Introdución á Seguridade Informática

A seguridade da información abrangue todas aquelas medidas preventivas que permitan protexer a información buscando manter a súa confidencialidade, dispoñibilidade e integridade.

As medidas de seguridade para intentar sortear as distintas ameazas poden clasificarse:

- Segundo ó recurso a protexer
  - *Seguridade física:* Intenta mitigar situacións debidas a ameazas de tipo físico, como roubos, incendios, terremotos, etc. As medidas deste tipo poden ir dende o estudo da situación física do equipamento, ata a implantación de sistemas antiincendio.
  - *Seguridade lóxica:* Protexe o sistema contra situacións provocadas polo software. Medidas comúns son as contrasinais, os permisos, o cifrado, os firewalls...
- Segundo o momento en que se toman as medidas
  - *Seguridade activa:* Son medidas preventivas. Intentan evitar os danos no sistema. Un exemplo pode ser un control de acceso a un recinto, ou un firewall.
  - *Seguridade pasiva:* Son medidas paliativas ou correctivas. intentan reducir o alcance dos danos unha vez producidos. Un exemplo pode ser unha copia de seguridade ou unha liña de comunicacións de reserva.

Confidencialidade

A **Confidencialidade** consiste en garantir que unicamente poderán acceder á información e a os sistemas os usuarios coa autorización requirida.

A Confidencialidade é difícil de garantir e se consigue normalmente empregando criptografía (**cifrado**). Cifrando a información podemos garantir que so os usuarios coa chave de descifrado poderán acceder á mesma. Este tipo de cifrado se realiza habitualmente utilizando ***chaves de cifrado simétricas*** (se usa a mesma chave para cifrar e descifra) que pode ser a nivel de disco, ou a nivel de sistemas de arquivos (cifrados de disco e cifrados de arquivos e carpetas).

Integridade e Non Repudio

A **integridade** pretende garantir que a información non é modificada durante a transmisión, e que a información recibida é igual a información transmitida. As sumas hash MD5 son un medio común de verificación de integridade, existindo sistemas que protexen os arquivos importantes calculando e gardando as súas sumas hash.

O **non repudio** consiste en que o receptor dunha mensaxe ten a completa seguridade da autoría da mensaxe (*non repudio en orixe*), ou que o emisor ten a seguridade de que o receptor recibiu a mensaxe (*non repudio en destino*).

Estas medidas de seguridade teñen gran importancia na web para evitar ataques como o Phising (suplantación) ou MiM (man in the middle), que poden dar lugar a multitude de fraudes.

As medidas para garantizar a integridade e non repudio máis habituais consisten no uso de ***cifrado de chave pública***.

Cifrado de Chave Pública

O cifrado de chave pública ou de cifrado asimétrico a diferencia do cifrado simétrico, emprega dúas chaves de cifrado distintas. O que se cifra con unha das chaves unicamente se pode descifrar coa outra.

Unha das chaves se garda en segredo, e se denomina **chave privada**. A outra chave se distribúe a todo o mundo, e se denomina **chave pública**.

Este sistema de cifrado proporciona Confidencialidade, Integridade e non repudio en orixe, polo que é ampliamente utilizado nas comunicacións como conexións de acceso remoto (ssh), protección de emails (cifrado e firma), protección de documentos (cifrado e firma) ou http seguro.

O funcionamento é o seguinte:

Cando un usuario desexa enviar información de modo seguro empregando cifrado de chave pública sabe que os destinatarios teñen acceso a súa chave pública, xa que é de libre distribución.

O que ese usuario cifre coa súa chave privada (que so ten él) e accesible por todo o mundo que teña a chave pública. Eso *garantiza o non repudio en orixe*, xa que si a ***chave pública*** é capaz de descifrar a información é completamente seguro que esa información foi cifrada coa ***chave privada*** correspondente.

Si o que queremos é garantizar a confidencialidade, bastará con cifrar a información coa chave pública do destinatario, e este a poderá descifrar coa súa chave privada.

Si o que queremos é garantizar a integridade, deberíamos cifrar coa chave privada un ***checksum*** da información a transmitir de xeito que si esta cambia se detecte a corrupción. Esto verifica tamén a autoría (non-repudio en orixe) polo que se coñece co nome de ***firma dixital***.

En realidade a criptografía de chave asimétrica por motivos matemáticos non é eficiente para cifrar volumes de información medios ou grandes sendo moito máis útil para esta funcionalidade o cifrado simétrico, polo que se combinan os dous sistemas. A información se cifra cunha chave simétrica que se distribúe cifrada coa chave pública do destinatario.

O punto débil deste sistema radica *na distribución das chaves públicas*. Si nos enganan para que pensemos que unha chave pública pertence a alguén, e non é certo, a comunicación con esa entidade está comprometida. Imaxinemos que dispoñemos da chave pública do que pensamos é o noso banco porque nola facilitou un terceiro ou porque a descargamos de internet e resulta que en realidade esa chave pública corresponde a *Ladróns S.L.*. Teremos a seguridade (errónea) de que a información que nos está a enviar *Ladróns S.L.* ven do noso banco abrindo a posibilidade de roubo de información privada e de credenciais.

Para reducir ao máximo este punto débil do sistema se empregan dúas aproximacións distintas:

- **Confianza entre pares:** Para confiar na veracidade dunha chave pública se exixe que estea firmada (un ***hash*** da chave cifrado cunha chave privada) por unha chave privada de alguén en quen xa confiemos, ou que confíe nel alguén en quen confiemos. O firmado de chaves non é xerárquico se non a nivel particular, chegándose incluso a organizar “quedadas” de firmado de chaves (parties de firmas) nas que se obteñen os id das chaves que se van a firmar unha vez comprobada fisicamente a identidade do seu propietario. Este sistema o emprega ***PGP,*** que se utiliza amplamente no correo electrónico. Habitualmente as chaves

unha vez firmadas se aloxan en servidores públicos de chaves PGP de onde poden ser recuperadas facilmente por calquera que as necesiten

- **Autoridades de Certificación**: Se utilizan entidades legalmente recoñecidas que teñen como misión asegurar a identidade das chaves públicas e firmalas. Cando unha entidade ou usuario desexan facer uso de criptografía de chave pública que empregue este sistema deben "mercar un certificado" a unha autoridade de certificación, o que é nin máis nin menos que pedirlle a unha Autoridade de Certificación recoñecida que firme a nosa chave pública. A autoridade de certificación previa comprobación da nosa identidade (de xeito máis ou menos rigoroso segundo o nivel de certificación solicitado e pagado) procederá a firma creando un ***Certificado*** en formato X.509. Este sistema se emprega na web para a creación de servidores web seguros (https) e para asegurar o correo electrónico. Actualmente todos os cidadáns de España poden dispoñer de certificados e chaves privadas de firma de modo gratuito a través do seu DNI dixital.

Hoxe en día é esencial o usio do cifrado asimétrico na web para evitar suplantacións (phising) e interceptación de información confidencial como chaves de acceso a aplicacións web. O sistema utilizado emprega X.509 e o protocolo se denomina **https.** O funcionamento é o seguinte:

1. O cliente se conecta co servidor, solicitando unha conexión https://
2. O servidor responde co seu certificado (chave pública firmada por unha autoridade de certificación)
3. O cliente comproba a validez do certificado, descifrando a firma coa chave pública da autoridade de certificación que ven normalmente pre-instalada no navegador. Si non é a sí se emite un aviso de alerta.
4. O cliente crea unha chave ao azar para cifrar a información que se va a intercambiar co servidor e a cifra coa chave pública do certificado recibido (co que so o que ten a chave privada correspondente poderá descifrala, e ese é o servidor...). Se cifran as cabeceiras da petición con esa chave e se envía todo ao servidor.
5. O servidor recibe a petición cifrada coa chave simétrica, e a chave simétrica cifrada coa súa chave pública. Descifra a chave simétrica, e logo descifra a petición e envía a resposta cifrada. Temos garantizada así a ***Confidencialidade*** (toda a información que se intercambien irá cifrada coa chave simétrica), a ***Integridade*** (a información vai cifrada, si se altera, non se poderá descifrar) e o ***Non Repudio*** (so as dúas partes coñecen a chave de cifrado, e a autenticidade do servidor a garantizou o certificado firmado)

Dispoñibilidade

A dispoñibilidade fai referencia a que a información debe estar dispoñible no momento en que se necesite acceder a ela. A dispoñibilidade pode estar comprometida por múltiples factores como fallos do hardware, de software, ataques maliciosos ou incluso inclemencias do tempo, terremotos, inundacións ou incendios.

Par evitar a falla de dispoñibilidade por fallos hardware se recurre normalmente á redundancia: Fontes de alimentación redundantes, SAIs, conexións de datos redundantes, tarxetas de rede redundantes, almacenamento reduntantes, RAID... etc.

Tamén é común o uso de clústers (redes de ordenadores que ofrecen servizos de modo que si un falla, outro pode tomar o relevo) ou balanceadores de carga.

Garantir a dispoñibilidade o 100% do tempo non é posible, polo que a dispoñibilidade se contrata en función do tempo máximo de fallo que se quere soportar. Os sistemas de Alta dispoñibilidade poden ofrecer dispoñibilidades dende 99.9% ao ano ata o 99.999% (5 minutos ao ano de falla).

Vulnerabilidades

Humanas

A vulnerabilidade máis importante e máis difícil de corrixir é a humana. As equivocacións ou enganos ao persoal da empresa son un dos problemas máis graves na seguridade informática. Hoxe en día, moito malware (como troianos ou rootkits, envíos de spam..) recorren á Enxeñería Social como medio de propagación. Todo o mundo coñece famosos correos como o do príncipe nixeriano, os correos ameazantes solicitando a instalación de software no sistema “para evitar o perigo” ou os “avisos de seguridade” de bancos e sistemas de crédito para que “aseguremos a nosa identidade”.

Contra este tipo de vulnerabilidades so cabe a formación do persoal e o sentido común.

Hardware

As vulnerabilidades debidas ao hardware se deben a posibles fallos no seu funcionamento debido a defectos de fabricación, desgaste ou desastres que podan afectar. Para reducir o impacto destas vulnerabilidades se recorre a redundancia (SAI, RAID, bonding de tarxetas de rede, fontes de alimentación redundante, varios accesos de rede... etc) e a ubicar os sistemas en sitios co medio ambiente (temperatura e humidade), acceso e sistema de construción controlados denominados CPD (Centros de Proceso de Datos).

Software

As vulnerabilidades software se deben a defectos de programación que poden permitir a posibles atacantes saltarse as medidas de seguridade rompendo a confidencialidade, integridade ou dispoñibilidade da información. Vulnerabilidades típicas son os Buffer Overflow que permiten escaladas de privilexios ou as SQL injections ou vulnerabilidades XSS nos servizos web.

Bases de datos de vulnerabilidades

As vulnerabilidades do software de uso máis común se recollen en bases de datos públicas que permiten aos administradores de sistemas coñecer e paliar os posibles fallos dos seus sistemas.

Estas bases de datos se utilizan para a realización de test de penetración (pentesting) que persiguen localizar as debilidades dos sistemas para a súa posterior protección, e moitas de elas incorporan probas de concepto que permiten explotar e verificar as vulnerabildades (exploits).

Bases de datos de vulnerabilidades coñecidas son CVE (Common Vulnerabilities and Exposures), ou Exploit-DB.

O software especializado en Pentesting como Nessus ou OpenVAS utilizan estas bases de datos para facer tests automáticos que xeneran informes de vulnerabilidades.

Vulnerabilidades e Ameazas

Ameazas Físicas

As ameazas físicas son aquelas que atinxen aos elementos hardware, e poden deberse a accesos non autorizados, fallos no hardware, catástrofes naturais ou a simples accidentes.

Para minimizar os efectos de estas ameazas cando é posible se instalan os sistemas en ***centros de proceso de datos***, que son lugares especialmente deseñados para resistir catástrofes naturais (terremotos, incendios), con control do ambiente (humidade, temperatura) para minimizar os fallos de hardware, con sistemas de control de acceso físico (sistemas biométricos, sistemas de videovixilancia... etc) e sistemas redundantes (comunicacións, subministro eléctrico... etc).

Os fallos de hardware común como os dispositivos de rede, ou de almacenamento se palían cons sistemas de redundancia como sistemas de alimentación ininterrumpida (SAI), xeneradores autónomos, diversos proveedores de acceso a internet, sistemas RAID... etc.

Os ***Sistemas de Alimentación ininterrumpida*** pretenden evitar os cortes abruptos no servizo debidos a fallas na corrente eléctrica e protexer os sistemas das inestabilidades que podan provocar avarías. Cando se detecta unha caída do subministro eléctrico, manteñen os sistemas o tempo suficiente para realizar un apagado ordenado. Podemos distinguir varios tipos de SAI:

- ***Off-Line:*** Son os máis simples, e realmente non protexen das inestabilidades eléctricas, simplemente en caso de fallo de subministro dan un tempo para o apagado.
- ***Interactive***: Incorpora un filtro que permite en gran medida evitar as inestabilidades eléctricas. Sen embargo, o equipamento sensible aínda pode ser afectado. Son os recomendados para uso doméstico ou en equipos de usuario.
- ***Line-Interactive:*** Son os máis eficientes. O subministro eléctrico é completamente estable e sempre proven do SAI. O equipamento non percibirá as posibles inestabilidades eléctricas. Se emprega nos equipos servidores e nos CPD.

Os sistemas de RAID (*Redundant Array Of Independent Disks*) permiten protexer os sistemas da perda de información debida a falla do sistema de almacenamento gardando copias da información en diversos dispositivos e proporcionando ademais unha mellora na velocidade. Actualmente se empregan dous sistemas:

- ***Raid Hardware***: Se implementa o RAID mediante unha tarxeta controladora especial. O sistema únicamente verá un dispositivo de almacenamento, e a tarxeta se encarga de repartir as lecturas e escrituras entre os dispositivos reais.
- ***Raid Software***: Un software se encarga de xestionar os distintos dispositivos de modo que manteñan a redundancia e de amosar ao sistema un dispositivo especial que os agrupa.

Se poden empregar distintos modos de RAID. Os máis utilizados son:

- ***RAID 0:*** Non é realmente un modo de RAID, xa que non proporciona ningún tipo de protección, so un aumento da velocidade de lectura/escritura. Se coñece tamén como segmentación e consiste en repartir as lecturas e escrituras entre varios dispositivos, aumentando a velocidade e multiplicando a posibilidade de fallo. Un fallo en un dispositivo produce a perda total da información.

- ***RAID 1:*** Se coñece como espello ou “mirror” e consiste en copiar en varios dispositivos a mesma información, de xeito que si un falla, a información estará dispoñible no resto. Mellora a velocidade de lectura.
- ***RAID 5***: Necesita como mínimo 3 dispositivos, e consiste en gardar a información segmentada xunto con un cálculo de paridade que permitirá reconstruír a información en caso de fallo. Este modo pode sacar realmente partido do RAID hardware xa que liberaría a CPU do sistema de facer os cálculos dos datos de paridade. Se gaña velocidade tanto en lectura como en escritura.
- ***RAID 10***: Se emprega moito hoxe en día, aínda que non é un modo de RAID, se non unha mezcla de dous. Consiste en realizar un RAID 0 encima de dous RAID 1. Necesita como mínimo 4 dispositivos.

Os sistemas de bonding de rede consisten na agrupación de tarxetas de rede de xeito que proporcionen redundancia e segundo o modo, un aumento de velocidade. Existe un protocolo estándar (***802.3ad***) para esta práctica denominado ***LACP (Link Aggregation Control Protocol)*** que soportan os switches modernos. Algúns modos non requiren soporte dos switches. En Linux, o driver de bonding soporta os seguintes modos:

- **Active Backup**: So funciona un interfaz e o outro queda en reserva por si se da unha falla. NON precisa soporte do switch, e proporciona tolerancia a fallos.
- **Balance rr:** Os paquetes se van distribuíndo entre todos os enlaces. Necesita que os portos do switch estén nun grupo de agregación de enlaes. Proporciona aumento de velocidade e tolerancia a fallos.
- **Balance xor:** Realiza unha operación XOR coas MAC de orixe e destino para asignar o enlace da comunicación. Necesita que os portos do switch estén nun grupo de agregación de enlaces. Proporciona aumento de velocidade e tolerancia a fallos.
- **Broadcast:** Transmite por todas as tarxetas do grupo. Necesita que os portos do switch estén nun grupo de agregación de enlaces. Proporciona tolerancia a fallos.
- **802.3ad:** Transmite e recibe segundo as regras do protocolo 802.3ad que debe soportar o switch. Proporciona aumento de velocidade e tolerancia a fallos.
- **Balance tcp:** Se distribúe o tráfico de saida entre os enlaces, pero unha conexión so utilizará un único enlace. NON precisa configuración do switch. Proporciona aumento de velocidade de transmisión e tolerancia a fallos.
- **Balance alb:** Se distribúe o tráfico de saida e de entrada entre os enlaces, , pero unha conexión so utilizará un único enlace. NON precisa configuración do switch. Proporciona aumento de velocidade e tolerancia a fallos.

Ameazas Lóxicas

As ameazas lóxicas son as que atinxen ao software dos sistemas. Estas ameazas podemos clasificalas do seguinte modo:

Ameazas contra a seguridade no Acceso

É a ameaza de que persoas/sistemas sen autorización consigan acceso ao sistema. Para evitalo se recurre a mecanismos de autenticación e de autorización.

Os ***mecanismos de autenticación*** pretenden identificar a persoa/sistema que pretende realizar o acceso, mentres que os ***mecanismos de autorización*** regulan o grao de acceso que se lles concede.

As principais ameazas contra a seguridade de acceso son os ataques de forza bruta ás contrasinais, e a enxeñería social.

Ameazas contra a integridade do Sistema

É a ameaza de que se modifiquen arquivos do sistema que permitan ao atacante accesos en principio non permitidos. E típico de malware como os troianos ou rootkits.

Ameazas contra a privacidade

É a ameaza de que alguén poda obter información en principio restrinxida. Estas ameazas poden concretarse mediante ataques como MiM (Man In The Middle), sniffers de rede, keyloggers, Phishing de páxinas web... etc.

Ameazas contra a dispoñibilidade

É a ameaza de que alguén poda interrumpir o servizo dun sistema. Estas ameazas se concretan maioritariamente mediante ataques de rede levadas a cabo por *BotNets* (formadas por sistemas alleos que foron comprometidos e dos que os atacantes tomaron o control mediante instalación de sistemas de acceso remoto) denominadas DoS (Deny Of Service) (syn flood, Ping Of Death...).

Seguridade Física

A seguridade física é a que afecta aos dispositivos físicos dos sistemas (hardware).

Medidas de Seguridade Activas

As medidas de seguridade activas pretenden *evitar os fallos* de dispoñibilidade ou confidencialidade da información tomando medidas previas, que poden ser:

- Restricción de acceso físico a persoal non autorizados (videovixilancia, controis biométricos...)
- Ubicación dos equipos en zonas a salvo de inundacións, a proba de terremotos e con sistemas antiincendios
- Control do ambiente (temperatura/humidade) para minimizar os fallos de hardware

- Redundancia do subministro eléctrico, e fontes de alimentación de emerxencia (xeneradores)

Estes puntos se consiguen edificando centros especialmente deseñados con estes puntos en mente, denominados Centros de Proceso de Datos (CPD). Os servicios poden estar replicados en varios CPD para maior seguridade.

Outro tipo de medidas activas na seguridade física pasan pola redundancia, como os sistemas RAID, o Bonding de tarxetas de rede ou os SAI (baterías de respaldo).

Medidas de Seguridade Pasivas

As medidas de seguridades pasivas consisten en tomar as precaucións necesarias para recuperarse dun posible fallo. Medidas deste tipo son os Backups ou os sistemas de recuperación de arquivos.

Seguridade Lóxica

A seguridade Lóxica é a que afecta ao software dos sistemas. Podemos distinguir entre seguridade no acceso, integridade do sistema, aseguramento da dispoñibilidade e a confidencialidade.

Autorización e control de Acceso

O ***control de acceso*** aos sistemas utiliza dous pasos: *Identificación* e *Autenticación*. A *Identificación* consiste en que un usuario se da a coñecer ao sistema, e a *Autenticación* son os medios de verificación de identidade do usuario identificado.

O ideal, é que o usuario unicamente precise identificarse e autenticarse unha vez, de xeito que sucesivos accesos se realicen sen necesidade de facilitar de novo as credenciais, tanto no sistema no que se realizou a identificación e autenticación como nos sistemas asociados. Isto denomínase Single Login ou Single Sign On (SSO).

As ventaxas dos sistemas SSO radican en que como o usuario non ten que autenticarse tan a miudo e non precisa recordar múltiples contrasinais se reduce a posibilidade de que o usuario introduza o seu contrasinal onde non debe, a posibilidade da intercepción das contrasinais e se aforra o tempo perdido nas diversas autenticacións. Ademais, dende o punto de vista da administración do sistema, como SSO utiliza servidores de autenticación, se reduce o traballo xa que so e necesario configurar e asegurar un único equipo.

O principal inconveniente é que si se comprometen unhas credenciais de autenticación,se facilita o acceso a múltiples servizos e máquinas, o que fai necesario que para sistemas críticos se combine este tipo de control con outras medidas, como poden ser o uso de *smartcards* ou passwords de un so uso (OTP Tokens).

Hoxe en día é moi común o uso da autenticación en dous pasos, na que unha vez suministradas as credenciais se envía un “token” a que so o usuario pode consultar (por exemplo, mediante un SMS). O usuario debe completar a autenticación indicando ese token.

Probablemente o servicio máis común para SSO é Kerberos. O servidor Kerberos, unha vez que o usuario facilita as súas credenciais, facilita un “ticket kerberos” (TGT). Cando calqueira outra aplicación precisa autenticar ao usuario, utilizará o TGT para obter un “ticket de servicio” no servidor Kerberos, que asegurará a identidade do usuario e do servidor ao que se desexa acceder

(non repudio en destino). Active Directory de Windows é un sistema que emprega Kerberos como sistema de autenticación.

Outro sistema cun obxectivo similar de amplo uso na web é OpenID, que consiste no uso de Servidores de Identidade. Os servidores de identidade facilitan unha chave de identificación correspondente cun usuario previamente rexistrado e autenticado no Servidor de Identidade. Isto elimina a necesidade de rexistrarse en múltiples *sites* o que redunda nunha maior comodidade e seguridade.

A ***autorización*** consiste en determinar que accions ou a que información poden acceder os usuarios unha vez identificados. Existen dous modelos de autorización:

DAC (Discrectional Authorization Control): Se utilizan permisos establecidos polo administrador nos obxectos do sistema. O usuario pode acceder si os permisos indicados polo administrador o permiten. Exemplos deste tipo de control son os permisos sobre os arquivos e as ACL.

MAC (Mandatory Authorization Control): Se utilizan perfís de uso que se instalan no sistema. Os obxectos do sistema cumpren o establecido no seu perfil, aínda que dispoñan de privilexios superiores. Sistemas deste tipo son o MIC usado en Windows (Mandatory Integrity Control), e sistemas como AppArmor ou SELinux en Linux.

Nos sistemas con controis MAC habitualmente se debe primeiro obter permiso do perfil obrigatorio e logo cumprir cos permisos DAC establecidos.

A vantaxe do MAC é que as aplicacións que están funcionando con altos niveis de privilexio no sistema poden ter restrinxido o acceso ao mínimo necesario para o seu funcionamento mediante un perfil MAC, o que cumple co *principio de seguridade do mínimo privilexio (que establece que un sistema debe ter únicamente os privilexios mínimos para facer o seu traballo*). Deste xeito, un fallo de seguridade no software non comprometería todo o sistema.

Control da Integridade

O control de integridade pretende detectar cambios no sistema non desexados, particularmente en ficheiros do sistema críticos. Os sistemas teñen diversas utilidades que xeneran firmas para verificar que non se cambian.

Windows dispón dun sistema denominado System File Checker (SFC), que verifica a integridade das súas utilidades básicas.

Existen sistemas máis complexos como ***tripwire*** que monitorizan un conxunto flexible de ficheiros para notificar ao administrador das súas modificacións.

Privacidade

A privacidade se proporciona mediante criptografía. A privacidade dos arquivos mediante cifrado de arquivos ou disco (empregando cifrado simétrico), e a privacidade das comunicacións empregrando cifrado asimétrico de chave pública, que ademáis nos proporciona non repudio en destiño.

Dispoñibilidade

O aumento da dispoñibilidade se consigue mediante redundancia e protección contra ataques DoS. En canto a redundancia do procesamento se recorre a sistemas de clúster de alta dispoñibilidade na que varios servidores están capacitados para ofrecer o mesmo servizo, facilitando remprazos en casos de fallo.

A protección contra ataques DoS se consigue con configuracións axeitadas do firewall e establecendo perímetros de seguridade (DMZ).

Sistemas de Detección de Intrusos e UTM

Os sistemas de detección de Intrusos (SDI) son sistemas que monitorizan o funcionamento da rede en tempo real buscando comportamentos típicos de ataques a distintas vulnerabilidades dos sistemas. De xeito similar aos antivirus, os SDI incorporan "firmas" dos ataques máis comúns recoñecendo os patróns e notificando e/ou bloqueando o ataque.

As firmas se consiguen mediante sistemas especialmente preparados para ser atacados e examinar o método empregado (Honeypots).

Os UTM (Unified Threat Management) son sistemas que ademáis do SDI incorporan outras medidas de seguridade como antivirus, firewall, antispam .... etc.

A monitorización en tempo real require gran velocidade no procesamento dos paquetes de rede, e dispoñer das firmas de ataques actualizadas. Normalmente se mercan cunha subscripción anual que proporciona firmas actualizadas.

Existen tamén distribucións Software de UTM / SDI como Suricata ou Snort.

Auditoría e Plan de Seguridade

Cando unha empresa quere asegurar a súa estructura informática debe recurrir a unha auditoría de seguridade, esta auditoría debe revisar os sistemas e producir un documento cos puntos débiles a reforzar e as vulnerabilidades a tratar.

Os puntos máis importantes a cubrir son os seguintes:

- **Identificación de interlocutores e recollida de información** – Se identifica ao persoal responsable co que debemos tratar, e se recolle a información dos distintos sistemas e dos servizos que deben ofrecer, así como do ámbito organizativo da empresa.
- **Tests de vulnerabilidades** – Normalmente empregando ferramentas especializadas en pentesting (Nessus, Openvas) se realiza un exame dos servizos ofrecidos e das súas vulnerabilidades. Este punto é moi molesto na rede e consume moito tempo, polo que se debe elixir ben o momento en que se realiza. Se deben examinar os servizos tanto de forma remota como local.
- **Revisión de configuracións e da visiblidade externa** – A partir do informe xerado no test anterior revisamos as configuracións dos servicios
- **Xeración do informe de estado e de medidas a tomar**

Análise Forense

O análise forense e o estudio do sucedido nun sistema informático cando foi comprometido. A correcta realización dun análise forense ten implicacións legais, xa que as probas acadadas poden ser utilizadas en xuicio. Os pasos a realizar serían:

- Aseguramento da escena (para evitar modificacións no estado dos equipos) – Por exemplo, desconectando a rede.
- Determinar que equipos e con qué alcance se deben examinar. As evidencias volátiles (estado da RAM) se perden si se apaga o equipo, de xeito que é importante decidir si é necesario facer unha copia previa.
- Adquisición de datos – Se realizan imaxes dos discos, e si se estima oportuno da RAM do sistema.
- Análise de datos – Se examinan as copias obtidas, deixando os equipos orixinais sen cambios de modo que podan ser reexaminados por terceiros en caso necesario, e se examinan os “logs” do sistema.
- Informe de resultados

O RFC 3227 establece un estándar en manipulación de probas dixitais.