidas con sal y hasheadas con un hash específico como bcrypt
c) En claro
d) Cifradas

3 ¿Cuáles son las operaciones proporcionadas por PGP?

a) Firma digital, cifrado
b) Firma digital, cifrado, compresión, compatibilidad de e-mail, anonimato
c) Firma digital, compresión, compatibilidad de e-mail
d) Firma digital, cifrado, compresión, compatibilidad de e-mail

4 ¿Cuál es el modelo de PKI utilizado por PGP?

a) Modelo de PKI híbrido
b) Modelo de PKI en malla
c) Modelo de PKI en círculo
d) Modelo de PKI jerárquico

5 ¿Cuál es el modelo de PKI utilizado por S/MIME?

a) Modelo de PKI jerárquico
b) Modelo de PKI en círculo
c) Modelo de PKI híbrido
d) Modelo de PKI en malla

6 ¿Dónde se realiza el cifrado en el protocolo SSH?

a) En la capa de aplicación (debajo de otras aplicaciones)
b) En la capa física
c) En la capa de red (IP)
d) En la capa de transporte (TCP)

7 VeraCrypt es similar a TrueCrypt pero:

a) incluye operaciones de compresión para reducir complejidades
b) incluye un número específico de iteraciones para el cifrado
c) incluye un número específico de iteraciones para el cifrado y un conjunto de operaciones de compresión para reducir complejidades
d) incluye un número de algoritmos de cifrado equivalente a DoskCraptor

Bibliografía