Tècniques d'auditories

PID_00239290

Rafael Estevan de Quesada

Temps mínim de dedicació recomanat: 7 hores

Universitat Oberta de Catalunya

Cap part d'aquesta publicació, incloent-hi el disseny general i la coberta, no pot ser copiada, reproduïda, emmagatzemada o transmesa de cap manera ni per cap mitjà, tant si és elèctric com químic, mecànic, òptic, de gravació, de fotocòpia o per altres mètodes, sense l'autorització prèvia per escrit dels titulars del copyright.

Índex

Introducció

En els mòduls anteriors, s'han tractat aspectes més generals del procés d'auditoria com ara les fases i els diversos marcs de treball que l'equip auditor pot prendre com a referència, etc. També és interessant destacar que hem partit de les auditories de certificació més formals, per centrar-nos després en les de primera part i de seguretat. En aquestes últimes, el client de l'auditoria és al mateix temps l'auditat, i l'abast es limita no a la totalitat de la gestió de la informació, sinó al tractament d'aquesta informació en sistemes informàtics en xarxa. És el que hem denominat *auditories tècniques de seguretat*.

Les auditories de seguretat, com s'ha dit en mòduls anteriors, tenen una casuística particular i, per tant, el conjunt de proves que s'han de fer són variades. És a dir, el tipus de proves d'auditoria que s'ha de fer han de ser diferents per a recopilar totes les proves d'auditoria que siguin rellevants i útils a l'hora d'obtenir una conclusió. Per tant, precisament per aquesta diversitat de situacions que s'han d'auditar, no és possible indicar *a priori* quina tècnica d'auditoria s'ha d'utilitzar en una assignació específica d'auditoria sense abans fer una anàlisi de l'abast i l'objectiu de l'auditoria. No obstant això, es pot constatar que les tècniques o eines a disposició de l'auditor es poden agrupar en diferents categories:

- Revisió de documentació.
- Entrevistes.
- Visites a instal·lacions de l'auditat i observació de l'operativa habitual.
- Proves tècniques sobre els sistemes d'informació i comunicacions.

A més, s'ha de tenir clar que l'elecció de les tècniques depèn de molts factors, com ara:

- Abast de l'auditoria.
- Recursos de què es disposa per a fer l'auditoria.
- Experiència de l'equip auditor.
- Sistemes d'informació que hi estan involucrats.
- Etc.

La decisió sobre les tècniques d'auditoria que s'han d'utilitzar queda reflectida en el pla d'auditoria. Aquest document reflecteix el pla de proves previst i hauria d'indicar el tipus de proves que es faran i sobre quin personal, documentació, instal·lació i sistema d'informació.

Pla d'auditoria

En el mòdul 3 ("Auditoria de seguretat tècnica") s'expliquen les diferents fases en què es descompon el procés i els documents que les acompanyen.

Finalment, cal destacar que les tècniques d'auditoria en sistemes d'informació estan més definides en un ampli nombre de llibres, articles tècnics (*whitepapers*) i llocs web (alguns inclosos en la bibliografia d'aquest curs), i és possible

aprofundir en el seu estudi previ molt més enllà del que es tractarà en aquest mòdul. Per tant, en aquest apartat s'aprofundirà més en tècniques aplicables a les auditories de xarxa i d'aplicacions, per la seva especial importància com a vehicle d'amenaces externes. Concretament, les tècniques que es revisaran en aquest mòdul estan alineades amb els mètodes que recull el document NIST-SP 800-53A *Guide for Assessing the Security Controls in Federal Information Systems* i el document *NIST-SP 800-115 Technical guide to information security testing and assessment*. En aquests documents, les tècniques que s'hi descriuen s'agrupen en tres categories: examinar (*examine*), entrevistar (*interview*) i provar (*test*). A més, els mètodes d'auditoria es classifiquen en aquest document a partir de tres nivells segons la profunditat (*depth*) i l'abast (*coverage*). Per a cadascun dels mètodes i els seus diferents nivells, es donen indicacions sobre les característiques de la prova que s'ha de fer, per la qual cosa és recomanable la revisió d'aquest document.

Encara que hi reflectirem algunes tècniques d'auditoria, especialment les més aplicades, hem de reconèixer que les tècniques d'auditoria (especialment, d'aspectes tècnics) són molt àmplies i és difícil recollir-les en un únic document. Igualment, un auditor de sistemes d'informació ha de ser conscient de la dificultat de dominar totes les tècniques d'auditoria, sobretot en un ambient professional tan canviant com el de les tecnologies de la informació i les comunicacions. Per tant, hem d'insistir que l'auditor haurà de millorar de manera contínua el seu domini sobre les diferents tècniques d'auditoria, i anar desenvolupant les seves pròpies eines d'ajuda a la realització de proves. A més, haurà de recórrer als experts que siguin necessaris, quan li sigui impossible afrontar l'assignació d'auditoria amb prou garanties d'èxit per falta de perícia tècnica.

Resumint, en aquest mòdul tractarem les diferents tècniques més comunes de què disposa un equip auditor per a construir el seu pla d'auditoria.

1. Revisió de la documentació

Tota auditoria contrasta la realitat d'una organització amb una normativa per a obtenir les seves conclusions. En els casos d'auditories de segones o terceres parts, aquesta normativa sempre és externa a les normes internes de l'organització auditada, ja sigui un plec de condicions o requeriments contractuals, en el primer cas, o un estàndard, en el segon. No obstant això, en les auditories de primera part, aquesta normativa pot ser tant externa com interna. L'objecte de l'auditoria és comprovar si els controls estan implantats d'acord amb les millores pràctiques del sector, i comprovar si s'han implantat com indica la documentació dels controls generada per l'auditat. Aquest últim punt fa que sigui necessari que l'auditor conegui la documentació interna rellevant per a l'abast de l'auditoria.

Per tant, un dels aspectes que l'auditor revisarà inicialment és el de les polítiques i altres normatives que se'n deriven, tant internes com externes a l'auditat, i que estiguin sota l'abast de l'auditoria.

D'altra banda, tampoc no podem oblidar que, de vegades, molts controls són implementats essencialment mitjançant un suport documental. És, per exemple, el cas dels aspectes relatius a la subcontractació de serveis de TI. Una part essencial de la seguretat en aquest tipus de controls és que hi hagi un contracte en què estiguin documentats aspectes com la manera com es fa el servei o la manera com es mesura el nivell de servei. Aquests contractes són coneguts com a *acords de nivell de servei* o *service level agreement* (SLA). Els acords de nivell de servei han d'indicar, mitjançant mètriques clarament establertes, els paràmetres per a poder mesurar la qualitat del servei que s'ofereix. Quan s'audita la implantació d'aquest control, s'ha d'examinar i revisar la documentació i s'ha de contrastar amb el contingut mínim exigible. Posteriorment, si la inspecció de la documentació ha estat satisfactòria, pot ser rellevant fer alguna entrevista per a corroborar algun altre aspecte, com la manera de fer el seguiment dels acords de nivell de servei.

La llista de la documentació que s'ha de revisar depèn directament dels controls de seguretat que cal comprovar. En aquest sentit, segons el tipus de control, hi haurà més o menys documentació a revisar, o fins i tot cap. En aquest últim cas, l'auditor ha de prendre com a referència els catàlegs de controls i determinar la manera com s'implementen respecte a un marc de referència.

Per a determinar quina documentació s'ha de revisar, és destacable l'aportació de la ISACA i l'ITG, IT Governance Institute (vegeu el mòdul 4). La ISACA i l'ITG, juntament amb el mateix catàleg COBIT[1], han publicat un manual amb les directrius per a la comprovació o auditoria[2] del grau de compliment del marc COBIT.

(1)Fins a la data d'elaboració d'aquest material, en la versió 5.

(2)*ITAF - IT Assurance Framework.*

Per a cadascun dels processos COBIT, es facilita unes directrius per a crear un programa d'avaluació i auditoria de cadascun d'aquests processos[3]. Dins d'aquestes directrius, les quals inclouen gran nombre de detalls, en certs punts es faciliten algunes llistes d'informació i documents que l'auditor ha de recopilar. Les directrius plantegen obtenir aquesta documentació mitjançant entrevistes amb el personal, però també es pot obtenir directament mitjançant l'organització. És a dir, l'auditor pot lliurar la llista de documents necessaris a l'organització perquè sigui aquesta la que recopili la informació i la faciliti a l'auditor. En aquest cas, s'observa la clara relació entre els dos tipus de proves: entrevistes (que es tractaran més endavant) i revisió de documentació.

(3)Si s'és membre de l'ISACA es pot obtenir en la URL: http://www.isaca.org/knowledge-center/research/pages/audit-assurance-programs.aspx

Posem, per exemple, el procés COBIT d'alt nivell, "**EDM03 Ensure Risk Optimization**". En aquest cas, la ISACA considera necessari comprovar l'existència i la idoneïtat de la llista de documentació següent:

EDM03.01:

- *Emerging risk, issues, and factors* (I),
- *Risk appetite guidance* (O),
- *Approved risk tolerance levels* (O),
- *Enterprise risk management principles* (I),
- *Evaluation of risk management activities* (O),

EDM03.02:

- *Aggregated risk profile, including status of risk management actions* (I)
- *Risk management policies* (O)
- *Key objectives to be monitored for risk management* (O)
- *Enterprise risk management (ERM) profiles and mitigation plans* (I)
- *Approved process for measuring risk management* (O)

EDM03.03:

- *Risk analysis results* (I)
- *Remedial actions to address risk management deviations* (O)
- *Opportunities for acceptance of greater risk* (I)
- *Risk management issues for the board* (O)
- *Results of third-party risk assessments* (I)
- *Risk analysis and risk profile reports for stakeholders* (I)

La llista es pot considerar força exhaustiva, però s'ha de prendre només com una referència, ja que podem considerar que hi ha documents que també serien rellevants, com per exemple: inventari de maquinari, inventari de programari complet (no únicament el de control d'accés), plànols d'arquitectura de sistemes i comunicacions, entre altres. L'important és tenir en compte que les directrius d'auditoria de la ISACA són únicament una orientació. L'experiència de l'equip auditor és essencial a l'hora de fer aquest tipus de proves. El coneixement de la manera més habitual en què les organitzacions implementen aquest tipus de controls determinarà la documentació que haurà de sol·licitar l'auditor. Igualment, al llarg de les revisions, aniran sorgint noves peticions de documentació per revisar.

El nivell de detall a què arribi l'auditor, a l'hora de revisar la documentació, dependrà de l'objectiu de la revisió o del tipus de documentació revisada. Per exemple, si la documentació forma part de la implementació d'un control, aquesta requerirà una revisió més a fons. L'auditor determinarà el nivell de profunditat o detall amb què farà la revisió en funció dels recursos de l'auditoria, l'objectiu de la revisió, el tipus de documentació, la documentació de suport a la implantació d'un control, etc. En tot cas, l'elecció del nivell de detall no ha de comprometre els objectius de l'auditoria.

2. Entrevistes

Per a comprovar la seguretat dels sistemes d'informació d'una determinada organització, l'auditor ha de fer proves d'auditoria que no estan relacionades amb aspectes purament tècnics, sinó més aviat organitzatius.

A manera d'exemple, si prenem com a referència els controls definits per la Norma ISO/IEC 27002 per al control d'accés, veurem que els aspectes tècnics tenen molt de pes. No obstant això, aquesta norma inclou també proves d'auditoria relacionades amb aspectes purament organitzatius, com per exemple: quina política de control d'accés existeix?, com i quan es comunica aquesta als usuaris?, amb quina freqüència i de quina manera es fan revisions de l'assignació de permisos?, a qui s'informa d'aquestes revisions?, hi ha proves de tot això? La revisió d'aspectes organitzatius s'ha d'afrontar amb proves no únicament tècniques, sinó també per mitjà de converses amb els responsables organitzatius.

La majoria de vegades, l'auditor haurà de sol·licitar als entrevistats un suport documental que evidenciï les afirmacions que es facin en l'entrevista. Altrament, com que no hi ha més prova que el resultat d'una entrevista, les conclusions d'auditoria seran més febles. En aquest cas, l'auditor considerarà la possibilitat de determinar que el control no està correctament implementat, ja que no hi ha cap prova suficient que ho demostri.

A continuació, repassarem les entrevistes, una de les tècniques d'auditoria més habituals.

2.1. Planificació de les entrevistes

Com qualsevol altra prova d'auditoria, les entrevistes s'han de planificar per endavant. La raó no és únicament d'ordre logístic o de coordinació d'agendes entre entrevistats i auditors, sinó que la planificació té per objecte ajustar els objectius de la prova que s'ha de fer.

Per a planificar correctament aquestes proves, s'ha de determinar:

- L'objectiu de l'entrevista. Les entrevistes s'han de planejar amb un objectiu clar i específic. Si aquest no és clar, el resultat de la prova serà insuficient. Per tant, s'ha de determinar què és el que es pretén obtenir o comprovar mitjançant l'entrevista.

- Els interlocutors més adequats. Segons l'objectiu, hi haurà diversos candidats a ser entrevistats. El nombre d'interlocutors pot ser ampli i, en aquests casos, serà necessari un mostreig d'interlocutors. Així mateix, tenir diversos interlocutors servirà per a obtenir punts de vista contrastables sobre una temàtica, sobretot en situacions en què no es disposa d'altres elements objectius o demostratius (per exemple, documents oficials).

- Tipus d'entrevista que s'ha de fer. Com veurem més endavant, hi ha la possibilitat de recollir la informació de maneres diferents: entrevistes sense guió, amb qüestionari, autoavaluacions, etc.

- Nombre d'entrevistes que s'han de fer. El nombre d'entrevistes depèn totalment dels recursos d'auditoria que s'hi dediquin, de l'abast de l'auditoria i de la modalitat de les entrevistes. En tot cas, s'ha de planificar un nombre d'entrevistes que asseguri que s'aconsegueixen els objectius d'auditoria.

Per a planificar les entrevistes necessàries, l'auditor ha de conèixer l'equip auditat i l'abast de l'auditoria. A més, l'auditor també es basarà en la seva pròpia experiència i el seu coneixement de les estructures organitzatives més usuals. Quant a això, poques metodologies indiquen quines entrevistes s'han de fer i qui són els interlocutors més adequats.

2.2. Selecció dels interlocutors

Respecte a la selecció dels interlocutors, és difícil determinar *a priori* quins seran els més adequats. Òbviament, se seleccionarà el personal més adequat tenint en compte:

- El nivell de responsabilitat en l'organització i l'àrea d'interès de l'auditoria.

- El grau de coneixement de l'àrea d'interès, encara que no hi tingui una responsabilitat.

- La participació en les activitats d'una àrea, encara que només sigui per la qualitat d'usuari. Els usuaris serviran per a contrastar o comprovar com es duen a terme certes activitats o accions.

A l'hora de seleccionar el personal que s'ha d'entrevistar, podem organitzar els interlocutors potencials en alguna de les categories següents:

- Direcció. La direcció determina els objectius de seguretat de l'organització i la seva alineació amb els objectius de negoci. Per tant, serà interessant entrevistar membres de la direcció (direcció de TIC, per exemple) per a determinar la manera com es gestionen els recursos dedicats a la seguretat dels sistemes d'informació.

- Àrea de seguretat. L'organització no està gaire conscienciada; el personal de l'àrea de seguretat acostuma a estar dedicat únicament a la seguretat física. D'altra banda, en organitzacions amb una conscienciació elevada en matèria de seguretat, aquest personal tindrà en compte totes les facetes de la seguretat de la informació. És habitual que l'assignació d'auditoria estigui gestionada des d'aquesta àrea i que el seu personal serveixi d'enllaç entre l'equip auditor i la resta de l'organització.

La participació de l'àrea de seguretat en les entrevistes serà intensa, ja que gran part de la gestió dels controls recaurà a les seves mans. Normalment, aquest personal és l'interlocutor adequat per a tractar els aspectes relacionats amb la seguretat física, almenys quant als controls d'accés, encara que aquests aspectes poden ser gestionats des d'una altra àrea de l'organització.

- Recursos humans i gestió d'usuaris. El procés de selecció, contractació i baixa del personal, i la seva relació amb la gestió de comptes d'usuari i assignació de recursos informàtics, té impacte sobre els controls d'accés tècnics que s'hi hagin implantat. Per això, en primer lloc, pot ser interessant tenir la visió de l'àrea de recursos humans per a comprovar la seva coordinació amb l'àrea de TI a l'hora de gestionar els comptes d'usuari. En segon lloc, pot ser interessant tenir la visió de l'àrea de TIC encarregada de gestionar l'alta, baixa o modificació dels drets d'accés d'usuari.
  Altres aspectes que també poden ser tractats amb recursos humans són els relatius a la formació i conscienciació dels usuaris, encara que pot ser que aquesta responsabilitat estigui repartida amb l'àrea de seguretat.

- Gestió de relacions amb contractistes externs. La gestió de certes parts dels sistemes d'informació pot estar externalitzada en contractistes externs (allotjament de sistemes, desenvolupaments, operació dels sistemes d'informació, etc.). Per això, és interessant verificar la selecció i el control del personal extern que accedeix als sistemes d'informació. A més, pot ser aconsellable verificar la manera com es defineixen els contractes, els nivells d'acord de servei (SLA, *service level agreement*), el seguiment i l'auditoria de les accions d'aquests externs.

- Sistemes d'informació centrals i comunicacions de dades. És necessari comptar amb el personal que s'encarrega dels sistemes d'informació centrals (servidors, aplicacions corporatives, serveis de correu electrònic, web, etc.), per a verificar la seguretat en la seva arquitectura, configuració, operació i manteniment. Amb aquest personal, també es poden verificar aspectes de la seguretat física relacionats amb la protecció de les condicions operatives dels sistemes d'informació (temperatura, humitat, alimentació elèctrica, control d'accés, etc.).
  També és possible que, en aquesta mateixa àrea, es trobin les activitats de desenvolupament de nous sistemes d'informació. Aquestes activitats també són rellevants en les auditories tècniques de seguretat i, per tant, el personal associat també serà candidat a ser entrevistat. És habitual que les tasques de desenvolupament de nous sistemes estiguin externalitzades, per la qual cosa s'haurà d'explicar de nou, en aquest cas, amb les àrees externes.
  - Sistemes de control de processos. En les organitzacions en què hi hagi un procés productiu controlat mitjançant sistemes d'informació, és rellevant tractar aspectes de seguretat com el control d'accés, la segregació de funcions, l'administració d'operacions, el manteniment, etc. Aquests processos productius no cal que siguin exclusivament indus-

trials; es podria tractar, per exemple, dels terminals financers usats pels empleats d'un banc.

– Infraestructures d'usuari. Entenem aquesta àrea com la relacionada amb la gestió dels equips de treball d'usuari (PC d'usuari, portàtils, telèfons intel·ligents o *smartphones*, PDA, etc.), incloent-hi també, si n'hi ha, el servei d'atenció a l'usuari (*helpdesk*). La seva rellevància per a les auditories tècniques rau tant en els controls aplicats en aquests sistemes com en els processos de suport a l'usuari, mentre que poden ser víctimes d'un atac d'enginyeria social.

– Gestió d'incidents i de recuperació davant desastres. En certes ocasions, les organitzacions disposen d'àrees dedicades a la gestió d'incidents i a garantir la continuïtat del negoci (equips de recuperació davant desastres, o de continuïtat). En aquestes organitzacions, la seguretat és un aspecte madur, i serà interessant la participació del personal d'aquesta àrea en les entrevistes.

Encara que totes les organitzacions no disposen d'unitats específicament dedicades a la gestió dels temes anteriors, sí que podem afirmar que totes aquestes àrees s'han de tenir en compte a l'hora de fer una auditoria tècnica de seguretat. Per tant, una de les tasques prèvies a la fase d'entrevistes serà identificar el personal adequat. Per a això, és necessari un coneixement sobre l'organització interna de l'entitat auditada, que pot ser que l'auditor no tingui. Quan l'auditor no tingui un coneixement previ suficient sobre l'organització, hi ha d'haver una persona a l'entitat auditada que serveixi d'enllaç i permeti resoldre aquest tipus de qüestions. Aquest enllaç ha de tenir:

- Bon coneixement sobre l'organització (unitats, funcions, àrees importants per al negoci, flux de la informació, etc.).
- Cert nivell de responsabilitat o autoritat en l'organització, per poder convocar els interlocutors adequats.

Podem afirmar que, si un auditor extern no compta amb la col·laboració d'una persona d'enllaç amb aquestes característiques, les tasques d'auditoria seran poc eficients. Això estarà motivat pel coneixement limitat de l'organització i l'escàs o nul poder de convocatòria.

Per a fer la selecció d'interlocutors, és destacable de nou l'aportació de la ISACA i l'ITG. En la mateixa definició dels controls COBIT, a partir de la versió 4, s'ha definit un diagrama RACI per a cada procés. Aquest diagrama recull les diferents tasques o activitats d'un control i les relaciona amb cadascuna de les àrees d'una organització, assignant a cada àrea un tipus de responsabilitat:

- ***R**esponsable*. Responsable de fer-ho.
- ***A**ccountable*. Responsable funcional que es faci l'activitat, és a dir, qui ret comptes davant els seus superiors.

- *Consulted*. Consultat.
- *Informed*. Informat.

Procés de control DS-5 - Garantir la seguretat dels sistemes

Prenguem, per exemple, dins del domini DSS (*delivery, service and support*, lliurament de serveis, operació de servei i suport), el procés de control DSS-05: Gestionar els serveis de seguretat. Aquest procés inclou diverses activitats clarament rellevants quan s'està fent una auditoria tècnica de seguretat:

- DSS05.01: Protegir contra programari maliciós (*malware*)
- DSS05.02: Gestionar la seguretat de la xarxa i les connexions
- DSS05.03: Gestionar la seguretat dels llocs d'usuari final
- DSS05.04: Gestionar la identitat de l'usuari i l'accés lògic
- DSS05.05: Gestionar l'accés físic als actius de TI
- DSS05.06: Gestionar documents sensibles i dispositius de sortida
- DSS05.07: Supervisar la infraestructura per detectar esdeveniments relacionats amb la seguretat

El diagrama RACI d'aquest procés és el següent:

Matriu RACI DSS05

Pràctica Clau de Govern	Consell d'administració	Director General Executiu (CEO)	Director General Financer (CFO)	Director d'Operacions (COO)	Executius de negoci	Propietaris dels procesos de negoci	Comitè Executiu Estratègic	Comitè Estratègic (Desenvolupament de projectes)	Oficina de Gestió de Projectes	Oficina de Gestió del Valor	Director de Riscos (CRO)	Director de Seguretat de la Informació (CISO)	Consell d'Arquitectura de l'Empresa	Comitè de Riscos Corporatius	Cap de Recursos Humans	Compliment Normatiu (*Compliance*)	Auditoria	Director d'Informàtica /Sistemes	Cap d'Arquitectura del Negoci	Cap de Desenvolupament	Cap d'Operacions TU	Cap d'Administració TU	Gestor de Serveis (*Service Manager*)	Gestor de Seguretat de la Informació	Gestor de Continuïtat de Negoci	Gestor de Privadesa de la Informació
DSS05.01 Protegir contra programari maliciós (*malware*).						R	I				C	A			R	C	C	C	I	R	R		I	R		
DSS05.02 Gestionar la seguretat de la xarxa i les connexions.						I					C	A				C	C	C	I	R	R		I	R		
DSS05.03 Gestionar la seguretat dels llocs d'usuari final.						I					C	A				C	C	C	I	R	R		I	R		
DSS05.04 Gestionar la identitat de l'usuari i l'accés lògic.						R					C	A			I	C	C	C	I	C	R		I	R		C

Diagrama RACI del procés COBIT 5 - DSS05

Font: ISACA - COBITS

Pràctica Clau de Govern	Consell d'administració	Director General Executiu (CEO)	Director General Financer (CFO)	Director d'Operacions (COO)	Executius de negoci	Propietaris dels procesos de negoci	Comitè Executiu Estratègic	Comitè Estratègic (Desenvolupament de projectes)	Oficina de Gestió de Projectes	Oficina de Gestió del Valor	Director de Riscos (CRO)	Director de Seguretat de la Informació (CISO)	Consell d'Arquitectura de l'Empresa	Comitè de Riscos Corporatius	Cap de Recursos Humans	Compliment Normatiu (*Compliance*)	Auditoria	Director d'Informàtica /Sistemes	Cap d'Arquitectura del Negoci	Cap de Desenvolupament	Cap d'Operacions TU	Cap d'Administració TU	Gestor de Serveis (*Service Manager*)	Gestor de Seguretat de la Informació	Gestor de Continuïtat de Negoci	Gestor de Privadesa de la Informació
DSS05.05 Gestionar l'accés físic als actius de TU.						I					C	A				C	C	C	I	C	R		I	R	I	
DSS05.06 Gestionar documents sensibles i dispositius de sortida.											I					C	C	A			R					
DSS05.07 Supervisar la infraestructura per detectar esdeveniments relacionats amb la seguretat.				I		C					I	A				C	C	C	I	C	R		I	R	I	I

Diagrama RACI del procés COBIT 5 - DSS05

Font: ISACA - COBITS

A partir d'aquest diagrama, podem identificar fàcilment uns quants candidats a ser entrevistats per al grau d'implantació dels controls inclosos en aquest procés.

D'altra banda, les directrius d'auditoria també proporcionen guies sobre com s'ha d'avaluar la implantació dels processos de control de COBIT i, a més, es faciliten indicacions sobre quins interlocutors s'han d'entrevistar.

Tornant al nostre exemple, les directrius d'auditoria d'ISACA indiquen que, per a comprovar el procés de control DS.5, es recomana entrevistar:

- Els propietaris dels processos de negoci
- Oficial de seguretat sènior de l'organització (màxim responsable de la gestió de la seguretat en l'organització).
- Direcció de recursos humans
- Direcció d'IT
- Responsable/s de desenvolupament
- Responsable/s d'operacions d'IT
- Personal rellevant en la direcció de la gestió de la seguretat de TI.
- Personal rellevant administrador de bases de dades de TI.
- Personal rellevant administrador tècnic de la seguretat de TI.

- Personal rellevant en la direcció del desenvolupament d'aplicacions de TI.

A més, aquesta mateixa metodologia indica els objectius de les entrevistes i la informació que s'ha de recaptar d'aquest conjunt d'interlocutors. A partir d'aquí, el pas següent de l'auditor és definir els diferents tipus d'entrevistes i el contingut dels qüestionaris.

2.3. Tipus d'entrevista

De manera bàsica, podem catalogar les entrevistes en funció del tipus de qüestionari que s'utilitzi:

- Qüestionaris oberts, guiats pel mateix auditor.
- Qüestionaris tancats.
- Qüestionaris d'autoavaluació.

Evidentment, l'ús d'un tipus de qüestionari o un altre dependrà de la capacitat de l'auditor i, en gran manera, dels recursos d'auditoria de què es disposi (nombre d'auditors, coneixements i marc temporal). La qualitat dels resultats obtinguts pot variar de manera notable en funció del tipus escollit. Novament, l'equip auditor ha de sospesar els pros i els contres, valorar-ne les capacitats i, a partir d'aquí, determinar el tipus d'entrevistes.

2.3.1. Qüestionaris oberts

El primer tipus d'entrevistes són aquelles en què es conversa obertament amb l'auditat. En aquests casos, els resultats de l'entrevista dependran de l'habilitat i de l'experiència de l'auditor per a anar guiant la conversa cap als aspectes més rellevants. Un auditor amb experiència pot obtenir millors resultats amb una entrevista guiada que amb altres tipus d'entrevistes.

Com que es tracta d'una entrevista no dirigida mitjançant un qüestionari tancat, tant l'auditor com l'auditat tenen la llibertat d'aprofundir en els aspectes que, al llarg de la prova, es considerin més interessants. No obstant això, l'auditor no ha d'oblidar l'objectiu de la prova i, per tant, haurà d'organitzar mínimament el pla de l'entrevista per a assegurar-se que s'hi tracten els punts que interessen.

2.3.2. Qüestionaris tancats

Qüestionaris tancats. Aquestes entrevistes són l'evolució natural d'una tasca d'auditoria eficient. L'equip auditor pot preparar prèviament el detall de les qüestions que s'hi han de tractar si coneix bé quin és l'objectiu de la prova.

En aquest tipus d'entrevistes, l'auditor ha de ser prou flexible per a poder explorar aspectes que quedin fora del contingut del seu qüestionari. Al cap i a la fi, es tracta d'una prova en què l'auditat proporciona la informació rellevant, i

és possible que no es puguin obtenir les proves desitjades mitjançant un qüestionari absolutament tancat. D'altra banda, aquest tipus de proves les pot fer personal auditor amb poca experiència.

En qualsevol dels dos casos, l'equip auditor no ha d'oblidar en cap moment que la prova té com a objecte el descobriment de proves d'auditoria rellevants. En cap cas, les entrevistes no han de prendre un caràcter acusador o comprometedor per a l'entrevistat. Sempre s'ha de mantenir un bon grau de col·laboració perquè la informació recollida sigui confiable. D'altra banda, sempre que sigui possible, l'auditor haurà d'obtenir proves que corroborin el que ha exposat l'entrevistat. En cas contrari, l'única prova la constituirà el mateix contingut de l'entrevista. Això últim és el motiu pel qual es recomana elaborar actes de totes les reunions, i mantenir-les com a prova.

2.3.3. Desenvolupament de les entrevistes

De manera general, el desenvolupament d'una entrevista de qualsevol dels tipus seria:

- Preparar la reunió:
  - Si es tracta d'una entrevista amb un qüestionari tancat, preparar el qüestionari o seleccionar-lo si és que se'n disposa prèviament.
  - Preparar una agenda dels punts que s'han de tractar a grans trets i el temps estimat de durada (es recomana no excedir l'hora, o dues hores com a màxim).

- Comunicar l'agenda a l'auditat i concertar els aspectes logístics de l'entrevista.

- Fer l'entrevista prenent nota de tot el que s'hi ha desenvolupat i recollir tota la informació que l'auditat pugui proporcionar. És interessant subratllar que hi ha la possibilitat de gravar el contingut de l'entrevista. Sol ser molt poc habitual i, en tot cas, sempre haurà d'estar explícitament declarat i acordat amb anterioritat i reflectit en el pla d'auditoria i en l'acord de confidencialitat signat entre auditor i auditat, indicant la finalitat i el tractament que es donarà a aquests continguts d'àudio o vídeo. Igualment, en l'actualitat hi ha mitjans tècnics per tal que les entrevistes no hagin de ser realitzades de manera presencial, emprant recursos tecnològics de videoconferència. Aquests mitjans permeten, a més de la reunió remota, compartir recursos informàtics, realitzar demostracions, revisions o consultes de documents ofimàtics durant la reunió i, en alguns casos, enregistrar la sessió. Aquests enregistraments han de ser tractats de la mateixa manera que els enregistraments d'àudio comentats anteriorment.

- Elaborar una acta i obtenir l'aprovació documentada de l'entrevistat.

2.4. Qüestionaris d'autoavaluació

És interessant observar que, en el cas d'utilitzar qüestionaris tancats, hi ha la possibilitat de preparar el contingut de l'entrevista de tal manera que aquesta pugui ser resposta autònomament per l'entrevistat.

Els qüestionaris d'autoavaluació es poden utilitzar si l'equip auditor coneix bé quin és l'objectiu de la prova, pot preparar prèviament el detall de totes les qüestions que s'hi han de tractar, i pot preparar la forma de recollida de la informació. D'aquesta manera, es fan més proves simultàniament amb menys recursos d'auditoria. No obstant això, s'han de contrastar els resultats dels qüestionaris per a garantir la qualitat de la informació recollida. Per tant, és responsabilitat de l'auditor determinar l'ús o no d'aquest tipus de proves, documentar les raons que en possibiliten l'ús i descriure la manera com es desenvoluparà la prova.

És interessant apuntar que, en la comunitat auditora de sistemes d'informació, hi ha qüestionaris d'autoavaluació per a diferents temàtiques. Per exemple, cal destacar el SANS Institute que facilitava un qüestionari d'autocomprovació del nivell d'implantació dels controls de les normes ISO/IEC 27002, però de la seva versió de 2005. Ara per ara no ha estat actualitzat, però és una bona referència per a aquest tipus de documents. No obstant això, l'equip auditor ha de conèixer i estudiar molt bé aquestes eines abans d'aplicar-les de manera directa. Es requereix un estudi previ i una adaptació a les necessitats de l'assignació d'auditoria, i sempre és desitjable que l'equip auditor prepari els seus propis qüestionaris segons la seva experiència.

D'altra banda, s'ha de tenir en compte que, en algunes circumstàncies, les organitzacions auditores no permeten l'ús d'aquesta tècnica. Això és a causa del fet que la part auditada pot ser que no tignui prou independència a l'hora de respondre certes qüestions, i l'auditor no té la possibilitat de fer un altre tipus de preguntes per a contrastar la veracitat de la resposta. Per tant, aquesta tècnica pot anar en contra dels principis d'auditoria de cura professional adequada o de conducta ètica.

Cal esmentar que diferents organitzacions han preparat qüestionaris perquè les entitats puguin fer un exercici d'autoavaluació propi. Aquest exercici pot tenir validesa de manera interna a l'organització. En altres ocasions, les organitzacions auditores han emprat aquests qüestionaris com un element per a la promoció de la tasca d'auditoria, com a suport a la funció d'auditoria interna, i també com a eina per a millorar la conscienciació en matèria de seguretat de la informació.

2.4.1. Qüestionaris d'autoavaluació del PCI Security Standards Council

En aquest apartat, veurem un exemple d'aplicació dels qüestionaris d'autoavaluació en l'auditoria de sistemes d'informació en entitats que estan subjectes al compliment del PCI DSS.

Vegeu també

Aquest tema es tracta en el mòdul 4.

El PCI DSS Council ha obert recentment (des del 2008) la possibilitat que les auditories de PCI es facin de manera interna, mitjançant l'emplenament d'un qüestionari d'autoavaluació. D'aquesta manera, els comerços (denominats *merchants*) i proveïdors de servei que hagin estat autoritzats pels emissors de targetes (les grans corporacions de la indústria de les targetes de crèdit) no necessitaran fer una auditoria de compliment del PCI DSS *in situ* a les seves instal·lacions; podran fer l'avaluació ells mateixos. Tot i que és possible que aquests qüestionaris siguin seguits i completats pel mateix auditat, el PCI DSS Council recomana que es compti amb l'assistència d'assessors, per la qual cosa la tasca d'un auditor també pot ser requerida en aquests casos. Juntament amb el resultat de l'exercici d'autoavaluació, l'entitat autoauditada ha d'emplenar una declaració de compliment (anomenat *AoC - Attestation of Compliance*). Aquest document s'haurà de facilitar a altres entitats que, legítimament, li puguin exigir el compliment amb l'estàndard PCI DSS.

Hi ha diferents tipus de documents relacionats amb el mercat de les targetes de crèdit per a realizar les auditories. Entre aquests, trobem els denominats *PCI SSC self-assessment questionnaire* (SAQ). El PCI-SS Council ha identificat que, al llarg de la vida de l'estàndard, hi ha diverses situacions en els *merchants* i també en els proveïdors de serveis. Per aquesta raó, hi ha diversos tipus de qüestionaris SAQ, els quals es corresponen amb els diferents tipus de participants en el mercat i el tractament que aquests fan amb les dades de les targetes. Cada entitat que estigui obligada al compliment del PCI DSS haurà de determinar si és elegible per a fer l'exercici SAQ. En cas afirmatiu, l'entitat haurà d'emplenar el qüestionari i el document de declaració de compliment. Sempre és recomanable adreçar-se al lloc oficial de PCI-SS Council (en la seva secció de documentació) i revisar les últimes directrius publicades i els diferents tipus de SAQ existents, així com comptar amb un assessor PCI que ajudi a determinar quin és el més adequat per a l'activitat que es realitza. Fins a la data de publicació d'aquest material, s'han definit vuit tipus diferents:

1) A - Comerços que han delegat totes les funcions relacionades amb targetes de pagament en un tercer validat per la PCI DSS, de manera que el comerç en qüestió únicament emmagatzema informes o rebuts en paper amb dades de targetes. És a dir, tots aquells que gestionen transaccions no presencials (comerç electrònic i/o pagaments per telèfon o correu) i que no emmagatzemen, processen o transmeten cap dada de targeta de pagament en format electrònic en els seus sistemes o instal·lacions. No és aplicable als canals presencials.

2) A-EP - Aplicables a organitzacions que utilitzen el comerç electrònic com a canal de pagament i el seu lloc web no rep dades de targetes de pagament, però pot afectar la seguretat de la transacció i/o la integritat de la pàgina que accepta les dades de targeta de pagament provinents del client. És a dir, aquells comerços que han delegat de forma parcial el seu canal de pagament via comerç electrònic a un tercer certificat per la PCI DSS i que, en els seus sistemes o instal·lacions, no emmagatzemen de forma electrònica, processen o transmeten cap dada de targeta de pagament. És únicament per a entitats que fan comerç electrònic.

3) B - Aplica a comerços que processen dades de targetes de pagament únicament per mitjà de màquines impressores o terminals independents que connecten via telefònica (no connectada a xarxes de dades) per fer les operacions de validació. Poden ser comerços que processin transaccions presencials o pagaments per telèfon o correu (targeta no present) i que no emmagatzemin dades de targetes de pagament en cap sistema informàtic. No és aplicable a comerç electrònic.

4) B-IP - Aplica a comerços com els anteriors, però en aquests casos el terminal de punt de venda validat per la PCI-DSS connecta a través de tecnologies IP. Tampoc no és vàlid per a comerç electrònic.

5) C - Comerços amb aplicació de pagament (per exemple, un sistema de punt de venda) connectada a Internet (per exemple, mitjançant DSL, cable mòdem, etc). Els comerços que reportin el compliment utilitzant el SAQ C certifiquen que processen dades de targeta de pagament emprant un terminal de punt de venda (TPV/POS) o altres sistemes d'aplicació per a pagaments connectats a Internet. Poden ser comerços que processin transaccions presencials o pagaments per telèfon o correu (targeta no present) i que no emmagatzemin dades de targetes de pagament en cap sistema informàtic.

6) C-VT - Aplica a comerços que introdueixen les dades, transacció a transacció, en una aplicació via Internet facilitada per un tercer proveïdor validat per la PCI DSS, i no emmagatzemen les dades de la targeta. Tampoc no és vàlid per a comerç electrònic.

7) P2PE - Comerços que estan emprant terminals de pagament de maquinari inclosos i gestionats per un proveïdor certificat P2PE, sense emmagatzematge electrònic de dades de targetes de pagament.

8) D - Dins d'aquest tipus es distingeix:

- D - *Merchant*: comerços elegibles que no concorden amb cap dels criteris d'elecció descrits en els anteriors tipus de SAQ.

- D - *Service Provider*: proveïdors de servei definits per les marques de pagament com a elegibles per reportar el seu compliment emprant un SAQ.

A continuació, es presenten de manera resumida les preguntes més específiques d'auditoria incloses en el qüestionari (preses del SAQ-D Merchant). Com es pot observar, algunes preguntes poden tenir un caràcter més tècnic i altres més organitzatiu. D'altra banda, algunes preguntes són més senzilles de respondre que unes altres, encara que requereixin algun tipus de comprovació tècnica. Les preguntes més difícils requereixen un coneixement de la Norma PCI DSS, de la seva interpretació i de la seva implementació. La taula següent mostra preguntes amb un caràcter tècnic.

Requisit 1: Instal·lar i mantenir una configuració de tallafoc per protegir les dades

Pregunta de les PCI DSS		Proves esperades	Resposta *(marqui únicament una resposta per a cada pregunta)*				
			Sí	Sí amb CCW	No	N/C	No provat
1.1	Estan les normes de configuració del tallafoc i de l'encaminador establertes i implementades per incloure el següent?						
1.1.1	Existeix un procés formal per aprovar i provar tots els canvis i les connexions externes de xarxa en les configuracions dels tallafocs i els encaminadors?	· Revisar el procés documentat · Entrevistar al personal · Examinar les configuracions de xarxa	☐	☐	☐	☐	☐
1.1.2	(a) Existeix un diagrama de xarxa actual que documenti totes les connexions entre l'entorn de les dades de titulars de targetes i altres xarxes, fins i tot qualsevol xarxa sense fil?	· Revisar el diagrama de xarxa actual · Examinar les configuracions de xarxa	☐	☐	☐	☐	☐
	(b) Hi ha un procés implementat per assegurar que es mantingui actualitzat el diagrama?	· Entrevistar al personal a càrrec	☐	☐	☐	☐	☐
1.1.3	(a) Existeix un diagrama actual que mostri tots els fluxos de dades de titulars de targetes entre els sistemes i les xarxes?	· Revisar el diagrama de flux de dades actual · Examinar les configuracions de xarxa	☐	☐	☐	☐	☐
	(b) Hi ha un procés implementat per assegura que es mantingui actualitzat el diagrama?	· Entrevistar al personal	☐	☐	☐	☐	☐

Preguntes del PCI DSS SAQ - D per al requisit 1

La taula següent mostra preguntes amb un caràcter més organitzatiu:

Requisit 12: Mantenir una política que abordi la seguretat de la informació per a tot el personal.

Nota: A les finalitats del Requisit 12, «personal» es refereix a personal a temps complet i parcial, personal temporal, i contractistes i consultors que «residеixin» en les instal·lacions de l'entitat o que tinguin accés a l'entorn de dades dels titulars de targetes en l'empresa.

Pregunta de les PCI DSS		Proves esperades	Resposta *(marqui únicament una resposta per a cada pregunta)*				
			Sí	Sí amb CCW	No	N/C	No provat
12.1	Existeix una política de seguretat establerta, publicada, mantinguda i divulgada a tot el personal pertinent?	· Revisar la política de seguretat d'informació	☐	☐	☐	☐	☐
1.1.1	Es revisa la política de seguretat, com a mínim, una vegada a l'any i s'actualitza quan es realitzen canvis en l'entorn?	· Revisar la política de seguretat d'informació · Entrevistar al personal a càrrec	☐	☐	☐	☐	☐
1.1.2	a) S'implementa un procés anual d'avaluació de riscos que · identifiqui actius crítics, amenaces i vulnerabilitats? · Dóna lloc a una anàlisi formal i documentada del risc? Els exemples de metodologies d'avaluació de riscos inclouen, entre d'altres, OCTAVE, ISO 27005 i NIST SP 800-30.	· Revisar el procés d'avaluació de riscos anual · Entrevistar al personal	☐	☐	☐	☐	☐
	(b) El procés d'avaluació de risc es realitza, al menys, una vegada a l'any i després d'implementar canvis significatius en l'entorn (per exemple, adquisicions, fusions o reubicacions, etc.)?	· Revisar la documentació d'avaluació de risc · Entrevistar al personal a càrrec	☐	☐	☐	☐	☐

Preguntes del PCI DSS SAQ - D per al requisit 12

En alguns casos, a més de l'exercici d'autoavaluació, s'exigeix algun tipus d'auditoria tècnica de vulnerabilitats d'un tercer.

En cas que hi sigui aplicable el tipus de qüestionari D, s'està obligat a sol·licitar una anàlisi de vulnerabilitat dels sistemes intervinents en el processament de les dades de les targetes de crèdit. Aquesta anàlisi s'ha de sol·licitar a un proveïdor d'escaneig de vulnerabilitats aprovat pel PCI DSS Council. Per tant, en el cas de les auditories de compliment de PCI DSS, podem dir que les entitats estan autoritzades oficialment a fer auditories internes amb validesa com a auditories de terceres parts. No obstant això, aquest és un cas poc habitual.

3. Visites d'auditoria

Una altra faceta de les proves d'auditoria que no comporta un gran component tècnic són les visites d'auditoria. A més de les visites pertinents i necessàries per al desenvolupament d'entrevistes o execucions de proves tècniques sobre sistemes TIC, l'auditor pot fer també visites d'auditoria per observar directament circumstàncies físiques rellevants en diferents dependències de la instal·lació de l'auditat (per exemple, CPD), o comprovar la manera de treballar del personal. És habitual també que, en aquest tipus de visites en què s'observa el personal en les seves tasques professionals, es facin entrevistes breus per tal d'aclarir aspectes observats o sol·licitar algun tipus de demostració; de la mateixa manera que en el cas de les entrevistes, quan l'auditor fa visites d'auditories, també utilitza una llista de comprovacions preparades amb antelació.

Eludint el fet que les visites a les instal·lacions de l'auditat són necessàries per a la realització d'altres proves (entrevistes, execució de proves tècniques, etc.), l'objectiu d'aquestes visites pot incloure:

- **Proves de compliment de controls**. Es tracta de revisar la implantació real i efectiva de controls que afecten aspectes tècnics de les instal·lacions del client:
  - Controls d'accés físic a les instal·lacions.
  - Condicions de les sales de processament de dades o centres de càlcul, tenint en compte el control d'accés, la protecció contra incendis, la protecció del subministrament elèctric, alarmes, etc. Així mateix, la revisió de les mesures de protecció d'altres elements de la infraestructura de TIC, com ara el cablatge estructurat de l'edifici.
  - Seguiment per part dels empleats de les normatives de seguretat.
  - Execució dels procediments operatius que s'hagin descrit en relació amb l'operació, la gestió i el manteniment dels sistemes d'informació i comunicacions.

    Les proves de compliment de controls consistiran en una combinació de visites (que poden ser guiades o no) en què l'auditor es desplaçarà lliurement per les instal·lacions, prenent anotacions i fent entrevistes breus amb el personal.

    La política de taules netes, o l'ús correcte dels mecanismes d'identificació de persones, etc.

- **Complementar auditories tècniques**. Les visites d'auditoria poden tenir també per objectiu detectar i evidenciar problemes o vulnerabilitats en els processos organitzatius. Aquestes visites faran especial recalcament en els

problemes relacionats amb l'accés físic i la introducció d'equipament no autoritzat en instal·lacions tècniques (les sales de processament de dades, però també les instal·lacions d'usuari). D'altra banda, la realització de certes proves tècniques requerirà també visitar les instal·lacions de l'auditat i treballar des d'aquestes.

- **Complementar aspectes tractats en una entrevista**. Complementar aspectes tractats en una entrevista. L'entrevista proporciona a l'auditor un enteniment ràpid d'una situació determinada. No obstant això, la informació que s'obté pot estar esbiaixada, ja que l'interlocutor pot estar involucrat en el fet en qüestió. Així mateix, és possible que s'hagin emprat qüestionaris per a agilitar el procés d'auditoria, però que la informació obtinguda a partir d'aquests sigui parcialment errònia. Això pot passar per errors involuntaris o per l'ocultació intencionada d'alguns elements desfavorables per a l'auditat.
  Per a reduir el risc d'obtenir una informació equivocada, hi ha la possibilitat de fer una segona ronda d'entrevistes. Aquestes requeriran menys esforç que el necessari en una primera ronda, i permetran comprovar punts que no han quedat clars.
  En tot cas, és necessari contrastar els aspectes declarats pels interlocutors en visites i inspeccions. Això permet corroborar i confirmar la informació obtinguda amb proves més objectives (per exemple, registres de funcionament, actes, documents signats, etc.). Aquestes proves es poden considerar constatacions d'auditoria.

En resum, podem afirmar que les visites d'auditoria són una tècnica complementària de les entrevistes que permet inspeccionar de manera efectiva la manera com s'executen i s'organitzen certes tasques.

Les característiques, en termes de suficiència, validesa, confiabilitat i rellevància de les proves que s'obtinguin, a partir d'una visita d'auditoria, dependran del grau de detall amb què es faci la visita. En aquest sentit, podem distingir tres nivells de visites:

- Proves d'observació. Consisteixen en l'observació de l'execució d'una activitat, d'un procés o d'una implantació d'un control (en oposició a la lectura de la documentació sobre el control produïda per la mateixa organització auditada). Aquesta prova té per objectiu determinar si l'activitat o el control funciona segons el previst (o es configura segons el previst), i si hi ha errors, omissions o inconsistències en l'operació o configuració.

- Proves d'inspecció. Aquest tipus de prova complementa la prova d'observació amb una investigació activa per a obtenir altres arguments, amb l'objectiu de millorar la confiança en la conclusió. Aquest tipus de prova implica l'obtenció de proves més objectives que les simples observacions de l'auditor.

- Proves d'anàlisi. Com a complement final de les proves d'inspecció i observació, aquesta prova inclou l'anàlisi acurada i detallada de la informació recopilada durant la inspecció. L'objectiu és novament millorar la confiança en les conclusions. Les proves d'anàlisi es fan mitjançant un procés realimentat d'inspecció, observació i anàlisi dels resultats, fins a obtenir proves vàlides com a constatació d'auditoria.

L'esforç requerit per l'equip auditor serà més gran com més minuciosa sigui la revisió que es faci en la visita. Per tant, l'elecció del tipus d'activitats que cal dur a terme serà una decisió de l'auditor en cap, que ha d'estar reflectida en el seu informe. Encara que estigui basada en aspectes d'eficiència econòmica, aquesta decisió no ha de comprometre la consecució de l'objectiu de l'auditoria segons els nivells de qualitat i professionalitat exigibles.

4. Proves tècniques de sistemes d'informació i comunicacions

Finalment, en aquesta secció tractarem les tècniques d'auditoria que tenen un component més tècnic i que s'apliquen sobre els sistemes d'informació. Fins ara, les tècniques que s'han repassat permeten avaluar l'eficàcia de controls amb un component més organitzatiu. S'hi han tractat controls relacionats amb polítiques, normes i processos aplicats per a controlar especialment la manera com s'operen, es gestionen i es mantenen els sistemes de TIC. No obstant això, gran part d'aquests controls té una part de la seva implementació purament tècnica. Aquí és on entra, per tant, l'auditoria tècnica dels sistemes de TIC.

El conjunt de proves associat a una auditoria tècnica és molt heterogeni, ja que inclou tota acció que impliqui l'execució d'alguna comprovació sobre algun tipus de sistema tècnic del control de seguretat.

D'altra banda, és interessant constatar que, de vegades, les organitzacions sol·liciten als auditors aquest tipus de proves sense emmarcar-les, específicament, en un programa d'auditoria d'un SGSI. Les proves se solen limitar a infraestructures exposades a Internet, o a xarxes corporatives molt grans, i tenen com a objectiu determinar la seva seguretat i la manera com estan preparades per a afrontar atacs externs.

4.1. Auditoria dels mecanismes de control de riscos físics

La majoria de les proves tècniques es fan sobre els sistemes d'informació i comunicacions. No obstant això, si els recursos d'una auditoria o el seu objectiu ho justifiquen, també s'hi poden incloure proves tècniques sobre sistemes com:

- Mecanismes de control d'accés físic.

  Barreres d'accés, sistemes d'obertura dels accessos físics, mecanismes per a la traçabilitat dels accessos (càmeres, registres d'activitat, etc.). En general, qualsevol element que participi en el control dels accessos físics a les instal·lacions.

- Subministrament elèctric.

  Subministrament dels proveïdors, dispositius de redundància, sistemes d'alimentació ininterrompuda, generadors elèctrics dièsel, etc.

- Sistemes de control de temperatura i humitat.

  Redundància dels sistemes de ventilació, sistemes de monitoratge de temperatura i humitat, etc.

- Sistemes de detecció i extinció d'incendis.

- Sistemes de videovigilància i alarmes contra intrusions físiques.

Les proves tècniques que s'han de fer sobre aquest grup de sistemes verificaran que es compleixen els objectius i que es respecten els marcs reguladors, especialment els relacionats amb sistemes d'extinció d'incendis o de subministrament d'energia elèctrica. Per tant, les proves tècniques sobre aquests sistemes requeriran uns coneixements molt especialitzats en àrees diferents (electrotècnia, sistemes de climatització i control de condicions d'humitat, alarmes, etc.). Pot ser que l'auditor no tingui aquests coneixements, per la qual cosa serà necessari, en aquestes ocasions, comptar amb experts que facin les proves. No obstant això, és l'equip auditor qui decidirà si no hi ha cap més remei sobre els seus objectius.

D'altra banda, és interessant destacar que els sistemes industrials convergeixen cada vegada més amb els sistemes d'informació i hi comparteixen alguns subsistemes. Això obre tota una nova àrea per a l'auditoria de sistemes relacionada amb la seguretat dels sistemes de control industrial. Les tècniques que s'empraran per a auditar l'ús de les TIC, en els sistemes de control industrial, seran molt similars a les que s'examinaran en la resta del mòdul. No obstant això, es requereixen certs ajustos per a tenir en compte les circumstàncies específiques d'aquests sistemes.

4.2. Auditoria tècnica de sistemes, comunicacions i aplicacions

En la resta del mòdul, ens centrarem en les proves per a la revisió de la implantació de controls tècnics aplicats sobre sistemes d'informació i xarxes de comunicacions.

Quan es tracta de revisar la implantació de controls en sistemes d'informació, habitualment es parla d'*auditories tècniques* o *anàlisi de vulnerabilitats de sistemes*. Encara que l'abast de les proves que un auditor pot fer és molt ampli, podem fer la divisió següent, molt general:

- Anàlisi de vulnerabilitats de sistemes o xarxes.
- Anàlisi de vulnerabilitats de *hosts*.
- Auditoria d'aplicacions.

Aquesta separació es basa en el fet que els controls tècnics s'apliquen a diferent nivell en la infraestructura de TIC. Un gran nombre de controls s'implementen en parts de la infraestructura general, compartida per molts serveis, mentre que altres controls són específicament dissenyats i implementats en un sistema o aplicació concreta. D'aquesta manera, podem dir que hi ha, en primer lloc, proves més orientades a obtenir una visió general de l'estat de la infraestructura i dels elements crítics comuns a diversos serveis.

Exemples d'aquests elements poden ser: servidors de noms (DNS), elements de commutació, encaminament i filtratge de paquets (commutadors, encaminadors i tallafocs), filtres d'aplicació (servidors intermediaris SOCK, aplicacions específiques o servidors intermediaris web), entre d'altres.

La revisió d'aquest tipus d'infraestructura es denomina *anàlisi de vulnerabilitats de sistemes o xarxes*. En segon lloc, hi ha proves que busquen examinar com s'implementen els controls en un sistema, entorn o aplicació concrets.

D'altra banda, la diferència entre l'anàlisi de vulnerabilitats de sistemes o xarxes i l'anàlisi de *hosts* es tradueix, bàsicament, en el punt des d'on es fa l'anàlisi. En l'anàlisi de sistemes o xarxes, les vulnerabilitats es busquen des de fora del sistema, mitjançant la xarxa de comunicació. En canvi, en l'anàlisi de *hosts*, les vulnerabilitats es busquen des de la màquina en qüestió, tenint-hi accés local. Amb aquest tipus d'anàlisi, podem fer comprovacions més exhaustives. Els resultats seran similars als obtinguts per mitjà de l'anàlisi de vulnerabilitats de sistemes o xarxes. No obstant això, en el primer cas s'obtindran resultats més ampliats, gràcies a les comprovacions que només es poden fer amb un accés local al sistema: errors en la configuració dels permisos d'accés a fitxers, configuracions contràries a les polítiques de seguretat, programari maliciós, etc.

En aquest sentit, també és interessant destacar que l'objectiu és la recerca de vulnerabilitats en els sistemes TIC. La pregunta que ens podríem fer ara és: què s'entén per *vulnerabilitat* en el context d'una prova tècnica d'auditoria?

Vulnerabilitats en el context d'una prova d'auditoria

D'una manera general, en l'àmbit de l'anàlisi de riscos, s'entén per *vulnerabilitat* qualsevol problema en l'organització que pugui ser aprofitat per un atacant per a materialitzar un impacte sobre els actius de l'organització. En el nostre context, una vulnerabilitat tindrà la mateixa definició des d'una visió d'alt nivell, però podem concretar més la definició des d'una perspectiva més propera al problema que ens concerneix. Entendrem per *vulnerabilitat* qualsevol problema o error en la programació, configuració o especificació (en els casos més greus) en un component del sistema d'informació.

Exemples de vulnerabilitats

Poden ser: errors en un protocol, contrasenyes febles, sistemes no actualitzats amb els últims pegats de seguretat, serveis de xarxa amb ports oberts i sense coneixement per part de l'equip d'operació i manteniment, ús de serveis d'igual a igual o *peer-to-peer* no autoritzats, recursos compartits no autoritzats, instal·lacions d'accessos remots no autoritzats (per exemple, VNC o Terminal Server de Microsoft), entre altres.

Una anàlisi de vulnerabilitats consistirà en el procés de localitzar i reportar, en un informe, les vulnerabilitats existents en els sistemes que estan sota l'abast de l'auditoria. És important remarcar que l'anàlisi no examinarà els controls que s'apliquen internament en les aplicacions de negoci, que tracten finalment la informació i són específiques de les necessitats de negoci de l'organització.

L'anàlisi de vulnerabilitats estudiarà només la implantació dels controls tècnics de seguretat que afecten les infraestructures de comunicacions i dels sistemes en les parts més bàsiques (sistemes operatius, configuració d'aplicacions proporcionades per un tercer, etc.).

4.3. Mostreig en les proves d'auditories tècniques a sistemes de TIC

La importància d'identificar, correctament, els problemes d'implantació dels controls tècnics no és tan sols pel simple fet de fer una tasca d'auditoria amb una elevada excel·lència professional, sinó que té un valor intrínsec i comporta beneficis per a l'auditat.

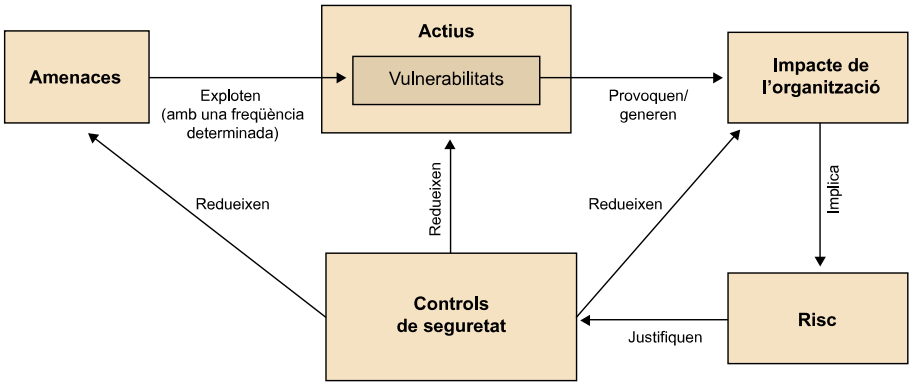
En una auditoria de segona o tercera part, l'objectiu principal de l'auditoria és respondre si l'objecte auditat s'ajusta al marc de referència. L'auditor farà un mostreig de proves de manera que es minimitzi el risc d'auditoria; aquestes proves s'executaran per a determinar la conformitat amb el marc de referència. Aquest procés s'aturarà quan l'auditor hagi trobat un nombre significatiu de no-conformitats, i l'auditoria es considera acabada. En aquests tipus d'auditoria, el resultat té valor tant per a l'auditat com per al client de l'auditoria.

D'altra banda, tal com s'ha dit anteriorment, les auditories tècniques sobre els sistemes de TIC solen ser, en la majoria de casos, auditories de primera part, en què l'auditat i el client d'auditoria són la mateixa entitat. En aquest cas, el client de l'auditoria, com que és l'objecte auditat, no està interessat únicament a determinar el grau de conformitat amb el marc de referència, sinó en el mateix resultat de les proves, a causa del benefici que comporta amb vista a aplicar millores en els seus sistemes TIC. Per tant, en les auditories de primera part purament tècniques, l'auditat no busca fer un mostreig de proves, sinó que vol que s'analitzi tota la infraestructura que queda sota l'abast de l'auditoria. Si l'auditat s'ha d'ajustar a uns determinats recursos, n'haurà de renegociar l'abast.

4.4. Valoració de les vulnerabilitats dels sistemes TIC

Com a resultat de les proves tècniques sobre els sistemes TIC, l'auditor detectarà vulnerabilitats en la seva infraestructura. El benefici que el client de l'auditoria obté de la determinació d'aquestes vulnerabilitats s'obté quan s'avalua el risc que aquestes comporten.

A continuació, mostrarem un diagrama ja presentat per repassar els diferents factors que determinen el risc d'una vulnerabilitat.



Factors que determinen el risc

És habitual valorar el risc en funció de:

- Valor de l'actiu amenaçat.
- Vulnerabilitats que es podrien aprofitar en un atac.
- Probabilitat que es materialitzi l'amenaça.
- Valor del dany que provocaria la materialització de l'amenaça.

Per a valorar el risc que comporta una vulnerabilitat, s'ha d'avaluar una sèrie de factors que estan fora de l'abast de l'auditor. L'auditor no està en disposició de valorar correctament la criticitat i l'aportació a la cadena de valor que pot tenir l'actiu en qüestió. No obstant això, sí que està en condicions de facilitar una visió de les característiques de la vulnerabilitat, la qual permetrà a l'auditat determinar:

- Quin tipus d'atac podria arribar a explotar la vulnerabilitat.
- En quines condicions es podria explotar.
- Amb quina facilitat es podria explotar.
- Quin tipus d'impacte provocaria la seva explotació (encara que l'auditor no pot valorar aquest impacte).

Tenint en compte aquests paràmetres, l'auditor pot oferir una valoració de la gravetat de la vulnerabilitat com a valor afegit al seu treball. Per la seva banda, l'auditat aportarà el coneixement de la valoració de l'actiu i l'estimació de l'impacte.

A partir de la valoració de la vulnerabilitat, que representa la probabilitat d'ocurrència de l'amenaça en certa manera, es pot determinar finalment el risc. L'assignació d'auditoria no inclou habitualment tot el procés de determinació del risc, però sí, almenys, la valoració de la gravetat de la vulnerabilitat. Fins i tot si l'auditat no arriba a avaluar el risc resultant, aquesta valoració li permetrà prioritzar les accions correctores resultants de l'auditoria.

La tasca de valorar una amenaça no és senzilla. Amb la gran quantitat de tipus de maquinari, aplicacions, interrelacions entre sistemes, etc., és molt difícil harmonitzar els mètodes de valoració d'una vulnerabilitat. Diferents proveï-dors de serveis d'avisos de vulnerabilitats empren sistemes de puntuació pro-

pis, però pocs són aplicables de manera general en qualsevol situació. A més, els seus mecanismes de puntuació no són públics i revisats per una comunitat oberta d'especialistes. Per això, per a facilitar la tasca de valoració de les amenaces, s'ha desenvolupat un sistema de puntuació coherent i sistemàtic de vulnerabilitats: el CVSS (*common vulnerability scoring system*).

4.4.1. CVSS (*common vulnerability scoring system*)

El CVSS[4] el va desenvolupar inicialment un organisme nord-americà: el NIAC (National Infrastructure Advisory Council[5]). No obstant això, aquest va designar la comunitat internacional d'equips de respostes davant incidents de seguretat, representats en el Forum of Incident Response and Security Teams (FIRST), com la institució que ha de continuar el seu desenvolupament i la promoció. El sistema ofereix com a més gran benefici l'estandardització del mecanisme de puntuació de les vulnerabilitats. Aquest sistema permet a una organització avançar en el camí de normalitzar la política de solució de problemes i resposta a les vulnerabilitats. Una vegada s'obté una puntuació normalitzada de les vulnerabilitats, es poden implementar altres sistemes que estableixin el temps en què s'ha de donar resposta a cada vulnerabilitat.

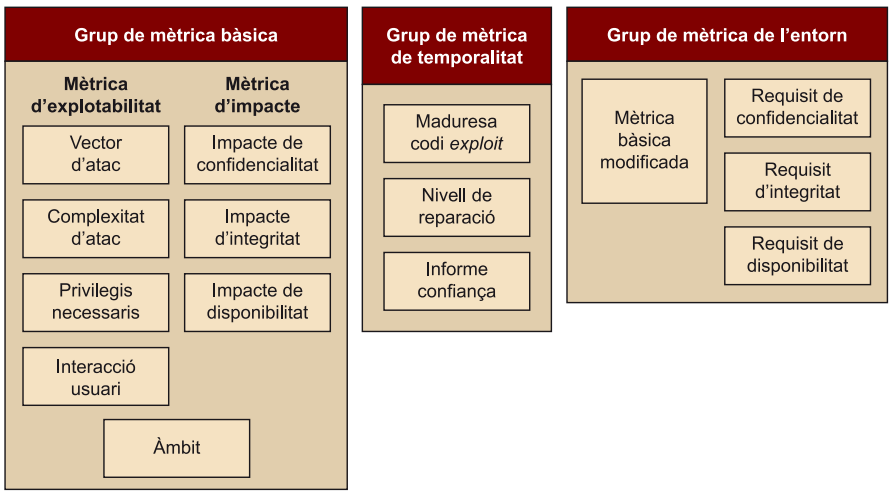
[4] En la versió 3, a data d'elaboració d'aquest material.

Enllaç recomanat

L'especificació del sistema de puntuació, així com altres materials interessants com ara exemples i calculadores, pot trobar-se a la pàgina oficial: https://www.first.org/cvss

[5] National Infrastructure Advisory Council, entitat que forma part del Departament de Seguretat de la Nació (Department of Homeland Security) dedicada a oferir consell al president dels Estats Units sobre la seguretat dels sistemes crítics del país i dels sistemes d'informació que hi donen suport.

El sistema de valoració CVSS està organitzat en tres grups de mètriques que reflecteixen tres aspectes al voltant de l'avaluació del risc que comporta una vulnerabilitat. Aquests grups, juntament amb les seves mètriques es mostren en el diagrama següent.



Mètriques de CVSS
Font: Especificacions oficials de CVSS versió 3, versió en anglès

Cada mètrica recull factors (o aspectes) comuns d'una vulnerabilitat, i facilita una visió de conjunt de les diferents facetes que s'han de considerar per a gestionar la vulnerabilitat. El mètode de puntuació consisteix, bàsicament, a valorar cadascun d'aquests factors. La valoració no es fa numèricament, sinó

mitjançant la selecció d'un qualificatiu (per exemple: *alt, baix, en xarxa, local, múltiple, senzill, etc*.). Aquests qualificatius estan descrits en la metodologia. El grup de mètriques bàsiques proporciona la informació més tècnica sobre les condicions de la vulnerabilitat. Les mètriques de temporalitat i d'entorn tenen com a objectiu contextualitzar la vulnerabilitat. Al llarg del temps, es donen circumstàncies que fan variar la valoració. De la mateixa manera, la variació de les circumstàncies de cada entorn en què s'avalua la gravetat també fa variar la valoració.

El grup de mètrica bàsica és l'únic requerit pel sistema de valoració CVSS. Habitualment, l'equip auditor avalua aquesta mètrica quan es detecta una vulnerabilitat. El sistema reconeix els següents grups com a opcionals i proporcionen més refinament al mecanisme d'avaluació. El grup de mètrica de la temporalitat requereix un seguiment en el temps de les circumstàncies que acompanyen la vulnerabilitat, i sol ser facilitat i mantingut per proveïdors del servei de vulnerabilitats. Finalment, el grup de mètrica de l'entorn se sotmet a la valoració dels usuaris finals del CVSS. El mètode descrit pel CVSS dóna diverses indicacions o consells sobre com realitzar la valoració de cadascun dels factors, per ajudar així a uniformitzar l'ús d'aquest sistema de valoració.

La valoració intrínseca de la vulnerabilitat és el grup de mètriques bàsiques. Els grups de temporalitat i d'entorn fan modificar aquesta valoració bàsica, la qual és inherent a la vulnerabilitat. En cada càlcul s'obté la valoració de la vulnerabilitat tenint en compte el grup bàsic, el bàsic i el temporal o bé tots tres.

A cada valoració (tant si és només bàsica, com bàsica i temporal, o bàsica temporal i entorn) se li pot atorgar un valor del 0 al 10 per a poder així prioritzar el tractament de les vulnerabilitats. Hi ha unes taules de conversió de les valoracions qualitatives de cada mètrica a un valor numèric i unes equacions per a realitzar l'avaluació numèrica final. En qualsevol cas, quan es realitza una valoració de criticitat de vulnerabilitats amb CVSS, s'ha de facilitar el valor numèric final i els usuaris finals del CVSS han de rebre sempre els qualificatius de cada mètrica, ja que són ells els que proporcionen la informació descriptiva i, en certa manera, justifiquen la valoració numèrica.

La puntació final de 0 a 10 pot ser traslladada a una valoració qualitativa d'acord amb aquesta taula:

Valoració qualitativa	Valor CVSS
Cap	0
Baix	0.1 - 3.9
Mitjà	4.0 - 6.9
Alt	7.0 - 8.9

Valoració qualitativa	Valor CVSS
Crític	9.0 - 10.0

Cadascuna de les mètriques i dels factors que s'han d'avaluar té la finalitat següent:

1) Mètrica bàsica. Aquesta mètrica representa les característiques intrínseques de la vulnerabilitat, les quals no depenen de les circumstàncies de l'entorn ni del temps. Constitueix la part més tècnica de la valoració, i és molt objectiva.

Habitualment, els portals que publiquen vulnerabilitats faciliten únicament la valoració d'aquest grup de mètriques.

Els factors que s'han de valorar són (dividits en tres subgrups):

a) Mètriques d'explotabilitat: aquest grup de mètriques fa referència a les característiques pròpies del component que és vulnerable. Es valoren les següents mètriques:

- Vector d'accés:
  - Valors possibles: local / xarxa d'àrea local / xarxa / físic.
  - Reflecteix com o des de quin punt de la infraestructura es pot explotar la vulnerabilitat.

- Complexitat de l'accés:
  - Valors possibles: alta / baixa.
  - Mesura la complexitat tècnica necessària perquè un atacant que disposa del vector d'atac pugui explotar la vulnerabilitat.

- Privilegis d'accés requerits:
  - Valors possibles: cap / baix / alt.
  - Nivell d'accés previ que ha de tenir un atacant per a poder explotar la vulnerabilitat.

- Interacció de l'usuari:
  - Valors possibles: Cap / Requerit.
  - Aquesta mètrica mesura si l'atacant requereix la col·laboració (voluntària o involuntària) d'un usuari legítim per poder explotar la vulnerabilitat.

b) Mètrica d'abast: aquesta mètrica s'ha introduït des de la versió 3 del CVSS. Fa referència a l'auge dels entorns virtualitzats o *sandboxes*. Avui dia hi ha vulnerabilitats que poden permetre a l'atacant traspassar els límits d'aquests entorns de computació on s'està executant el component vulnerable. Aquesta mètrica pretén recollir aquest aspecte.

- Abast:
  - Valors possibles: Sense canvi / Canvi.
  - Reflecteix si la vulnerabilitat permet canviar l'entorn de computació o no. És a dir, si permet a l'atacant traspassar aquest entorn i saltar a un altre (per exemple, en cas de màquines virtuals, saltar al sistema operatiu de l'entorn amfitrió de la màquina virtual).

c) Mètriques d'impacte: aquestes mètriques pretenen recollir de quina manera s'altera la seguretat de l'entorn.

- Impacte en la confidencialitat, integritat i disponibilitat:
  - Valors possibles per a cadascun: baix / alt.
  - Es mesura l'impacte objectiu que tindria l'explotació en cadascuna de les dimensions de la seguretat. El mesurament es fa separadament, ja que poden no estar afectades totes les dimensions en tots els casos.

2) Mètrica de la temporalitat. Representa les característiques pròpies de la vulnerabilitat (no de l'entorn en què es presenta) que poden evolucionar amb el temps.

Els factors que s'han de valorar són els següents:

- Maduresa del codi d'explotació:
  - Valors possibles: no provada / prova de concepte / funcional / alta / sense definir.
  - Mesura el nivell actual de disponibilitat de tècniques, eines o codis per a fer l'explotació real de la vulnerabilitat.
- Confiança:
  - Valors possibles: desconegut / raonable / confirmat / sense definir.
  - Mesura algun dels aspectes següents: el grau de confiança que es té en l'existència real de la vulnerabilitat, o la credibilitat de la font que proporciona la informació de la seva existència.
- Remei a la vulnerabilitat:

- Valors possibles: solució oficial / pegat temporal / solució pal·liativa (*workaround*) / no disponible / sense definir.
- Valora l'existència d'una solució definitiva o temporal proporcionada pel fabricant o altres fonts.

El valor "sense definir"

El valor "sense definir" s'ha disposat per a les situacions en què no es vol valorar un determinat paràmetre (per falta d'informació suficient). Aquest valor fa que el factor no es tingui en compte en les fórmules per al càlcul final.

3) Mètrica de l'entorn. Aquesta mètrica recull les circumstàncies pròpies de cada entorn en què s'estigui analitzant la vulnerabilitat. Evidentment, aquesta mètrica depèn totalment de l'entorn.

Els factors que s'han de valorar s'agrupen en dos subgrups, modificacions a les mètriques bàsiques i l'impacte real sobre CIA (confidencialitat, integritat o disponibilitat) en l'entorn de l'organització:

- Modificació de les mètriques bàsiques: encara que les mètriques del grup bàsic són inherents a les característiques tècniques pròpies de vulnerabilitat, és possible que algun canvi tècnic (configuració o arquitectura) pugui fer que tingui sentit ajustar alguna de les mètriques d'aquest grup a causa de les circumstàncies particulars de l'organització.

- Requisits de confidencialitat, disponibilitat i integritat:
  - Valors possibles: baix / mitjà / alt / sense definir.
  - Aquest factor permet particularizar l'anàlisi segons la importància d'un actiu determinat. D'una banda, l'explotació de la vulnerabilitat pot afectar alguna de les facetes CID (confidencialitat, integritat o disponibilitat) de la seguretat, i això està previst en alguns dels factors de la mètrica bàsica. Però, en aquest cas, el que es pretén valorar és, per als actius afectats per la vulnerabilitat, quina és la faceta CID de la seguretat que és més important. Així, aquest paràmetre ens permetria afinar l'anàlisi fins al nivell de cadascun dels sistemes afectats.

En l'actualitat, hi ha diversos proveïdors d'avisos de vulnerabilitats que empren aquest mètode per a fer la puntuació. Habitualment, proporcionen una valoració de les mètriques bàsiques i de temporalitat. D'altra banda, també és interessant destacar que hi ha eines (en format web o full de càlcul) que faciliten l'aplicació de les fórmules descrites en el sistema CVSS. Com hem comentat, aquest sistema de puntuació resulta també interessant per als auditors que facin avaluacions de seguretat purament tècniques de la identificació de vulnerabilitats tècniques, tant en infraestructures com en aplicacions.

4.5. Auditoria tècnica de sistemes i gestió de TIC

Les infraestructures de sistemes d'informació, fins i tot en organitzacions de grandària petita o mitjana, són molt heterogènies i nombroses. Per tant, podem estimar que el cost de fer una auditoria detallada de tota la infraestructura TIC (que inclogui els tres tipus d'anàlisi: sistemes, xarxes, *hosts* i aplicacions) és massa elevat. Fins i tot en l'àmbit d'una auditoria de tercera part, l'equip auditor n'ha de reduir l'abast, ja sigui limitant la profunditat o bé el nombre de sistemes analitzat. Encara que de vegades se sol·liciti a l'equip auditor la revisió puntual d'algun tipus d'element d'una infraestructura (o bé ell mateix en determini la necessitat), fer totes les proves tècniques en profunditat és inabordable. L'enfocament més habitual serà fer un programa d'auditoria que inclogui una planificació dels sistemes i de les xarxes que s'han d'auditar.

En l'àmbit d'una auditoria de primera part, l'objectiu de l'auditoria sí que serà probablement la revisió de la totalitat de la infraestructura. Aquesta revisió, no obstant això, s'abordarà per parts, d'una manera planificada. D'aquesta manera, l'auditoria tècnica passa a ser una eina més entre les que es tenen per a gestionar els sistemes de TIC.

D'altra banda, les tècniques d'anàlisi de vulnerabilitats es poden emprar per a auditar la seguretat dels sistemes en diferents fases de la seva implantació o del seu funcionament. A continuació, veurem un possible ús d'aquestes tècniques per a sistemes en desenvolupament/desplegament, i un altre possible ús per a sistemes en producció.

- **Anàlisi de vulnerabilitats en sistemes en desenvolupament o desplegament**. A la fase de desenvolupament o desplegament d'un nou sistema es pot incorporar un procés d'anàlisi de vulnerabilitats, que s'executarà de manera sistemàtica abans de la posada en producció.

- **Seguiment de les vulnerabilitats en sistemes en producció**. Sotmetre els sistemes en producció a una anàlisi de vulnerabilitats pot comportar una pèrdua de disponibilitat (veurem més endavant que això és un risc quan s'empren certes tècniques). Per això, en certes situacions es pot optar per una estratègia diferent: vigilància de les vulnerabilitats, que es fa per mitjà de les fases següents:
  - Seguiment de les vulnerabilitats dels sistemes de l'organització a partir del que hagi publicat la comunitat d'experts en seguretat. Hi ha serveis (alguns de gratuïts i d'altres de pagament amb diferents qualitats) que informen del descobriment de noves vulnerabilitats.

  - Una vegada publicada una nova vulnerabilitat, s'han d'analitzar els sistemes potencialment vulnerables.

  - Aplicació d'una política d'apedaçament dels sistemes vulnerables. Aquesta política hauria de determinar la planificació del desplegament

del pedaç segons la seva gravetat (emprant, per exemple, el sistema CVSS).

– Anàlisi de vulnerabilitats sobre els sistemes apedaçats per a la seva verificació.

Entre aquests serveis, podem destacar CVE Mitre, Secunia o el servei del NIST *National Vulnerability Database*. Alguns d'aquests serveis permeten filtrar i personalitzar els avisos en funció dels actius propis de l'organització o ofereixen la seva informació mitjançant interfícies públiques per a integrar amb entorns propis.

4.6. Tècniques d'anàlisi de vulnerabilitats de xarxa o de sistemes

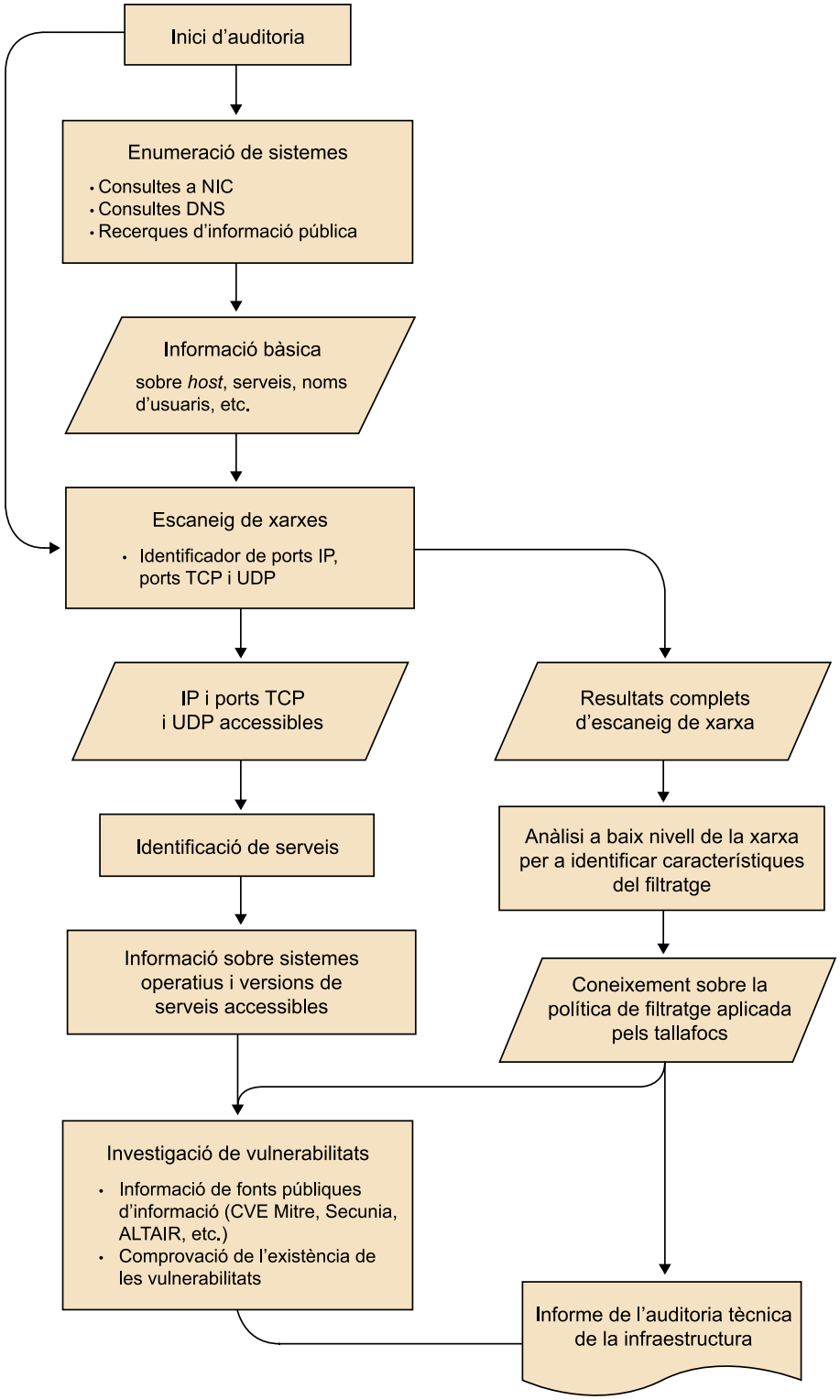
A continuació, ens centrarem en les tècniques i eines que es poden emprar per a fer una anàlisi de vulnerabilitats en xarxes o sistemes. Així mateix, destaquem que ens centrarem en xarxes basades en el protocol IP. Malgrat que aquestes proves poden ser molt útils per a l'auditor, s'ha de tenir en compte que tenen certes limitacions pròpies del seu enfocament. Les anàlisis de vulnerabilitats no seran capaces de detectar certs tipus de portes del darrere, determinats tipus d'errors en la configuració dels tallafocs o vulnerabilitats explotables únicament en mode local.

Recordem que la idea principal sobre aquest tipus de proves és que es fan des d'alguns punts de la infraestructura (per exemple, des d'Internet o des de segments de la xarxa corporativa). És a dir, l'anàlisi de la seguretat no es duu a terme mirant la configuració dels elements que componen els controls, sinó que s'avalua utilitzant mètodes similars als que utilitzaria un intrús que volgués atacar la infraestructura. Aquesta és la raó per la qual, per a l'explicació de les diferents eines, emprarem la mateixa metodologia que seguiria un intrús.

Les fases i tasques bàsiques que componen una anàlisi de vulnerabilitats de sistemes o xarxes s'enumeren a continuació de manera resumida. No obstant això, s'ha de tenir en compte que cada auditor és lliure de seguir la seva pròpia metodologia. La que es presenta aquí és la més usual. Està basada en una multitud de metodologies reconegudes internacionalment i implementada per un gran nombre d'aplicacions:

- Enumeració de xarxes per a identificar xarxes IP i servidors dins de l'abast de l'auditoria.
- Escaneig massiu d'adreces IP i ports accessibles des dels diferents punts d'anàlisi.
- Anàlisi automatitzada de vulnerabilitats.
- Examen manual dels resultats.

El gràfic següent reflecteix les diferents fases que hem apuntat per a entorns publicats a internet. En cas de ser sistemes interns, algunes fases podrien ser més reduïdes.



Fases d'una anàlisi de vulnerabilitats de xarxa

4.6.1. Enumeració i identificació de xarxes i sistemes

Aquesta fase es duu a terme quan l'organització vol conèixer el grau de coneixement de les seves infraestructures, que es pot obtenir des de l'exterior. De vegades, si es té la intenció de fer alguna prova d'enginyeria social, aquesta fase també es fa per a saber el grau de coneixement de les seves infraestructures que tenen les persones que hi operen i les mantenen. En aquesta fa-

se, no s'identifiquen vulnerabilitats del sistema, ja que únicament s'analitzen fonts d'informació pública. De vegades, també s'acostuma a denominar *anàlisi d'intel·ligència competitiva*[6], en què el concepte d'*intel·ligència* s'entén com la informació que s'ha obtingut, analitzat, comprès i aprofitat.

(6)El terme ve de l'anglès *competitive intelligence*; la Societat de Professionals d'Intel·ligència Competitiva (SCIP: www.scip.org), als Estats Units, la defineix com un procés ètic i sistemàtic de recol·lecció d'informació, anàlisi i disseminació pertinent, precisa, específica, oportuna, predictible i activa, sobre l'ambient de negocis, dels competidors i de la mateixa organització.

En aquesta fase, s'empraran fonts d'informació legals i públiques per a determinar, tan bé com es pugui, l'estructura TIC sota l'abast de l'auditoria. S'intentaran identificar

- subxarxes;
- adreces IP d'allotjadors;
- funcions que realitza cada sistema;
- noms d'usuaris (inferits a partir de les adreces de correu del personal, per exemple);
- telèfons;
- relacions entre persones i sistemes;
- informació tècnica sobre sistemes (sistemes operatius, eines emprades, etc.) que s'hagi pogut filtrar en llocs d'informació pública (fòrums de suport, per exemple);
- etc.

Cal destacar que, de vegades, aquesta fase no la sol·liciten els clients d'auditoria, malgrat el benefici indubtable que comporta i, sens dubte, forma part de qualsevol metodologia que s'empri per a realitzar un test d'intrusió des d'Internet, sobretot si és completament en mode caixa negra. No obstant això, encara que aquesta informació no sigui rellevant per a l'auditat, sí que pot proporcionar a l'auditor informació addicional necessària per a anàlisis posteriors. Per exemple, si l'auditoria tècnica té per objectiu determinar la infraestructura de l'organització exposada davant Internet, i el tipus d'auditoria sol·licitada pel client és de caixa negra, la realització d'aquesta fase és de summa importància.

Les tècniques més habituals per a fer aquesta recollida d'informació són:

Consultes a servidors de noms de domini (DNS)

Els servidors de noms són un element crític per a la infraestructura general d'Internet i per a la interna d'una organització. Per aquesta raó, és un element que haurà de ser interrogat per a fer aquesta fase i que, a més, pot ser auditat com un element més.

L'auditor consultarà els DNS per a esbrinar les adreces IP de les màquines, i també per a identificar les funcions que aquests sistemes fan, sobretot en la part de la infraestructura que està exposada a Internet. A partir d'aquestes consultes, s'obtenen les adreces IP de servidors de correu entrant (SMTP), servidors web, servidors de noms, entre altres.

Per a interrogar els servidors de noms, l'auditor pot utilitzar diferents eines. En la majoria de sistemes operatius, s'hi inclouen eines com *nslookup*, encara que l'eina *dig* és més adequada per a aquest propòsit.

Ordre *dig*

```
Usage: dig [+++global-server] [domain] [q-type] [q-class] {q-opt}
      {global-d-opt} host [+++local-server] {local-d-opt}
      [ host [@local-server] {local-d-opt} [...]]
Where: domain is in the Domain Name System
   q-class is one of (in,hs,ch,...) [default: in]
   q-type is one of (a,any,mx,ns,soa,hinfo,axfr,txt,...) [default:a]
         (Usi ixfr=version for type ixfr)
   q-opt is one of:
   -x dot-notation (shortcut for in-addr lookups)
[. . .]
         d-opt is of the form +keyword[=value], where keyword is:
         +[no]vc        (TCP mode)
[. . .]
   global d-opts and servers (before host name) affect all queries.
   local d-opts and servers (after host name) affect only that lookup.
   -h                 (print help and exit)
   -v                 (print version and exit)
```

També hi ha aplicacions similars que integren diverses eines, o eines *online* que permeten realitzar consultes DNS amb les mateixes facilitats que l'ordre dig, però des d'unes altres adreces IP, diferents de les emprades per l'auditor, per exemple:

- https://www.digwebinterface.com/

- http://www.kloth.net/services/dig.php

En general, hi ha multitud d'aplicacions similars.

El mètode més directe, per a recopilar informació sobre totes les màquines contingudes en un DNS, és consultar el mateix DNS, la qual cosa requereix conèixer els noms d'aquestes màquines. Per a determinar el nom d'una màquina, es poden fer consultes inverses, és a dir, sol·licitar al DNS el nom de la màquina a partir de la seva IP. Tanmateix, això requereix que el DNS tingui introduït el registre PTR per a totes les màquines, la qual cosa no és gaire ha-

bitual. Un altre mètode per a determinar el nom d'una màquina és mitjançant força bruta. Hi ha eines que permeten automatitzar aquesta consulta massiva i/o fer consultes inverses de manera massiva per a consultar tot un rang IP.

No obstant això, la manera més ràpida d'obtenir els noms de totes les màquines seria mitjançant una sol·licitud de transferència de zona. El fitxer de *DNS zone* conté tots els noms de màquina per a un determinat domini DNS, incloent-hi de vegades fins i tot informació sobre adreçaments privats. Les organitzacions, per a balancejar la càrrega i millorar la tolerància a fallades, utilitzen més d'un servidor DNS. Per tant, hi ha un DNS principal i un o diversos de secundaris. Qualsevol d'aquests pot ser consultat, per la qual cosa tots han de tenir els fitxers *DNS zone* sincronitzats. Per sincronitzar el contingut dels servidors secundaris amb el primari, els DNS secundaris realitzen una sol·licitud DNS de transferència de zona. D'aquesta manera, obtenen una llista completa dels noms del domini. Si el DNS primari no es configura per a evitar les transferències de zona des de qualsevol adreça IP, és fàcil obtenir una llista completa de les màquines registrades en el DNS. Per a això, es pot utilitzar l'ordre *ls –d* en l'eina *nslookup*, o l'opció *axfr* en l'ordre *dig*, o eines específiques per a *testing* de DNS com *dnswalk*. És important tenir en compte que el fet que un DNS primari accepti sol·licituds de transferència de zona des de qualsevol IP s'hauria de considerar un error.

Consultes WHOIS als Network Information Centers (NIC) i als Regional Internet Registries (RIR)

Per al funcionament correcte d'Internet, hi ha organismes que administren les assignacions d'adreces IP (els RIR) i altres que administren les assignacions de noms de domini (els NIC).

Tots dos tipus d'organismes mantenen les bases de dades WHOIS, que emmagatzemen informació registrada corresponent a dominis i segments d'adreces IP. La gestió dels diferents segments d'adreces IP és després delegada a altres entitats: els ISP. Les bases de dades WHOIS són consultables mitjançant eines en els nostres propis sistemes operatius (per exemple, mitjançant l'ordre *whois* en UNIX/Linux), o bé per mitjà d'aplicacions web que els NIC i els RIR publiquen a Internet. D'aquestes consultes es pot obtenir: informació de persones de contacte juntament amb els seus càrrecs, adreces de correu, adreçaments IP, adreces IP de servidors de domini, regles d'encaminament, etc.

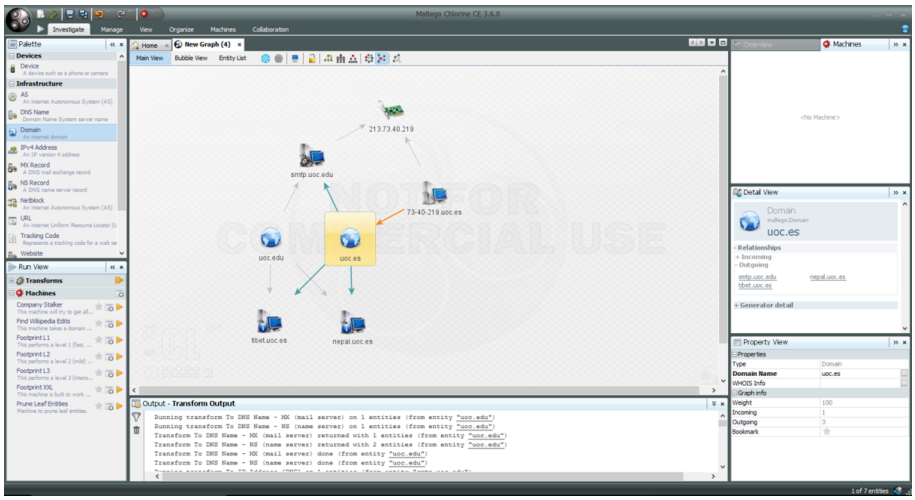
Les fonts habituals de consulta són:

- American Registry for Internet Numbers (ARIN)
- Asia Pacific Network Information Centre (APNIC)
- Réseaux IP Européens (RIPE)
- El NIC corresponent al domini que s'estigui auditant i, especialment, els NIC nacionals.

Recerques en repositoris públics d'informació d'Internet

Les tècniques anteriors han estat les més emprades tradicionalment, i encara ho són. No obstant això, amb l'auge de l'ús del World Wide Web, els fòrums d'usuaris, els grups de notícies, les llistes de correu, els cercadors i altres fonts d'informació pública d'Internet, cada dia es troba més informació sobre les organitzacions a Internet, és a dir, en llocs no controlats directament per elles mateixes. Mitjançant la consulta i recerca en aquestes fonts, es pot trobar informació que permeti inferir aspectes de l'arquitectura de l'organització, com noms de productes, versions, problemes, noms d'usuaris, etc.

Aquestes noves fonts d'informació estan augmentant la seva importància cada dia, i ja hi ha eines que permeten automatitzar-hi la recerca d'informació. Cal destacar l'eina Maltego, que combina tots dos tipus de recerques: les estructurades en bases de dades com WHOIS i DNS, i les recerques en diferents fonts d'informació a Internet, sobretot per a la recerca d'informació relacionada amb persones.



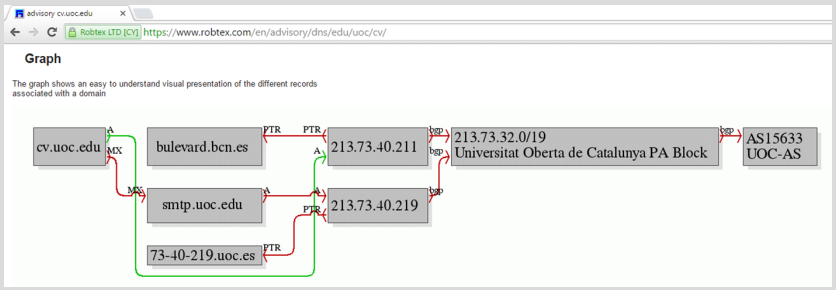
Ús de Maltego per a recollida d'intel·ligència competitiva

L'eina Maltego també resulta interessant per a investigar i obtenir informació rellevant sobre persones que tinguin relació amb l'entitat auditada. No obstant això, no tot el potencial d'aquesta eina està disponible en la seva versió "comunitat".

Dins de l'àmbit de les eines amb una representació gràfica de la informació, volem destacar també l'eina web robtex, que permet fer una multitud de consultes a les bases de dades que hem comentat anteriorment (WHOIS, consultes a DNS).

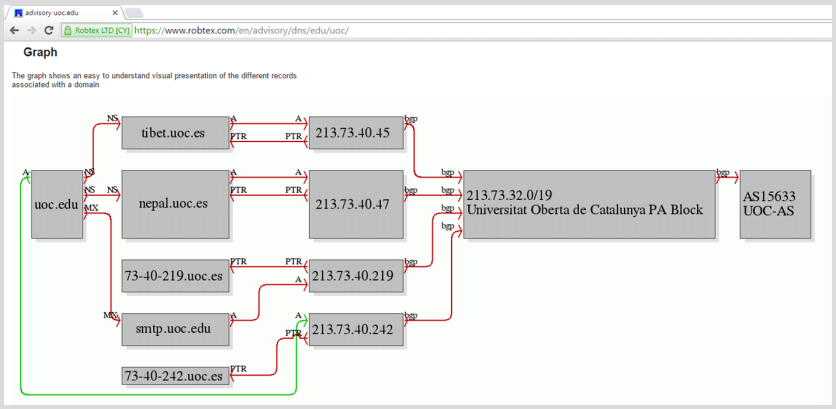
L'ús de l'eina robtex

A continuació, mostrem l'obtenció de certa informació pública sobre el domini de la Universitat Oberta de Catalunya, prenent com a punt de partida el nom del servei de classes virtuals al qual accedeixen els alumnes: cv.uoc.edu. S'ha emprat l'eina robtex, encara que s'ha d'entendre que el mateix que ofereix aquesta eina es podria fer amb eines més senzilles, com simplement l'ordre *dig*.



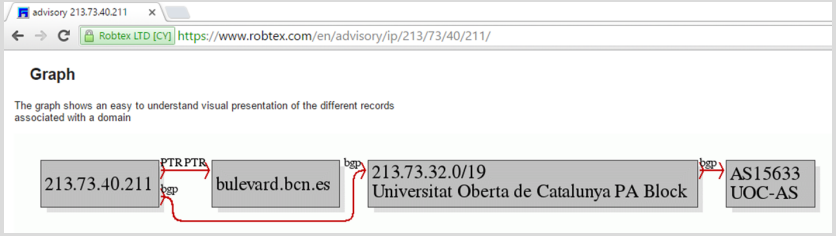
Consulta DNS del nom cv.uoc.edu

La consulta ens ha retornat la seva adreça IP, i el nom del servidor de correu entrant. Si es fa una consulta del nom de domini, ens proporcionarà la informació detallada sobre els principals registres del domini: MX i NS.



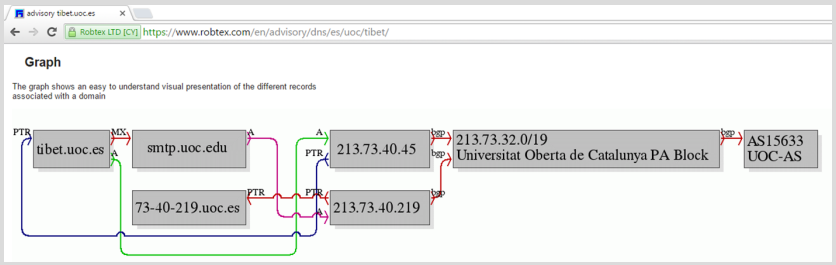
Consulta DNS del nom de domini uoc.edu

Si fen una consulta inversa de l'adreça IP del servidor de cv.uoc.edu, obtindrem més informació, com l'àlies d'aquest servidor i un altre domini que es troba servit per la mateixa màquina.



Consulta DNS inversa de l'adreça IP del servidor de correu

Finalment, podem consultar el registre corresponent a un dels servidors DNS.



Consulta DNS del nom del servidor DNS

Com es pot observar, la informació obtinguda sobre la infraestructura amb uns pocs clics és abundant. No obstant això, no ens hem de sorprendre, perquè no cal oblidar que es tracta d'informació pública.

Finalment, val la pena comentar que les organitzacions que fan proves d'intel·ligència competitiva complementen aquestes proves amb altres en què s'analitzen fòrums de diferents tipus, per a monitorar l'exposició de l'organització a possibles atacs futurs. Aquest tipus de proves són més complexes i requereixen un component d'intel·ligència que ha de ser aportat per analistes. Aquests analistes, a més, es basen en eines relacionades amb la mineria de dades (*datamining*), que es basa en la recollida massiva d'informació per a la seva posterior anàlisi, correlació, visualització, etc.).

4.6.2. Escaneig d'adreces IP i ports

Aquesta fase es fa després del reconeixement inicial de la fase anterior. També es pot fer directament si l'auditat facilita tota la informació necessària per a iniciar aquestes tasques i no està interessat en els resultats de la prova anterior. Aquesta fase és especialment crítica i necessària quan s'executen anàlisis de vulnerabilitats de sistemes exposats a Internet.

L'escaneig de la xarxa proporciona una imatge més clara de la visibilitat. No solament s'obtenen tots els *hosts* visibles (la qual cosa completa els identificats en la fase anterior), sinó que, a més, es recopilen tots els serveis IP que s'ofereixen. És important aclarir que aquesta visibilitat depèn del punt des d'on es facin les proves, ja que les xarxes IP solen disposar de mesures per al filtratge de trànsit (ja sigui mitjançant llistes de control d'accés en els encaminadors, per mitjà de l'ús de NAT –*network address translation*– o de tallafocs). L'auditor haurà de planificar els diferents punts des d'on fer les proves en funció dels objectius de l'auditoria.

Els objectius específics d'aquesta fase seran tenir tan clara com sigui possible la topologia de xarxa auditada des dels diferents punts d'anàlisi. Les tècniques més habituals utilitzades en aquesta fase són les següents:

1) Escombratge ICMP.
2) Escombratge de ports.
3) Identificació de sistemes operatius i serveis.

Escombratge ICMP

Mitjançant diferents tipus de missatges ICMP, es poden identificar *hosts* presents en una xarxa. El tipus més utilitzat és el 8 - *Echo Request*, que és l'usat per l'ordre *ping*. Mitjançant l'ús d'escombratges d'altres tipus –13 *Timestamp Request*, 15 *Information Request* o 17 *Subset Address Mask Request*– es poden identificar xarxes potencialment mal protegides o fins i tot desprotegides. És fins i tot possible enviar aquest tipus de missatges a les adreces de difusió de les subxarxes, per a identificar sistemes mal configurats. Habitualment, els dispo-

sitius de tallafoc haurien d'impedir l'entrada de missatges ICMP des d'altres xarxes i, dins d'aquestes, els equips no haurien de respondre aquests missatges (excepte el de tipus 8).

Algunes eines que es poden emprar són: *sing* o *nmap*.

Escombratge de ports

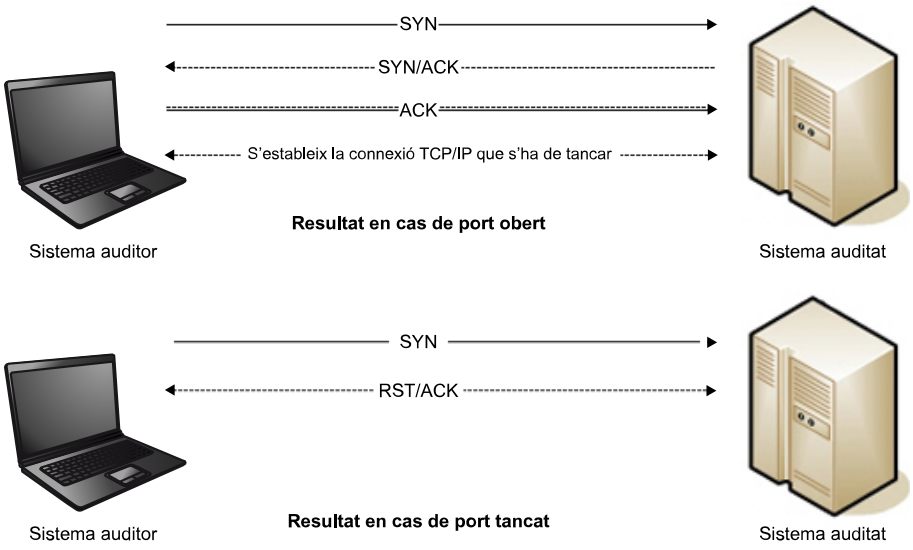
Es tracta d'identificar tots els serveis TCP i UDP accessibles en els *hosts* detectats. L'escombratge ICMP ens permetrà reduir el nombre d'adreces IP contra les quals fer aquest tipus d'escombratges. No obstant això, és possible que els sistemes no responguin a l'ICMP Echo Request en configuracions molt segures. Això últim no és gaire habitual, ja que dificulta el manteniment dels sistemes, el monitoratge i en general la resolució d'incidències tècniques.

D'altra banda, és molt habitual que els encaminadors i tallafocs filtrin aquest tipus de trànsit en les vores de les xarxes corporatives. Per tant, si es fa una anàlisi des de l'exterior, no es pot confiar en el resultat de l'escombratge ICMP, i s'hauria de fer l'escombratge de ports en totes les adreces IP que, potencialment, es volen analitzar. Això pot ser molt costós en termes temporals.

Per a descriure les tècniques utilitzades, hem de distingir entre ports TCP i UDP, a causa de la naturalesa diferent que tenen: el primer és orientat a connexió, mentre que el segon, no.

1) Escaneig de ports TCP. Hi ha diverses tècniques d'escaneig que fan ús de les diferents respostes que un port TCP ha de donar a diferents tipus de missatges. Per limitacions d'espai, esmentarem només les tècniques més habituals:

- *TCP connect() scan*. Es crida a la màquina en qüestió per a iniciar una connexió TCP. Si la crida finalitza amb èxit, el port està obert; en cas contrari, no.

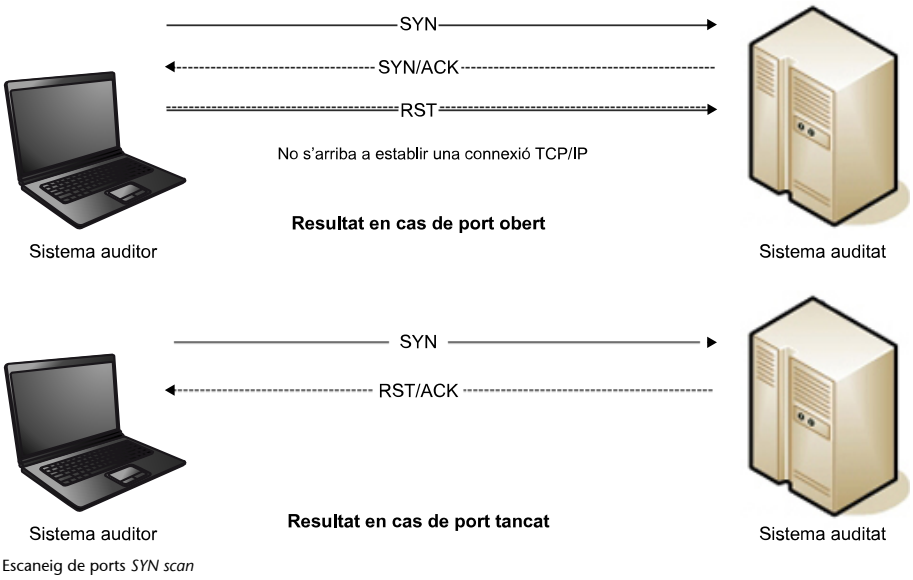


Escaneig de ports *TCP connect()*

Si s'ha pogut fer la connexió, el sistema auditor tancarà la connexió, o deixarà que la connexió es tanqui automàticament per *timeout*. Aquest mètode té l'inconvenient que requereix completar el procés de connexió. Per tant, aquesta prova pot quedar registrada en els registres d'activitat del sistema auditat. Aquest inconvenient pot no ser problemàtic en certs escenaris però, en d'altres, l'equip auditor necessitarà un mecanisme d'escaneig més discret i al mateix temps més ràpid.

- *SYN scan*. Per a aquesta prova, es requereix una aplicació que tingui accés directe al protocol TCP. D'aquesta manera, els paquets TCP necessaris per a fer l'escombratge són construïts per la mateixa aplicació. Aquest mètode d'escombratge difereix de la connexió normal, en què, quan es rep un paquet TCP de tipus SYN/ACK, el sistema auditor respon amb un RST, i la connexió es tanca immediatament. Per tant, en cap moment no s'arriba a obrir la connexió, per la qual cosa no cal enviar cap altre paquet IP, ni queda registrada la connexió.

  Aquest tipus d'escaneig és més discret, encara que la gran majoria de tallafocs són capaços de detectar-ho. D'altra banda, l'existència d'un tallafoc alterarà els resultats segons el tipus de política de filtratge que tingui implementat. Per tant, aquesta tècnica ens permetrà examinar el filtratge aplicat pels tallafocs.



Escaneig de ports *SYN scan*

Pàgines web

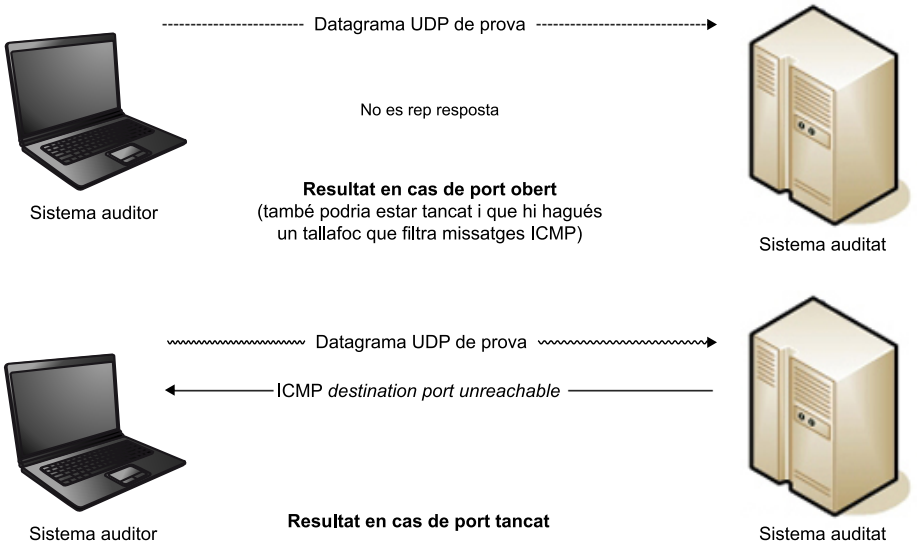
Hi ha altres mètodes per a escanejar xarxes que, per la seva complexitat tècnica, considerem fora de l'abast d'aquest mòdul. Per a obtenir-ne més informació, podeu consultar el lloc web: http://www.insecure.org/nmap/man i http://www.nmap-tutorial.com.

Com a conclusió, direm que l'ús encertat de l'escaneig de xarxes, juntament amb altres tècniques d'un nivell més baix, permeten comprovar la política de filtratge implementada en els tallafocs de l'organització.

2) Escaneig de ports UDP. L'escaneig de ports UDP és més complicat, a causa de la naturalesa d'aquest tipus de protocol no orientat a la connexió. En aquest cas, els ports UDP no han d'enviar cap resposta, i els ports tancats tampoc no han d'enviar un missatge d'error. És per aquesta raó que és poc fiable l'escaneig de ports UPD, encara que les aplicacions disponibles faciliten aquesta tasca. Les dues opcions disponibles seran:

- Enviar un datagrama UDP de prova a un port i esperar a rebre el missatge ICMP *"Destination port unreachable*", la qual cosa demostra que el port està tancat. Si no es rep el missatge, pot significar que efectivament el port està obert, encara que també pot significar que hi ha un tallafoc que impedeix la sortida de missatges ICMP (cosa que és habitual).

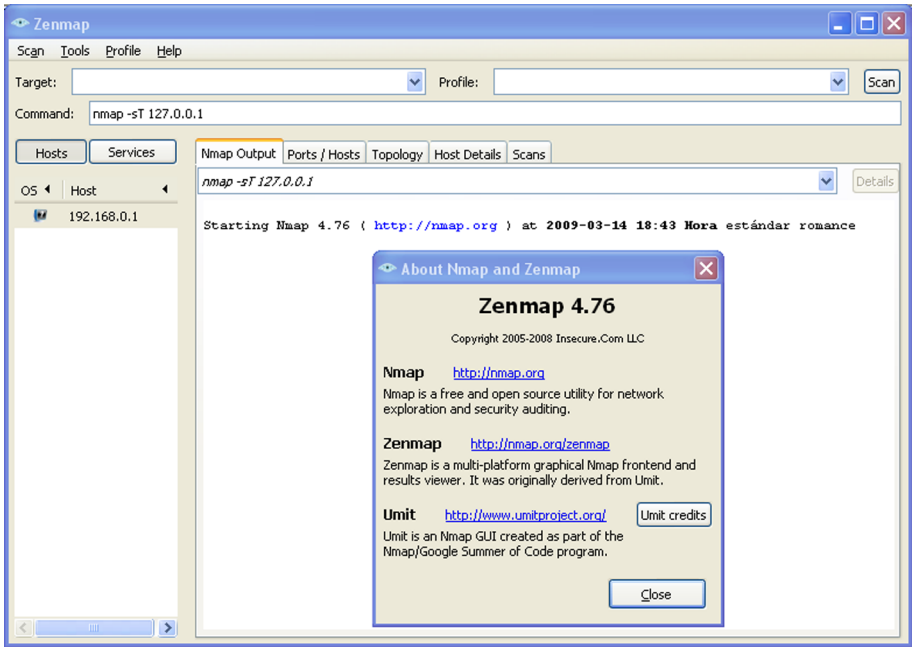
- Emprar programari client que enviï datagrames UDP "legítims" de l'aplicació que es pressuposi que està escoltant en el port (DNS, SNMP, TFTP, etc.), i esperar la resposta corresponent del protocol de la capa d'aplicació.



Escaneig de ports UDP

Qualsevol d'aquestes dues opcions proporciona uns resultats més pobres que els que es poden obtenir de l'escaneig de ports TCP, però el segon ofereix resultats més precisos, encara que la seva execució és més tediosa perquè necessita una eina específica per a cada port.

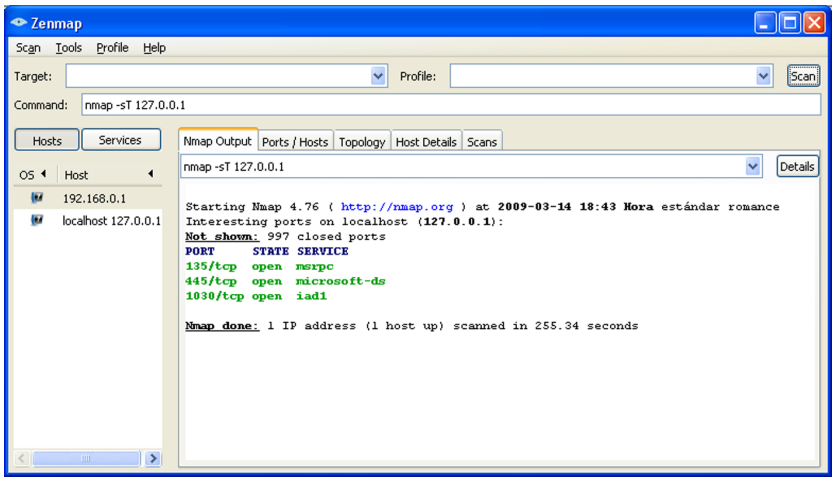
Respecte a les eines més idònies per a aquest tipus de tasques, s'ha de destacar NMAP, per sobre de gairebé qualsevol altra eina fins i tot comercial. En la data de realització d'aquest material, NMAP es troba en la versió 7.12 i inclou, a més de la interfície tradicional de línia d'ordres, una interfície gràfica.



Eina *NMAP* en la versió amb interfície gràfica

Escaneig amb *NMAP*

En l'exemple següent, emprem *NMAP* per a escanejar ports fent ús del mètode *TCPconnect() scan*:



Ús de *NMAP* per a escaneig *TCP connect()*

Hi ha més maneres de fer un escaneig de ports, però la seva utilitat es veu reduïda a situacions en què, o bé volem ser més sigilosos, o bé volem identificar les polítiques implementades per un tallafoc per mitjà de tècniques molt elaborades.

Identificació de sistemes operatius i serveis

Una vegada localitzades les màquines i enumerats els ports oberts, queda identificar el sistema operatiu i els serveis que estan escoltant en cadascun dels ports oberts. En la mesura que es pugui, s'intentarà identificar també la versió d'aquests serveis i aspectes de la seva configuració. És important notar que, en l'exemple anterior, s'identifica el servei que hi ha escoltant en cada port sobre la base del número de port. No obstant això, aquesta relació entre número de port i servei és la determinada per la Internet Assigned Numbers Authority (IANA) i no cal que sigui la realment implementada en la màquina en qüestió. És a dir, es pot instal·lar un servidor web no solament en el port 80, sinó en qualsevol altre.

La detecció del sistema operatiu de la màquina remota es basa en el fet que l'estàndard del protocol IP no especifica com s'ha de respondre a paquets IP mal formats. La tècnica rep el nom de *TCP/IP stack fingerprinting*. La manera com un sistema operatiu respon a paquets mal formats depèn de cada implementació concreta, per la qual cosa cada fabricant o implementador de la pila de protocols IP dissenya les respostes al seu gust. Això proporciona una via per a determinar quin sistema operatiu es troba en la màquina auditada.

Les eines que duen a terme aquesta tasca disposen d'una base de dades de respostes típiques per a cada sistema operatiu. A partir dels paquets de resposta rebuts, es pot identificar un sistema operatiu de la màquina remota amb una elevada probabilitat d'encert.

Respecte a la identificació del servei que es troba darrere de cada port TCP o UDP, ja hem esmentat que la IANA, a més de ser la responsable de l'assignació d'adreces IP, s'encarrega també de l'assignació de ports. Tanmateix, això no im-

plica que sigui necessari respectar aquestes assignacions per al funcionament correcte d'una aplicació. Per tant, quan un port està obert, no es pot inferir directament que el servei que hi ha al darrere es correspon amb el previst per la IANA. És necessari recórrer a algun mecanisme per a identificar el servei.

Habitualment, la tècnica utilitzada és fer una connexió al port en qüestió i observar quin missatge inicial es retorna. Sovint, aquest missatge conté el nom del servei i fins i tot la versió. Per tant, es poden aplicar sistemes similars als explicats anteriorment per a identificar el sistema operatiu. Les eines disposen d'una base de dades de respostes típiques a certs paquets IP de prova. Aquesta tècnica se sol denominar *banner grabbing*. Malgrat l'eficàcia aparent d'aquesta eina, el seu ús no és de gaire utilitat quan els serveis no mostren cap informació. A més, si presenten alguna, s'ha de desconfiar *a priori*. Per tant, aquesta tècnica ha perdut gairebé totalment la validesa, encara que es pot seguir considerant.

Respecte a les eines disponibles per a fer aquesta tasca, de nou destaca sobre gairebé qualsevol altra NMAP, encara que també es pot considerar AMAP. A més de permetre fer l'escaneig de ports, NMAP es pot emprar per a identificar el sistema operatiu que utilitza una màquina, i els serveis que s'executen darrere de cada port. L'opció a emprar en NMAP per a identificar el sistema operatiu és –O, i per a identificar els serveis –sV. L'opció –A fa totes dues coses alhora.

Identificar sistema operatiu i servei - NMAP línia d'ordres

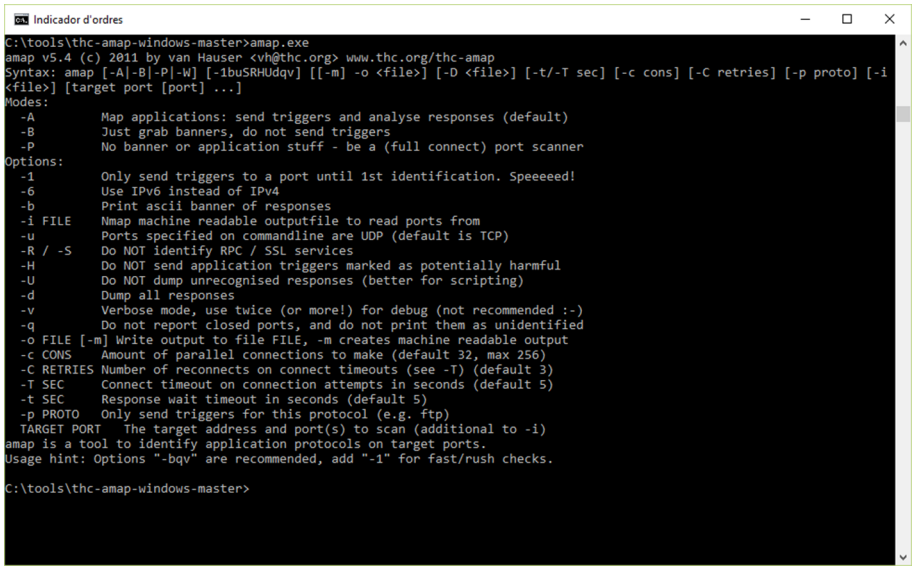
```
C:\Program Files (x86)\Nmap>nmap.exe -A 192.168.43.1

Starting Nmap 7.12 ( https://nmap.org ) at 2016-09-19 22:05 Romanç Daylight Estafi
Nmap scan report for 192.168.43.1
Host is up (0.0075s latency).
Not shown: 999 filtered ports
PORT STATE SERVICE VERSION
53/tcp open domain dnsmasq 2.62
| dns-nsid:
|_ bind.version: dnsmasq-2.62
MAC Address: 9C:D3:5B:9B:29:CF (Samsung Electronics)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X|3.X
US CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
US details: Linux 2.6.32 - 3.10, Linux 2.6.32 - 3.13, Linux 3.2 - 3.16
Network Distance: 1 hop

TRACEROUTE
HOP RTT  ADDRESS
1 7.47 ms 192.168.43.1
```

```
US and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap doni: 1 IP address (1 host up) scanned in 31.99 seconds


C:\Program Files (x86)\Nmap>
```



Eina AMAP

Ús d'AMAP per a identificar serveis

```
C:\tools\thc-amap-windows-master>amap 127.0.0.1 135 445 1688
amap v5.4 (www.thc.org/thc-amap) started at 2016-09-19 22:22:00 - APPLICATION MAPPING mode


Protocol on 127.0.0.1:1688/tcp matches netbios-session
Protocol on 127.0.0.1:135/tcp matches netbios-session
Protocol on 127.0.0.1:445/tcp matches ms-ds


Unidentified ports: none.


amap v5.4 finished at 2016-09-19 22:22:18


C:\tools\thc-amap-windows-master>
```

4.6.3. Investigació de vulnerabilitats

Les fases que s'han explicat fins ara són les prèvies a la investigació de vulnerabilitats, que és la fase que principalment interessarà l'auditor. Quan l'auditor ja coneix el sistema operatiu d'una màquina, els serveis que estan publicats a la xarxa (i la seva visibilitat des de diferents punts de la xarxa), i les versions de tots dos, pot passar a aquesta fase següent. L'anàlisi de vulnerabilitats consistirà a comprovar si hi ha alguna vulnerabilitat coneguda que afecti el sistema operatiu o els serveis en qüestió. A més d'això, posteriorment es podria fer una investigació de noves vulnerabilitats, però això requereix uns coneixements tècnics molt més avançats i, a més, no es pot garantir un resultat concret. Cal

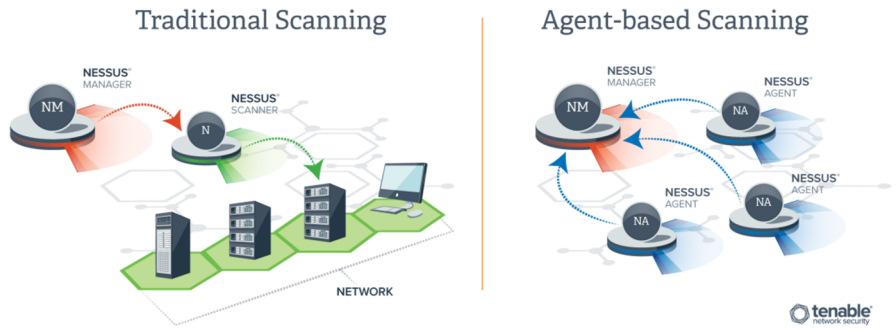
tenir en compte que el fet de no identificar cap vulnerabilitat en una màquina no significa que aquesta sigui completament segura. Només implica que, fins ara, es desconeix si hi ha vulnerabilitats. Una vegada executada aquesta fase, l'auditor finalitzarà la seva feina.

Per a fer el procés d'investigació de vulnerabilitats, s'utilitzaran bases de dades que permeten saber quines vulnerabilitats hi ha per a cada versió d'un servei o sistema operatiu. Una vegada trobades les vulnerabilitats dels serveis i el sistema operatiu en qüestió, es comprovarà si realment aquestes vulnerabilitats hi són presents. Aquest procés pot ser molt llarg i costós, per la qual cosa habitualment l'auditor utilitzarà eines que automatitzen aquestes proves. A més, aquestes eines poden automatitzar no solament aquesta fase, sinó també les anteriors.

Entre les eines existents, tant comercials com del moviment de programari lliure, s'ha de destacar molt especialment *Nessus*, que s'ha estès com l'eina més emprada comunament pels auditors de seguretat. Un dels seus punts forts és l'arquitectura. Hi ha diverses modalitats de l'eina, però la més emprada pels auditors s'instal·la en un sistema que actua de sonda des d'on es realitzen els escanejos. L'auditor accedeix a l'eina via una interfície web. En modalitats més avançades de l'eina, l'auditor pot instal·lar diferents sondes en diferents segments de xarxa i coordinar els escanejos de cada sonda des d'un punt central. Un altre dels aspectes que li confereixen gran versatilitat és que ha integrat diferents eines com *NMAP*, *HYDRA* (per a fer proves de contrasenyes en cerca de vulneracions de la política de contrasenyes de l'organització), *NIKTO* (per a comprovar *scripts* i CGI en servidors web), un motor per a realitzar comprovacions de configuracions de sistemes (s'ha de facilitar a la sonda accés remot al sistema que ha de comprovar), etc.

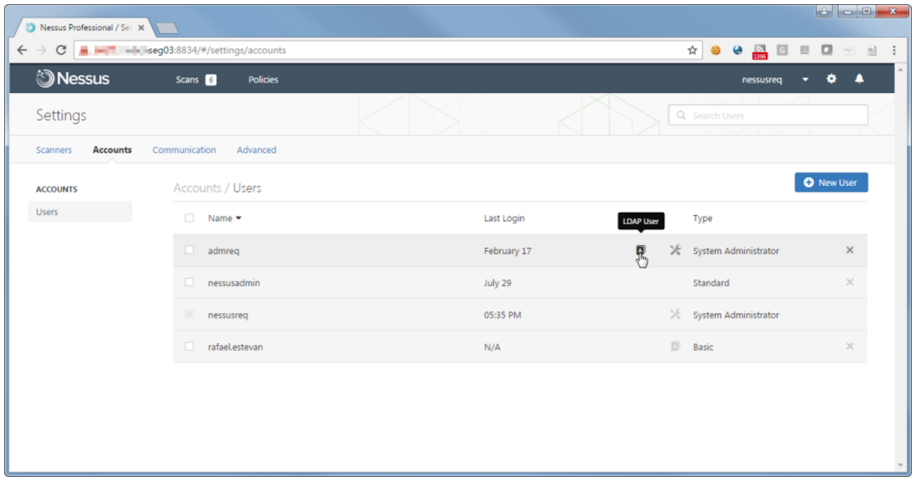
Les diferents versions de Nessus permeten realitzar desplegaments en grans infraestructures, especialment amb la versió Nessus Manager, la qual permet tant integrar diferents sondes Nessus com també l'ús d'agents instal·lats en els sistemes i que reporten al servidor central de Nessus Manager. Aquesta solució facilita enormement la gestió de credencials amb privilegis elevats i, a més, és necessària per a realitzar escanejos en profunditat en els sistemes.

Diferents modalitats de desplegament de Nessus Manager



Font: Tenable

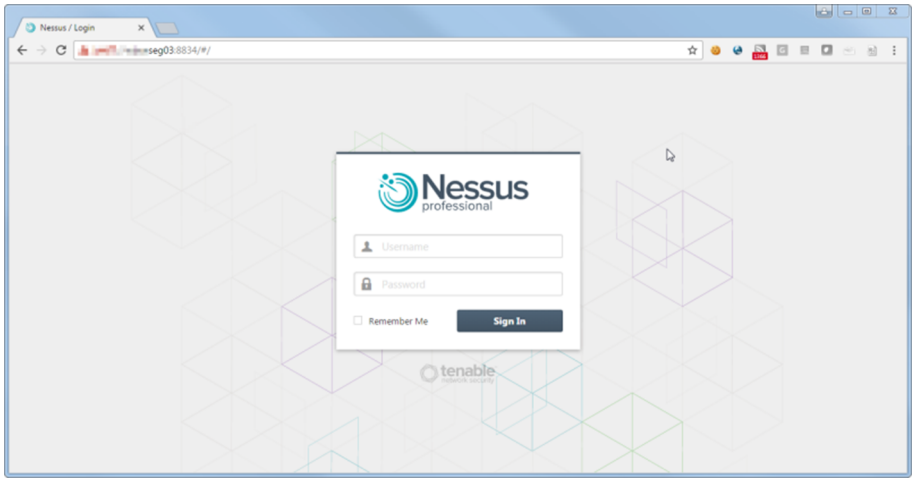
La manera de treballar més habitual per a un auditor és que empri la seva pròpia màquina per a executar el servidor. Convé comprovar que el port que utilitza el servidor web de Nessus estigui obert, per a poder connectar amb un navegador. Com que es tracta d'una arquitectura client/servidor, s'ha de crear prèviament un usuari en el servidor perquè s'hi pugui accedir des del client.



Usuaris definits en el servidor Nessus (versió Windows)

Hi ha diferents tipus de rols d'usuaris i la possibilitat de compartir certa informació entre ells. El nivell de versatilitat depèn de la versió de Nessus. Per exemple, amb la versió Nessus Manager hi ha la possibilitat d'integrar usuaris d'un directori LDAP per a realitzar l'autenticació de manera centralitzada.

L'accés a l'eina es realitza amb un simple navegador, emprant l'usuari definit prèviament.

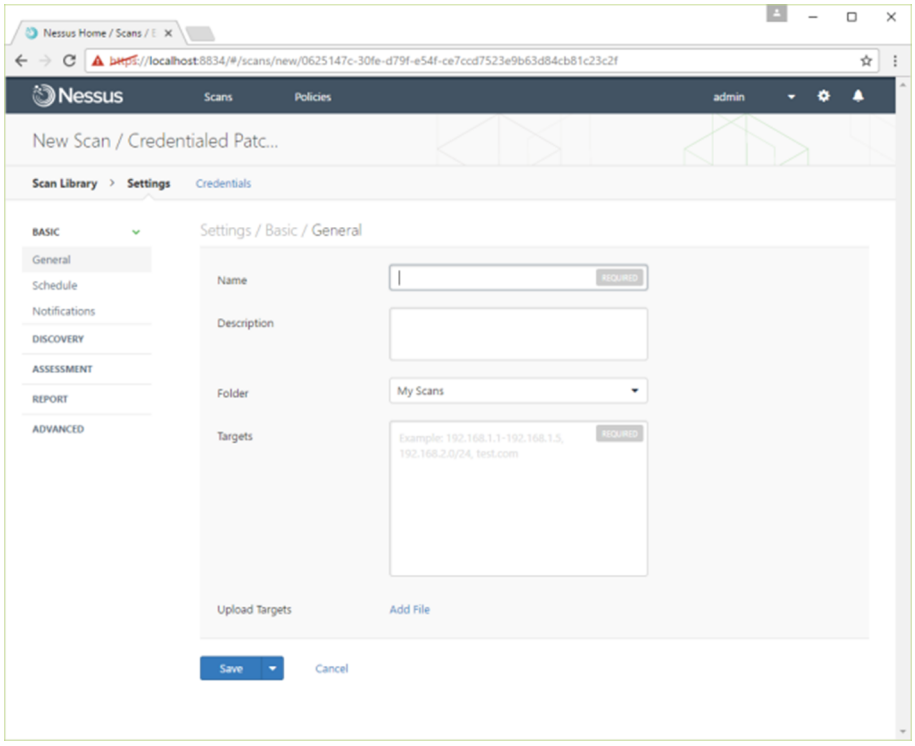


Configuració del client Nessus (versió Windows)

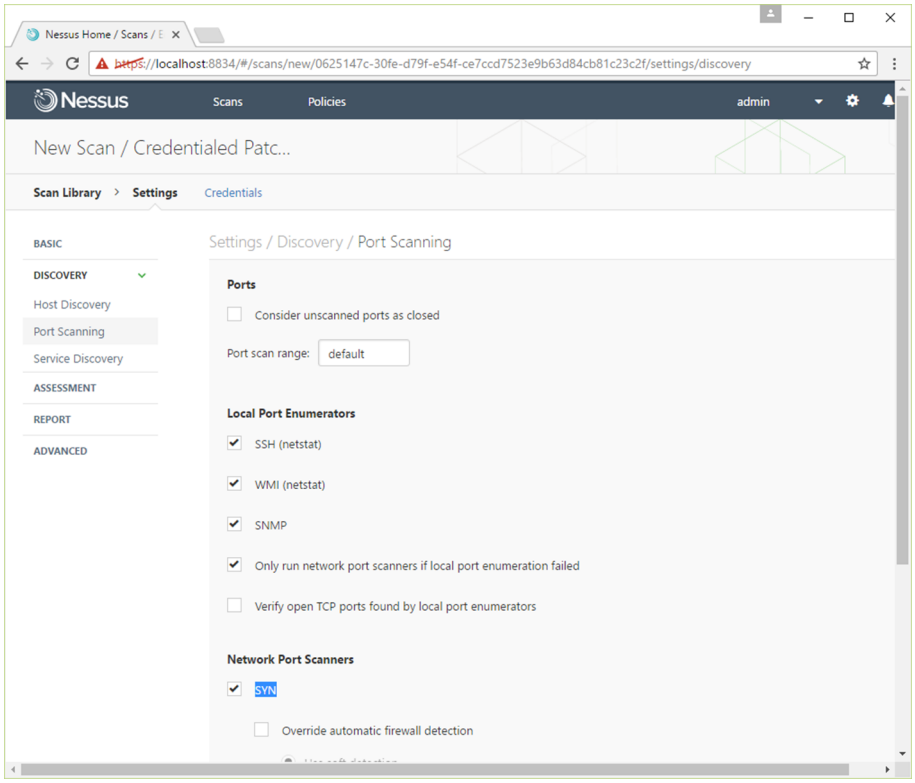
Nessus implementa les dues fases anteriorment exposades i fins i tot comprova les vulnerabilitats conegudes.

Mètodes d'escaneig de Nessus

Nessus empra els mateixos mètodes que NMAP per a fer l'escaneig d'IP i ports, i permet configurar l'escaneig segons els diferents mètodes existents, i fins i tot emprar directament NMAP.

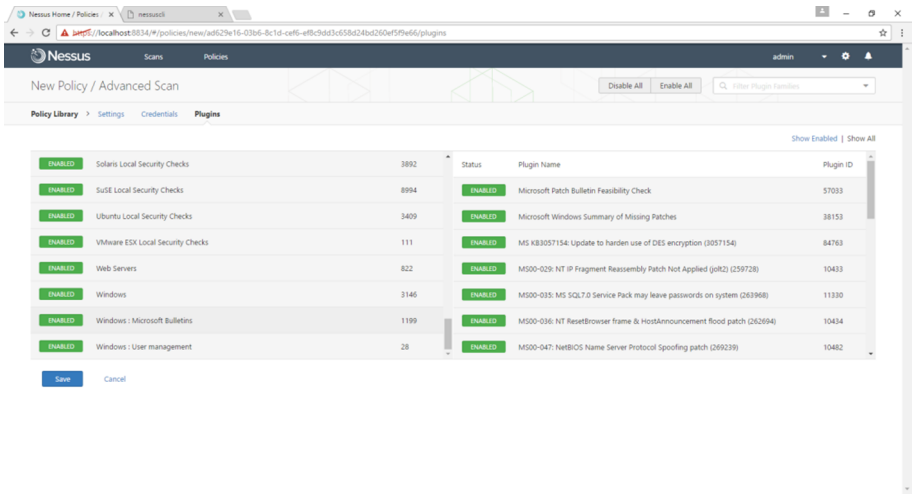


Configuració de l'abast



Configuració dels paràmetres d'escaneig (versió Windows)

La prova de vulnerabilitats es fa mitjançant l'ús de connectors (*plug-in*). Els connectors són petits components integrables en el servidor Nessus que han estat dissenyats pel proveïdor de l'eina. Cada connector permet comprovar una vulnerabilitat concreta.

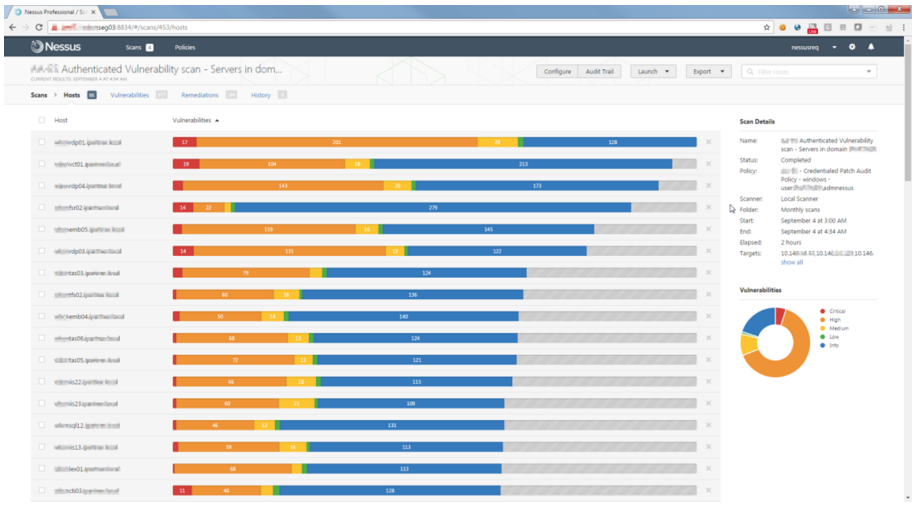


Nessus: selecció de connectors

La base de dades de connectors està organitzada per temàtiques, perquè l'auditor pugui seleccionar únicament els que siguin pertinents. Així mateix, els connectors que poden causar una interrupció del servei estan marcats com a perillosos, i es poden seleccionar o desseleccionar senzillament per a evitar que la realització de les proves tècniques de l'auditoria causin una interrupció

d'un servei. De totes maneres, aquest aspecte s'ha de consensuar amb l'auditat i, en cas de dubte, l'auditor ha d'evitar qualsevol tipus de prova que afecti de manera negativa els sistemes de l'auditat.

Per tant, l'auditor seleccionarà únicament els connectors que es corresponguin amb el pla d'auditoria previst. Els resultats de l'anàlisi es mostraran organitzats d'acord amb les adreces IP de les màquines escanejades, i és interessant destacar que cada vulnerabilitat estarà valorada emprant el sistema CVSS.



Exemple d'un escaneig de vulnerabilitats amb Nessus sobre un conjunt de servidors que pertanyen a un domini Windows

La qualitat de l'anàlisi obtinguda mitjançant Nessus (i, en general, mitjançant qualsevol altra eina, ja que totes empren el mateix esquema de proves), depèn exclusivament de la qualitat dels connectors que fan les proves, i el grau d'actualització de la base de dades de connectors. Per tant, que aquesta base de dades estigui actualitzada és essencial per a la qualitat dels resultats.

A mesura que les vulnerabilitats són descobertes, el fabricant de Nessus dissenya els connectors necessaris per a comprovar-les. A part de Nessus, hi ha altres eines similars de fabricants, com Nexpose i Qualys entre d'altres, i també dins de l'àmbit del moviment de Programari Lliure hi ha l'eina OpenVAS (creada a partir d'una versió de Nessus quan aquesta encara tenia una llicència d'ús més públic). OpenVAS té la peculiaritat que els connectors són creats per la comunitat d'usuaris de l'eina. En general, totes aquestes eines aconsegueixen, d'una manera o una altra, mantenir les actualitzacions dels connectors de manera que es puguin detectar noves vulnerabilitats en productes a mesura que la comunitat de seguretat les va descobrint i publicant.

De vegades, per a vulnerabilitats especialment greus, algunes eines (especialment les de pagament) realitzen aquest procés en un sol dia. De la mateixa manera, és important que l'auditor mantingui correctament al dia la seva eina d'anàlisi de vulnerabilitats; per a això, segons el tipus d'eina, s'haurà de subscriure als serveis d'actualització d'aquest programari i pagar per ells si pensa usar-los amb finalitats comercials.

És important aclarir que el treball de l'auditor de sistemes informàtics és proper al de l'investigador de seguretat TIC, però no és el mateix. El treball d'un investigador de seguretat TIC no se centra a detectar vulnerabilitats ja conegudes, sinó que pretén buscar-ne de noves encara no conegudes. En canvi, l'auditor se centra a comprovar com s'han implementat els controls tècnics de seguretat, i a identificar les vulnerabilitats conegudes que els puguin afectar. La identificació d'una vulnerabilitat coneguda revela un error en el manteniment dels sistemes. Per tant, quan l'auditor revisa una infraestructura tecnològica, únicament es preocupa de l'existència d'alguna de les vulnerabilitats conegudes.

D'altra banda, cal destacar que és possible que l'organització decideixi actualitzar els sistemes en dates fixes i no quan apareguin les vulnerabilitats. En aquest cas, l'auditor s'haurà de plantejar la idoneïtat d'aquesta política, i no específicament la seva implementació.

En aquest sentit, l'auditor disposarà de la informació de les últimes vulnerabilitats conegudes, independentment del seu reconeixement o no per part del fabricant del programari o dispositiu afectat. Sovint, les vulnerabilitats són detectades per equips d'analistes/investigadors de seguretat independents, els quals comuniquen a la comunitat d'usuaris l'existència d'un risc potencial en algun dispositiu o servei. Més tard, el fabricant reconeix la vulnerabilitat i emet alguna solució, habitualment mitjançant un pegat de programari que s'ha d'instal·lar. Per tant, l'auditor ha de conèixer les vulnerabilitats més recents i poder identificar aquelles per a les quals es disposa d'una solució i aquelles que no tenen encara una solució coneguda. Aquesta diferenciació permet determinar la gravetat d'una constatació i discriminar entre errors d'apedaçament, debilitats de la política d'apedaçament (per exemple, per a imposar un calendari d'actualitzacions estricte i poc freqüent), o bé problemes coneguts en els sistemes pels quals no es disposa de solució.

Tal com hem dit al principi d'aquest apartat, hi ha moltes fonts d'informació públiques i de pagament sobre vulnerabilitats. Les eines d'anàlisi de vulnerabilitats també empren aquesta informació i solen oferir un servei d'actualització d'aquestes. De fet, l'agilitat amb què el proveïdor proporcioni les actualitzacions és un punt crític amb el qual comparar la qualitat de diferents eines, com també ho és la població potencial de sistemes que siguin capaços d'examinar.

Altres eines de proves de vulnerabilitats

Hi ha altres eines que implementen el mateix tipus de proves que fa Nessus. Entre aquestes, podem destacar les següents:

1) Pel seu valor "històric", podem destacar COPS, TITAN i SATAN, desenvolupades per Dan Farmer i Wietse Venema. Aquestes van ser les primeres eines d'anàlisi de vulnerabilitats internes en servidors Unix. Actualment, SARA i SAINT són una evolució de SATAN, i permeten anàlisis remotes de vulnerabilitats.

2) Posteriorment, han aparegut moltes altres aplicacions, tant de codi font obert com comercials: ISS Internet Scanner, QualysGuard, eEye Retina Network Security Scanner, GFI LANguard Network Security Scanner, Vigilante SecureScan, N-Stealth, Shadow Security Scanner, Cerberus Internet Scanner, entre d'altres.

3) El mateix concepte d'anàlisi de vulnerabilitats que fa Nessus (i les exposades en el punt anterior) s'ha estès a les aplicacions web, i s'han creat eines per a l'anàlisi de vulnerabilitats d'aplicacions. Entre les eines comercials de comprovació de vulnerabilitats, hi ha: Nexpose, Qualys, WebInspect, de SPI Dynamics; AppScan, d'IBM; AppDetective, d'Application Security; ScanDo, de Kavado; N-Stealth Security Scanner, de N-Stalker, i Web Vulnerability Scanner, d'Acunetix.

Finalment, hem de destacar que els els auditors han d'usar aquestes eines amb cura, perquè de vegades generen resultats falsos, per més evolucionades que siguin. Per tant, els resultats d'aquestes eines han de ser sempre analitzats i, arribat el cas, s'han de fer proves manuals de la vulnerabilitat revelada.

4.7. Revisió de la seguretat en xarxes sense fil 802.11

La revisió de la seguretat en xarxes sense fil 802.11 és una tasca que, essencialment, és la mateixa que per als seus anàlegs de les xarxes fixes. Les fases d'enumeració de sistemes i anàlisis de ports i serveis, i l'avaluació de les vulnerabilitats dels serveis, són les mateixes. No obstant això, la seva naturalesa és especial pel fet de mancar d'un mitjà de transmissió físic. En el seu lloc, el mitjà utilitzat és l'espai radioelèctric, al qual pot tenir accés qualsevol intrús. Per tant, la seva revisió ha d'incloure a més la verificació dels controls que gestionin riscos específics.

4.7.1. Riscos de les xarxes sense fil 802.11

Tota implantació de xarxes sense fil s'ha de fer tenint present que, a més dels riscos habituals que comporten els sistemes TIC, per la seva peculiaritat, aquelles estan exposades a riscos nous. Aquests riscos es poden recopilar en les categories següents:

- Atacs d'inserció de trànsit.
- Intercepció i/o monitoratge del trànsit de la xarxa sense fil.
- Denegacions de servei.

Atacs d'inserció de trànsit

Usuaris no autoritzats poden intentar fer ús de la xarxa sense fil. Per a això, abans s'hauran d'associar al punt d'accés, la qual cosa pot ser senzilla o no segons si s'implementen mesures de xifratge a la xarxa sense fil, o algun altre mecanisme com ara la limitació per adreces MAC. Tanmateix, aquesta última mesura (limitació per adreces MAC) no és efectiva, ja que l'atacant pot examinar tots els paquets que circulin per la xarxa sense fil, llegir les adreces MAC autoritzades (encara que s'hi empri un xifratge, les capçaleres de la capa d'accés al mitjà no estan xifrades) i canviar la seva adreça MAC per a fer ús de la xarxa quan no hi estigui l'usuari legítim.

Un altre risc, en aquest mateix sentit, és la instal·lació de punts d'accés no autoritzats. Aquests poden ser instal·lats per usuaris maliciosos per a aconseguir que els usuaris legítims de la xarxa sense fil s'hi associïn. A partir d'aquí, els usuaris legítims poden ser atacats fàcilment. Els punts d'accés poden ser instal·lats també per personal propi de l'organització per a la seva pròpia comoditat, però sense l'autorització ni el control de l'àrea de seguretat o de gestió TIC. Per tant, aquests punts d'accés són susceptibles de ser atacats.

Una vegada associat l'atacant amb la xarxa sense fil, té a la seva disposició un vector d'atac contra sistemes que hi estiguin connectats. Si l'atacant ha aconseguit associar-se a un punt d'accés corporatiu, podrà atacar les seves màquines i ens trobarem davant una situació similar a la d'un atacant amb accés físic a la xarxa fixa. Els riscos que se'n deriven són els mateixos.

Un sistema especialment susceptible de ser atacat per l'intrús és el mateix punt d'accés. Com qualsevol altre sistema informàtic, no és exempt de la possibilitat de tenir vulnerabilitats, i aquestes se solen explotar des de la seva interfície d'administració. Per aquesta raó, és una bona pràctica limitar l'accés a la interfície d'administració únicament des del costat de la xarxa fixa, i prohibir-lo des del costat sense fil.

Si trobem un punt d'accés que ha estat instal·lat sense autorització, els riscos que afecten els usuaris legítims són els mateixos que en el cas anterior.

Intercepció i/o monitoratge del trànsit de la xarxa sense fil

La naturalesa sense fil d'aquestes comunicacions fa que sigui possible l'escolta passiva d'aquestes sense intervenció al canal. Per tant, és necessari proveir la infraestructura de mecanismes per a reduir aquest risc. Actualment, l'estàndard 802.11 facilita diferents mitjans: el protocol WEP, que ha demostrat ser insegur per a totes les longituds de clau sigui quina sigui la complexitat de la contrasenya, i el protocol WPA (des de la definició de l'estàndard 802.11i), que té diferents modalitats. La modalitat més bàsica és la PSK (*pre-shared key*), i és també la més àmpliament implantada. Altres modalitats més robustes, i també més recomanades, són l'autenticació contra servidors RADIUS, o l'ús de certi-

ficats digitals. També es poden utilitzar xarxes privades virtuals (VPN) sobre la xarxa sense fil, tant en mode transport com túnel, però això no impedeix que l'intrús pugui continuar accedint a la xarxa. L'avantatge de les VPN és que l'atacant no pot interceptar o inspeccionar el trànsit dels usuaris legítims, però sí que pot fer atacs contra la disponibilitat de la xarxa, tal com comentarem a continuació.

Denegacions de servei

La denegació de servei en una xarxa sense fil és un risc al qual està constantment exposada i que és de difícil mitigació. Qualsevol equip de ràdio capaç d'emetre en la banda dels 2,4 GHz pot interferir, intencionadament o no, en el funcionament d'una xarxa 802.11. Per això, abans d'instal·lar una xarxa d'aquest tipus, s'han d'identificar les fonts de radiació en aquesta banda, i també els requisits de disponibilitat que ha de complir la xarxa. El control de la interferència és difícil, encara que es pot intentar utilitzar antenes direccionals i triangulació per a detectar la font origen de la interferència i neutralitzar-la.

De manera intencionada, un atacant disposa de diferents tècniques per a inutilitzar una xarxa sense fil: inundació de la xarxa amb trames de desautenticació i de desassociació, enviament de trames d'autenticació mal formades (que causin que el punt d'accés desautentiqui l'usuari legítim), saturació de la memòria dels punts d'accés amb sol·licituds d'autenticació, etc.

Finalment, per a aplicacions crítiques, és possible que no sigui recomanable l'ús d'aquesta tecnologia, encara que els beneficis que comporta poden portar l'organització a assumir els riscos. En tot cas, és un risc que l'organització no ha de menystenir.

4.7.2. Política corporativa de seguretat per a les xarxes sense fil

Les organitzacions que implantin xarxes sense fil han de gestionar, adequadament, els riscos exposats anteriorment. Hi ha d'haver una política corporativa de seguretat per a les xarxes sense fil que s'integri amb la resta de les polítiques i sistemes de gestió de la seguretat de la informació. Aquesta política ha de definir l'arquitectura, els usos legítims i els mecanismes de protecció, incloent-hi aspectes recomanables com els següents:

- Tractar els punts d'accés com a xarxes de no-confiança. Això implica que les xarxes sense fil s'han de tractar com si fossin xarxes externes. Per tant, s'hi haurien d'aplicar una o diverses de les mesures de protecció següents: separar les xarxes sense fil de la resta de la infraestructura amb un tallafoc; configurar l'accés des d'aquestes xarxes a la xarxa corporativa per mijtà de VPN; disposar de sistemes de detecció d'intrusions (IDS); implantar mecanismes d'identificació i autenticació per a l'accés a qualsevol recurs de la xarxa corporativa des d'aquestes xarxes, entre altres.

Això també implica que s'han de protegir els equips corporatius que es connectin per mitjà d'aquestes xarxes, com si estiguessin en xarxes no confiables, com és el cas d'Internet. Això comporta les mesures següents:

– Ús de tallafocs personals en els equips.
– Accessos mitjançant VPN als serveis corporatius, a més del xifratge requerit per a accedir a la xarxa sense fil.
– Ús de programari per a detectar amenaces (virus, programes maliciosos, etc.), d'acord amb la política corporativa a aquest efecte.

- Disposar d'una política de configuració dels punts d'accés. Els administradors haurien de disposar d'una política que descrigui la configuració bàsica que s'ha de donar als punts d'accés, la qual ha de reflectir: SSID a emprar, tipus d'encriptació (descartar WEP i usar com a mínim WPA amb una contrasenya complexa i actualitzada periòdicament), valors de les comunitats SNMP.

- Auditories periòdiques de la seguretat de les xarxes sense fil:
  – Política de revisió periòdica de la cobertura de les xarxes sense fil per a identificar punts d'accés no autoritzats i verificar les àrees cobertes.

  – Auditoria periòdica dels punts d'accés: vulnerabilitats dels serveis que ofereix, fortalesa dels mecanismes de xifratge, regles de filtratge de trànsit que s'hi apliquin, valors de les comunitats SNMP configurats en els agents instal·lats, etc.

  – Anàlisi periòdica de la seguretat dels equips client, per a detectar errors de configuració o insuficiències en les polítiques de seguretat definides.

4.7.3. Proves d'auditoria per a la revisió de xarxes sense fil

Com es pot observar, la implantació de xarxes sense fil té certes diferències respecte a les xarxes fixes. Per tant, l'auditor s'hauria de plantejar revisions de seguretat de la mateixa manera, però amb certes peculiaritats. A més de les tasques d'avaluació de la seguretat que trobem en un altre tipus d'entorns TIC, les proves d'auditoria haurien de preveure el següent:

- Revisió de la cobertura de la xarxa sense fil. Un dels factors que s'hauran de tenir en compte és l'avaluació del plànol de cobertura, per a evitar-ne l'extensió més enllà de les instal·lacions en la mesura que es pugui. És important que la cobertura es redueixi el màxim possible a les zones on es pretén oferir el servei, mitjançant l'ajust de la potència dels punts d'accés i l'ús d'antenes amb diagrames de radiació no omnidireccionals.
  Les proves destinades a comprovar la manera com es gestiona el risc han de seguir els passos següents:

  - Establir amb l'auditat quin és l'àmbit previst per a la xarxa sense fil. És a dir, conèixer les instal·lacions, els punts d'accés planificats i les àrees de cobertura previstes.

  - Avaluar l'abast de la instal·lació sense fil. Per a això, l'auditor ha de fer visites d'auditoria amb una eina que mesuri la potència de senyal rebut en diversos punts de les instal·lacions i també fora d'aquestes instal·lacions. Les eines més tradicionals per a aquesta tasca solen ser els analitzadors NetStumbler o Kismet, que a més es poden combinar amb eines de representació gràfica i fins i tot amb dispositius GPS externs que registrin, de manera automàtica, les coordenades i els nivells de potència de tots els punts d'accés detectats. Actualment hi ha múltiples eines (algunes comercials, com Acrylic Wifi o Ekahau Site Survey) que, mitjançant interfícies gràfiques i l'ús de posicionadors GPS, ajuden a generar una anàlisi de cobertura de xarxes wifi. D'aquesta manera, l'auditor obtindrà un plànol de les instal·lacions i dels voltants amb la cobertura de ràdio de cadascun dels punts d'accés instal·lats.

- Identificar fonts d'interferències o de punts d'accés no autoritzats. Les eines i tècniques seran molt similars a les descrites en el punt anterior. No obstant això, ara l'auditor no estudiarà els punts d'accés corporatius, sinó que intentarà descobrir punts d'accés no autoritzats i també identificar fonts d'interferències en la mateixa banda de freqüència.

- Control d'accés al mitjà. Finalment, l'auditor ha d'avaluar els mecanismes de control d'accés al mitjà implantats a les xarxes sense fil. Això implica que l'auditor identificarà la xarxa i observarà el tipus de xifratge. A data d'elaboració d'aquest material, es pot considerar que el xifratge que ofereix per WEP no és segur per a cap de les dues longituds de clau que ofereix (40 o 104 bits), independentment de la complexitat de la clau. El xifratge recomanat és, com a mínim, WPA amb claus amb una certa complexitat. Encara seria millor que, si es disposa de maquinari modern o actualitzable, s'utilitzés WPA2. Tots dos protocols són similars, però WPA empra com a algorisme simètric de xifratge RC4, el qual s'ha demostrat que no és segur en cas d'emprar claus poc complexes (és possible descobrir la clau WPA aplicant atacs amb diccionari en molt poc temps i amb molt pocs paquets capturats). En canvi, WPA2 utlitza AES, que fins ara no ha estat compromès.

Les eines per a fer aquest tipus de proves són molt variades: *kismet*, *airodump*, *aireplay*, *aircrack, airdecap*, entre altres, així com distribucions de Linux per a auditors especialitzades en anàlisis de seguretat com Kali (més generalista) o Wifislax (especialitzada en anàlisi de xarxes wifi). No obstant això, cada dia apareixen noves tècniques, per la qual cosa es recomana que l'auditor recorri a un expert, o bé es mantingui al dia en l'auditoria del xifratge de xarxes sense fil.

4.8. Tècniques d'anàlisi de vulnerabilitats d'aplicació

Les auditories d'aplicació tenen, per objecte, la verificació dels controls aplicats sobre les pròpies aplicacions i dels que aquestes incorporen en la seva lògica. Aquests controls poden tenir per objecte aspectes generals, com aplicar un control d'accés a la informació, amb les seves fases d'identificació, autenticació i posterior autorització. També poden tenir un objectiu més específic, com impedir que es generi dues vegades la mateixa factura en una aplicació de facturació. Aquest últim tipus de controls se sol denominar *control d'aplicació o de lògica de negoci*.

No hi ha tècniques dissenyades específicament per a l'auditoria de controls d'aplicació. L'auditor haurà de conèixer la lògica del negoci, l'objectiu del control i la implementació feta. Segons aquesta informació, l'auditor dissenyarà les proves que consideri necessàries per a obtenir la certesa que el control s'està aplicant correctament.

De la mateixa manera, els controls genèrics que se solen trobar als catàlegs de bones pràctiques també són extremament heterogenis, i no és possible indicar una única llista de proves a fer. No obstant això, sí que es pot recomanar l'ús de les tècniques següents:

- Anàlisi estàtica.
- Anàlisi de la configuració / parametrització dels sistemes.
- Anàlisi dinàmica: anàlisi d'aplicacions web.

4.8.1. Anàlisi estàtica

L'anàlisi estàtica consisteix en la revisió sistemàtica del codi font d'una aplicació, amb el propòsit de corregir errors en les primeres fases del seu cicle de vida. D'aquesta manera, es millora la qualitat general del programari i, al mateix temps, es redueix el nombre de vulnerabilitats potencials en un sistema. Sense cap dubte, una anàlisi de codi és la millor prova que es pot fer per a prevenir les vulnerabilitats més comunes.

Exemples de vulnerabilitats més comunes

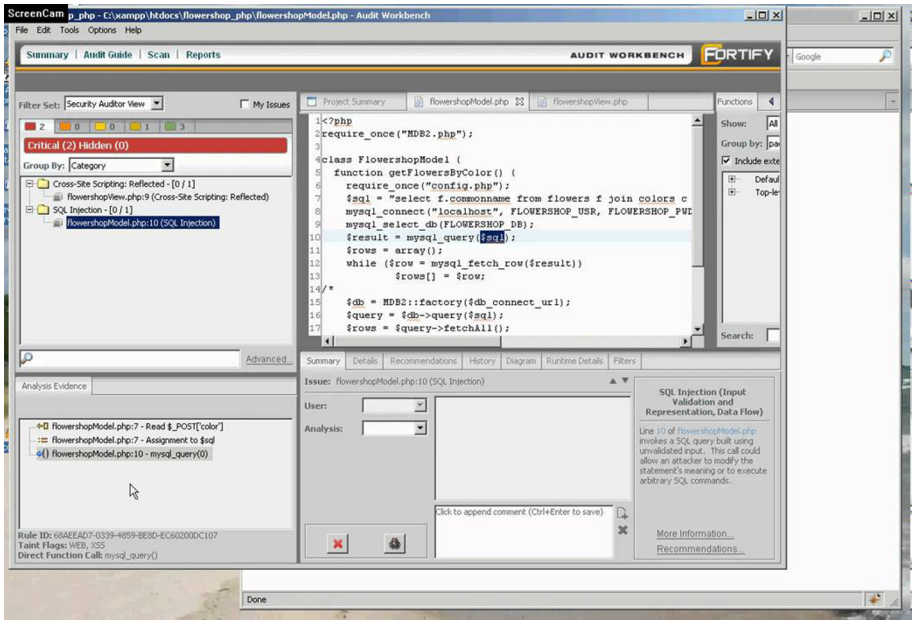
Falta de control en les cadenes d'entrada, condicions de carrera, gestió incorrecta de la memòria, desbordaments de memòries intermèdies o *buffers*, etc.

Aquesta anàlisi estalvia també molts costos a les organitzacions desenvolupadores de programari. No obstant això, aquest tipus de proves requeriran una gran experiència de l'auditor, i un gran coneixement del llenguatge en què estigui desenvolupada l'aplicació.

Hi ha un gran nombre d'eines per a facilitar, i en certa manera automatitzar, les tasques de revisió de codi. No obstant això, aquesta tasca és bàsicament manual, i les eines només serviran per a facilitar la revisió del codi, realització i inventariat de reconeixements sistemàtics automàtics i la realització de recerques elaborades, i tots aquests resultats han de ser examinats per l'auditor per a identificar els falsos positius dels positius reals. En podem destacar:

- *Flawfinder*. Examina codi C i C identificant possibles problemes i calculant, per a cadascun, un nivell de risc.

- *Fortify source code analysis*. Eina comercial que s'integra amb els entorns integrats de desenvolupament (IDE) més habituals i permet fer una revisió de codi en temps de codificació. Suporta un gran nombre de llenguatges.



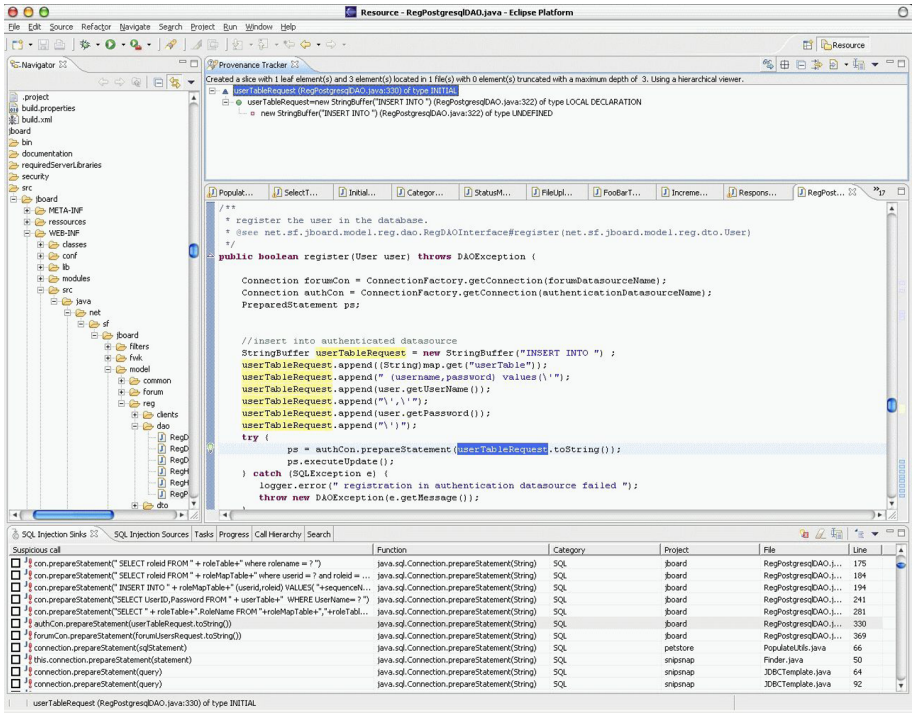
Eina Fortify analitzant codi PHP

- IBM Appscan. És una eina d'anàlisi estàtica de codi per a aplicacions web i mòbils.

- Veracode. Aquest és un altre dels líders quant a anàlisi de codi, que facilita gran nombre d'eines, des d'analitzadors de codi estàtic (el qual ens ocupa)

a solucions completes integrades de gestió del cicle de desenvolupament del programari.

- LAPSE. Especialment dissenyada per a servir de suport en el procés de revisió de codi d'aplicacions Java J2EE. Permet localitzar vulnerabilitats potencials en aplicacions web (manipulació dels paràmetres d'entrada, manipulació de les capçaleres dels missatges HTTP, manipulació de galetes, injeccions de codi en els paràmetres d'entrada, etc.). Aquesta eina s'integra amb l'entorn de desenvolupament Eclipse i permet que la revisió de codi es faci en paral·lel a la codificació.



Eina LAPSE integrada en l'IDE ECLIPSE

4.8.2. Anàlisi de la configuració / parametrització dels sistemes

Els elements següents poden requerir una auditoria de la configuració:

- Tallafocs.
- Encaminadors i altres elements de comunicació, com balancejadors de càrrega o commutadors gestionables.
- Sistemes operatius.
- Sistemes gestors de bases de dades.
- Aplicacions.

També és una tasca que requereix una gran experiència de l'auditor, ja que es tracta de comprovar la situació de tots els paràmetres de configuració d'un sistema. A més, per a poder determinar si un sistema està ben configurat, s'han

de tenir en compte les polítiques de seguretat de l'organització. En cas que no existeixin aquestes polítiques, l'auditor ha de donar la seva opinió d'auditoria segons els catàlegs de bones pràctiques.

Tal com hem apuntat, l'auditor necessita un bon coneixement del sistema que ha d'auditar. Com que això és complex, hi ha llistes de comprovació, o llistes de control, per a fer la revisió de la configuració d'un sistema. Les llistes de control solen contenir instruccions sobre com cal fer la configuració mínima necessària perquè un sistema es pugui integrar, de manera segura, en un entorn operacional. Alguns fabricants ja proporcionen aquestes llistes de control i, altres vegades, són terceres organitzacions les qui les faciliten. Aquestes organitzacions solen estar enquadrades en organismes públics dedicats a la seguretat de la informació o la gestió d'incidents telemàtics (els anomenats *CERT*[7]). En aquest sentit, són destacables les iniciatives següents:

[7]Per a obtenir més informació sobre la comunitat d'equips de resposta davant incidents de seguretat informàtica, podeu visitar les pàgines web: http://www.first.org o http://www.cert.org

- El National Institute of Standards and Technology (NIST) ha fet una recopilació exhaustiva de llistes de control recollint recomanacions de fabricants i criteris comuns per a diverses organitzacions governamentals americanes, i també ha emès un document (SP 800-70 *Security Configuration Checklists Program for IT products*) que dóna les indicacions necessàries per a desenvolupar una llista de control i/o emplear les llistes de control recopilades pel NIST o altres fonts. L'auditor emprarà aquest document per a construir la seva pròpia llista de comprovació segons la seva experiència i altres llistes que hi pugui haver. No hem d'oblidar que aquestes llistes de control són genèriques, i que s'hauran d'adaptar a les circumstàncies específiques de l'auditat.

- Els CERT nacionals, com, per exemple, el CCN-CERT a Espanya, publiquen guies per a la protecció de programari (amb accés restringit a usuaris registrats). L'auditor podria construir la seva pròpia llista de control a partir de les recomanacions donades en aquestes guies.

- El Center For Internet Security (CIS) ha desenvolupat els *CIS benchmarks*. Igual que les guies del CCN-CERT, aquests *benchmarks* contenen les recomanacions per a la configuració segura de diferents paquets de programari i sistemes operatius. És important destacar que aquests *benchmark* contenen el consens establert entre la National Security Agency (NSA), la Defense Information Systems Agency (DISA), el NIST, la General Services Administration (GSA), el SANS Institute, i els membres del CIS sobre la seguretat de diferents sistemes operatius i paquets de programari en relació amb la seva configuració. Els CIS *benchmarks* són similars a les llistes de control, però tenen l'avantatge que proporcionen mecanismes per a fer una valoració numèrica de la seguretat del sistema. Per tant, constitueixen una font d'informació molt valuosa per a l'auditor. Cal destacar, també, que els membres adherits al CIS tenen a la seva disposició eines amb les

quals executar en local els test descrits en els *benchmarks*, i obtenir així la puntuació directament.

En aquest punt, és interessant comentar que realitzar la verificació del compliment d'una *checklist* (llista de comprovació) pot ser una tasca llarga, però fàcilment automatitzable mitjançant *scripts* (guions) o l'ús d'eines d'escaneig. Algunes eines d'escaneig de vulnerabilitats inclouen, com a funcionalitat addicional, la realització de comprovacions de paràmetres de seguretat. En la terminologia del mercat, aquestes es denominen habitualment *compliance checks*. Eines com Nessus, Qualys o Nexpose poden realitzar aquest tipus de tasques i fins i tot el fabricant facilita els fitxers de configuració basats en fonts reconegudes com el NIST o el CIS, esmentats anteriorment. En general, aquestes eines es connecten remotament al sistema a analitzar amb credencials d'administrador o empren un agent (si s'implementa d'aquesta manera) instal·lat amb privilegis elevats, i es realitza un conjunt de verificacions que l'auditor prepara mitjançant algun tipus de fitxer de configuració. Aquesta llista de verificació pot estar realitzada en algun tipus de sintaxi pròpia del fabricador (és el cas, per exemple, de Nessus) o bé es poden acceptar llistes de configuració en els llenguatges de marques estàndards OVAL (*open vulnerability and assessment language*) i XXDF (*extensible configuration checklist description format*), conegut com a OVAL. Aquests dos estàndards formen part del conjunt d'estàndards SCAP (*security content automation protocol*). El terme *protocol* no s'ha d'entendre com un terme tècnic de comunicació de dades, sinó com un conjunt d'especificacions per a definir una manera d'actuar. En aquest cas, aquest protocol facilita l'automatització de processos relacionats amb la seguretat (aquesta sí, des del punt de vista tècnic). El NIST ha elaborat una guia introductòria per a SCAP en el document SP800-117 (*Guide to Adopting and Using the Security Content Automation*). El protocol SCAP conté diferents components:

- *Extensible configuration checklist description format* (XCCDF),
- *Open vulnerability and assessment language* (OVAL®),
- *Open checklist interactive language* (OCIL#),
- *Common platform enumeration* (CPE#),
- *Common configuration enumeration* (CCE#),
- *Common vulnerabilities and exposures* (CVE®),
- *Common vulnerability scoring system* (CVSS) i
- *Common configuration scoring system* (CCSS).

L'objecte d'aquesta estandardització és establir l'ús d'un llenguatge comú en el sector privat de la seguretat informàtica i facilitar l'intercanvi d'informació i la interoperabilitat d'eines. Un exemple d'interoperabilitat és el que acabem de comentar respecte a l'elaboració de llistes de comprovació per part d'una organització aliena a un fabricant de productes de seguretat, com pot ser un escàner de vulnerabilitats.

4.8.3. Anàlisi dinàmica: anàlisi d'aplicacions web

A continuació, presentarem l'últim grup de tècniques a la disposició de l'auditor per a l'avaluació de la seguretat. Es tracta de l'anàlisi dinàmica del programari. En aquest tipus de proves, l'auditor analitzarà el comportament del programari quan aquest es troba en execució. Aquest tipus de tasca és altament especialitzada i requereix uns coneixements tècnics elevats de programació, depuració i seguretat.

No tractarem en aquesta secció de les tècniques existents per a l'anàlisi de qualsevol codi en execució, sinó que ens centrarem en l'anàlisi dinàmica d'aplicacions web. Hi ha més tipus d'anàlisis dinàmiques d'aplicacions que entren en l'àmbit de l'enginyeria inversa de codi, la qual està fora de l'abast d'aquest curs.

El nombre d'aplicacions web que empren les organitzacions ha crescut recentment de manera considerable. Això és a causa de l'aparició d'un nou esquema d'aplicació en tres capes: la capa client –el *browser*–, la capa de presentació –el *webserver*–, i la capa que conté les bases de dades i altres sistemes que implementen la lògica de negoci –els *backends*. Aquest tipus d'aplicacions web ha crescut notablement, i molts sistemes que utilitzaven una arquitectura clàssica client/servidor han migrat ara a aquest nou esquema.

A més de les aplicacions web en tres capes, també hem de destacar el projecte OWASP, que hem comentat en el mòdul 4. Les aplicacions que utilitzen aquest tipus d'arquitectura són força similars les unes de les altres, i per això solen tenir el mateix tipus de vulnerabilitats. Per tant, i d'acord amb la metodologia descrita per OWASP, l'auditoria d'una aplicació web es compondria de les fases o proves següents[8]:

[(8)]Hem exclòs proves que, per la seva complexitat tècnica, es consideren fora de l'abast d'aquest material. Si són d'interès per al lector, el referim a la metodologia OWASP i al seu projecte OWASP *Testing Guide*.

- Recollida d'informació.
- Revisió del procés d'identificació i autenticació.
- Revisió de la gestió de sessions.
- Revisió de la validació de les dades d'entrada.

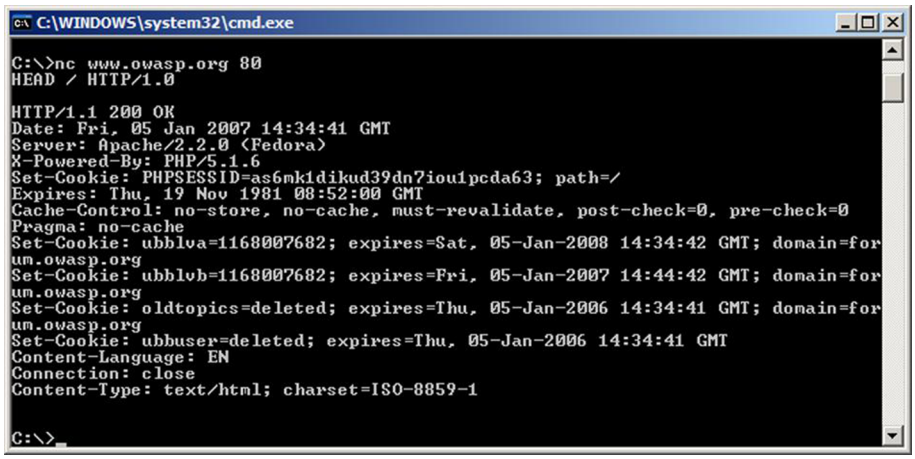
Recollida d'informació

L'objectiu d'aquesta fase és comprovar quina informació relativa a l'aplicació auditada pot ser obtinguda, de manera legítima, per mitjà dels diferents canals existents a Internet.

1) Identificació del servidor web. Identificar el tipus de servidor web que allotja la capa de presentació de l'aplicació. Si es determina correctament la versió exacta del servidor web, es podran determinar les vulnerabilitats publicades en la data de l'auditoria, i determinar la política adequada d'apedaçament/manteniment del servidor.

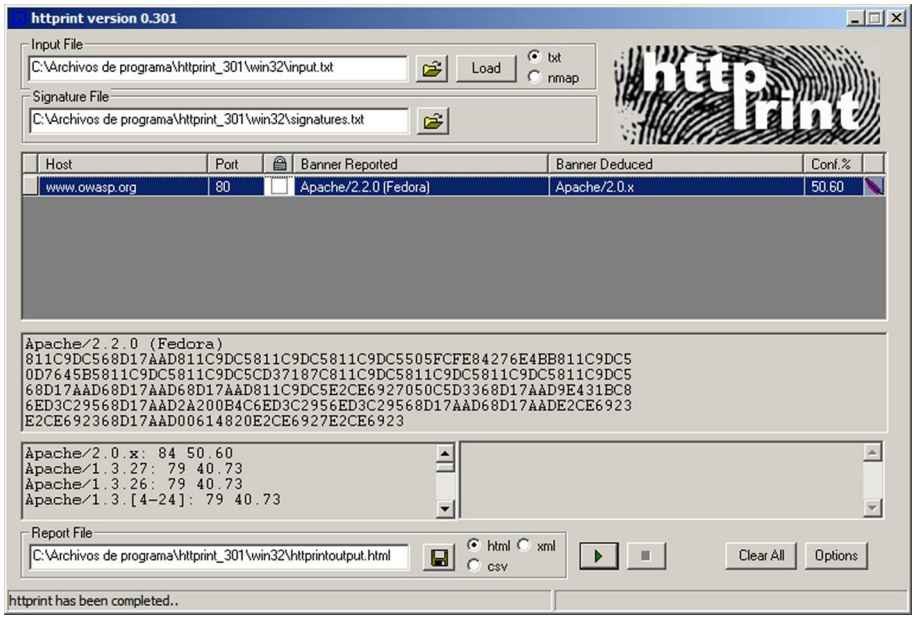
Per a fer aquesta comprovació, es connecta amb el servidor HTTP en el port 80 (o un altre si escau) utilitzant eines com les que es mostren a continuació, i així es determina quin programari i quina versió d'aquest s'estan utilitzant:

- Netcat. Permet recollir el bàner mostrat pel servidor.



Eina Netcat

- HTTPRINT: permet examinar la resposta del servidor a diverses peticions HTTP, i comparar aquestes respostes amb diferents mostres (denominades *firmes*) mantingudes en el catàleg de l'aplicació HTTPRINT.



Eina HTTPrint

D'altra banda, l'auditor ha de tenir en compte que, en l'actualitat, els servidors web permeten configurar les respostes que aquest tipus de proves analitzen, amb la qual cosa els resultats només han de ser considerats com a indicatius i no concloents.

2) Identificació de les aplicacions. Quan l'objectiu de l'auditoria consisteix en la comprovació general de la seguretat d'una infraestructura, s'hauran d'identificar totes les aplicacions o els portals servits des d'un servidor web determinat. En cas que només s'hagi d'auditar una aplicació concreta, aquesta prova no tindrà sentit. Per a identificar les diferents aplicacions que s'executen darrere d'un servidor web, es poden fer les accions següents:

- Investigar si hi ha diferents URL base que allotgen diferents aplicacions web.

Cercadors tradicionals

www.live.com,
www.dnsstuff.com,
www.google.com, etc.

- Investigar si en la IP hi ha altres aplicacions instal·lades en altres ports diferents dels estàndards (443, 8080, 8000, etc.). Per a això, es pot emprar l'eina NMAP.

- Per a identificar *hosts* virtuals i trobar els noms de dominis assignats a la IP auditada:
  - Comprovar la possibilitat de fer transferències de zona en el servidor DNS del domini examinat.
  - Comprovar la possibilitat de fer resolució inversa de noms (*reverse DNS query*).
  - Connectar amb serveis a Internet per a examinar registres DNS o usar directament cercadors tradicionals.

3) Mineria de dades. L'objectiu d'aquesta prova és extreure tota la informació allotjada sota l'aplicació web analitzada. Especialment interessant és la informació que roman oculta a l'usuari durant l'ús esperat de l'aplicació. No hi hauria d'haver informació accessible de manera pública amb dades sensibles.

Mitjançant aquesta prova, s'examinen tots els enllaços accessibles en l'aplicació, la qual cosa pot revelar informació confidencial o almenys rellevant sobre l'aplicació web. L'objecte d'aquesta prova és comprovar la fuita o filtració d'informació (*information leaking*) que es produeix en una aplicació pel simple fet d'estar exposada a Internet. De la mateixa manera, també s'examinaran llocs web de caràcter tècnic (fòrums, llistes de correu, etc.) en cerca d'informació que el personal intern del client pugui haver publicat i que pugui ser rellevant.

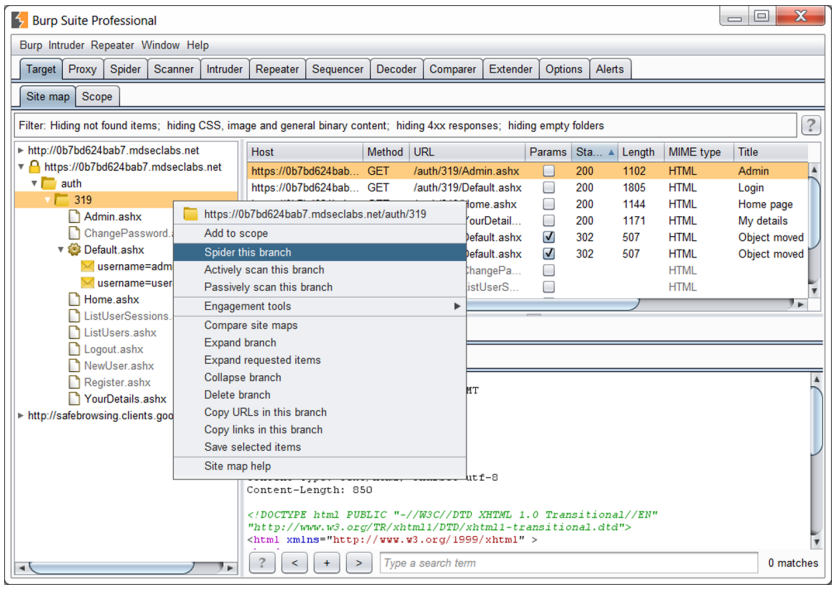
Per a obtenir un mapa complet de l'aplicació, amb tots els punts d'accés i tot el contingut que s'hi hagi publicat, es fa ús d'eines denominades *spider*. Heus aquí alguns exemples:

Nota

La prova es denomina *mineria de dades*, encara que no es refereix a cap aspecte conegut habitualment com a *datamining*. En el nostre context, entenem com a *mineria de dades* la recollida d'informació dins de la mateixa aplicació.

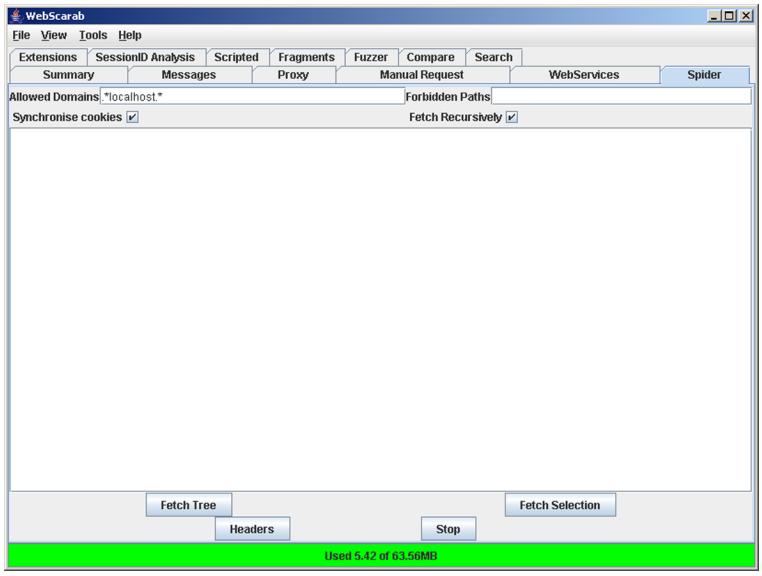
Eines *spider*

- Burp spider, que és part de l'aplicació Burp Suite.



Eina BURP Suite

- WebScarab, que utilitza el *plugin spider* per a fer la tasca que ens interessa.



Eina WebScarab

A més de les eines esmentades, s'utilitzaran cercadors tradicionals. La raó d'utilitzar cercadors és que aquests usen "robots" que tenen la virtut d'examinar tots els enllaços accessibles de cada web. Per això, són en realitat eines potents de mineria de dades.

4) Inspecció dels codis d'error de l'aplicació. En cas que es generi un error en l'aplicació web, la informació que es mostri ha de ser la menor possible. És a dir, no s'han d'oferir detalls tècnics sobre la infraestructura o sobre la naturalesa de la fallada. Igualment, l'aplicació controlarà l'ús de diferents plantilles a l'hora de generar els errors, de manera que l'usuari no pugui determinar la naturalesa de l'error.

Per a inspeccionar els diferents codis d'error, es generaran peticions HTTP de diferents tipus, les quals donaran lloc a errors en l'aplicació. D'aquesta manera, s'estudiarà la manera com l'aplicació gestiona les condicions d'error.

Nota

No s'ha de buscar generar errors que provoquin denegacions de servei. Aquests aspectes s'han de tractar en un conjunt de proves específiques.

5) Determinar l'arquitectura dels sistemes. És important determinar el tipus de plataforma en què es troba l'aplicació amb la màxima exactitud possible. Es tracta d'identificar quins dels elements següents intervenen en la prestació del servei:

- Tallafocs, que es poden identificar mitjançant l'ús de l'eina NMAP.
- Servidors intermediari o tallafocs de nivell d'aplicació, que es poden identificar mitjançant l'eina netcat.
- Servidor d'aplicacions, que es pot identificar a partir de l'observació dels recursos que ofereix l'aplicació auditada.
- *Backend*, que es pot identificar a partir de la navegació per l'aplicació. Els *backends* que es poden trobar són:
  - Bases de dades d'autenticació. No obstant això, és difícil determinar l'existència d'una base de dades per a l'autenticació (LDAP, base de dades relacional, RADIUS...) des d'un punt de vista extern.
  - Bases de dades per a la gestió de la informació.

6) Interfície d'administració. Una interfície d'administració és un punt candidat a sofrir intents d'atacs per intrusos. Hi pot haver interfícies d'administració tant de la mateixa aplicació com dels diferents components que conformen l'arquitectura tecnològica de l'aplicació. S'ha d'identificar si hi ha interfícies d'administració accessibles des del punt de prova. En cas afirmatiu, s'ha d'estudiar quina informació ofereix aquesta interfície i quins mecanismes de control d'accés implementa.

El primer pas d'aquesta prova consisteix a enumerar totes les interfícies d'administració que hi pot haver. Això es fa a partir de l'anàlisi de la mateixa aplicació i la seva arquitectura. La llista d'interfícies es pot completar mitjançant la recerca d'aplicacions en els diferents components que conformen l'arquitectura. Per a això, es pot emprar l'eina NMAP.

El segon pas és determinar si aquestes interfícies d'administració són accessibles des de localitzacions públiques (Internet). En cas que les interfícies d'administració siguin accessibles des d'Internet, s'estudiaran els mètodes de control d'accés implementats i les seves possibles debilitats.

7) Manteniment de l'aplicació. Les tasques de manteniment i suport de l'aplicació poden donar lloc a filtracions d'informació cap a l'exterior. De vegades, s'inclouen comentaris o funcions de depuració (*debugging*) en la part client que podrien estar revelant informació sobre el funcionament intern de l'aplicació. Així mateix, també pot passar que, durant el pas a producció, les

versions antigues d'alguns fitxers de codi no siguin eliminades, sinó simplement reanomenades. De vegades, es pot arribar a accedir al codi font d'aquestes versions antigues si no s'han eliminat, i es poden veure com a fitxers de text.

Es poden dur a terme diferents proves per a intentar determinar l'existència de vells arxius o *backups* que encara estigui fent servir l'aplicació.

- Inferència a partir de l'esquema de noms utilitzat en el contingut publicat. L'objectiu és trobar arxius vells que no són manejats correctament, de tal manera que l'aplicació els mostri com a fitxers de text, o fins i tot els executi. Això últim podria permetre l'explotació de vulnerabilitats que s'han corregit en la versió definitiva.

- Examen dels comentaris en el codi del client a la recerca d'informació sensible. Per a això, es pot utilitzar l'eina WebScarab.

- Examen de continguts no referenciats, obtinguts en la mineria de dades.

- Recerca de continguts en la memòria cau (*cache*) de Google o Yahoo.

Revisió del procés d'identificació i autenticació

En aquesta fase, es revisa el procés d'identificació i autenticació d'usuaris. A l'entorn d'una aplicació multiusuari, hi ha un procés d'identificació i autenticació que permet verificar la identitat *digital* de la persona que inicia la comunicació. D'acord amb aquesta identitat digital, s'atorguen a la persona uns drets d'accés a la informació. En el context d'una aplicació web, una vegada fet el procés d'identificació i autenticació, se sol atorgar a l'usuari un element (*token* d'identificació) que identifica unívocament la sessió que s'ha establert. Aquest *token* d'identificació pot ser una galeta (*cookie*) o un número de sessió passat com un paràmetre en les peticions HTTP. A causa del fet que el protocol HTTP no està orientat a connexió, és necessari que el *token* d'identificació sigui intercanviat en cada transacció entre el client i el servidor de l'aplicació web, per a poder saber en tot moment a quina sessió d'usuari correspon la petició HTTP. Si aquest procés no està implementat adequadament, un usuari pot ser vist per l'aplicació amb un rol que no li pertany i, per tant, pot ser que se li apliquin privilegis que no li corresponen. Un usuari podria fins i tot arribar a accedir sense tenir cap de dret d'accés si fos capaç d'endevinar com són gestionats aquests *tokens*. Per a revisar el procés d'identificació i autenticació, s'han de seguir els passos següents:

- **Determinar la topologia dels *tokens* d'identificació**. Les tasques que s'han de fer serien:
  - Trobar els diferents *tokens* d'identificació de què disposa l'aplicació per a autoritzar l'accés.

(9)Per a obtenir més detalls sobre què determina si l'esquema d'identificació i autenticació és correcte, cal consultar l'OWASP *Development Guide*.

  - Determinar la topologia d'aquests *tokens* d'identificació: longitud, contingut, com es fan arribar fins a l'aplicació, si són recuperables, nombre màxim d'intents, etc.

  - Concloure si el nombre de *tokens* utilitzats i la seva topologia són adequats[9] en el context de l'aplicació.

- **Revisar l'ús de contrasenyes per defecte o de diccionari**. S'han d'evitar i eliminar, si n'hi ha, contrasenyes per defecte en les aplicacions que se serveixen. Igualment, s'han d'evitar contrasenyes predictibles, fàcilment endevinables, per exemple, a partir d'un diccionari de paraules. En interfícies d'administració o aplicacions públiques, s'ha de revisar que no s'estiguin utilitzant noms d'usuari i contrasenyes de la instal·lació per defecte de l'aplicació.
  En aplicacions específiques d'una companyia, desenvolupades a mida, s'ha d'evitar l'ús de comptes d'usuari típics (com *Admin*, *Administrador*, *System*, etc.) i contrasenyes fàcilment predictibles (contrasenya igual al nom d'usuari, paraules d'un diccionari, etc.). Per a fer aquesta prova en entorns d'aplicacions web, es pot utilitzar l'eina hydra (o una de similar).

- **Comprovar la vulnerabilitat a atacs de força bruta**. S'ha d'evitar l'ús de contrasenyes que es puguin trencar en un temps raonable mitjançant atacs de força bruta, és a dir, mitjançant la prova sistemàtica de totes les contrasenyes possibles. La prova de força bruta s'executa contra contrasenyes vulnerables a aquest tipus d'atac. Per a la prova sistemàtica de totes les possibles combinacions, es pot utilitzar el programari hydra (o un de similar).
  D'altra banda, els *token* d'identificació (els que identifiquen una sessió en una aplicació web) també són susceptibles de ser compromesos per força bruta. Com a resultat de l'anàlisi de la topologia del *token*, hi ha la possibilitat de determinar-ne el grau d'aleatorietat (idealment haurien de ser totalment aleatoris o almenys pseudoaleatoris). En cas que es detecti algun patró de construcció, es pot determinar si és possible predir totalment o parcialment els *tokens* i, a continuació, acabar l'atac mitjançant l'aplicació de la força bruta.

- **Comprovar l'efectivitat del marc d'autenticació**. Una aplicació amb autenticació ha de controlar, en tot moment, que no es pugui evitar el marc d'autenticació per a accedir de manera directa als seus recursos. Per a determinar si és possible evitar el marc d'autenticació, es dissenyen una sèrie de tests que es descriuen a continuació:
  - Accés directe a recursos de l'aplicació. Consisteix a dissenyar peticions directes a continguts protegits de l'aplicació, sense passar prèviament per l'autenticació.

– Modificació de paràmetres relacionats amb l'autenticació. Estudiar l'existència de variables relacionades amb l'autenticació que l'usuari pugui modificar per accedir a recursos protegits.

– Anàlisi d'ID de sessió. Si l'aplicació web utilitza ID de sessió per a garantir l'accés als recursos una vegada l'usuari s'ha autenticat, la predicció d'aquests ID pot comprometre el sistema. Per a l'anàlisi d'ID de sessió, es pot utilitzar l'eina WebScarab.

– Injecció. Consisteix a determinar si el *backend* utilitzat per a l'autenticació i el marc d'autenticació que treballa sobre aquest són susceptibles a problemes de validació de les dades d'entrada (descrits més endavant). Aquests problemes podrien permetre a un atacant disposar de *tokens* correctes per a accedir a continguts restringits.

Per a fer aquests tests, és necessari construir o modificar les peticions que s'envien a l'aplicació web analitzada. Per a això, es pot utilitzar el navegador Mozilla Firefox i diversos connectors que permeten observar i estudiar, detalladament, la informació que envia i rep l'aplicació.

Exemple de connectors

Web Developer, Live HTTP Headers, FireBug, Add 'n' Edit Cookies, Tamper Data, entre altres.

Igualment, pot ser necessari l'ús d'un servidor intermediari web que permeti estudiar i alterar el flux d'informació intercanviada entre el navegador i l'aplicació web. Les eines que es poden utilitzar són BURP i WebScarab.

- **Revisar els mecanismes de gestió de fitxers**. En les aplicacions web actuals, és habitual l'accés a arxius del sistema de fitxers per a servir informació o obtenir codi. De vegades, la selecció de l'arxiu al qual s'ha accedit pot estar determinada per paràmetres de la petició. El maneig dels arxius ha d'estar correctament implementat, per a evitar l'accés a recursos o l'execució de codi sense autorització.
  Per a dur a terme la prova, en primer lloc s'ha de determinar si hi ha maneres d'utilitzar els mecanismes de maneig d'arxius per a accedir a recursos no autoritzats. Es tracta d'identificar en quina mesura els paràmetres de la comunicació HTTP entre el client i l'aplicació determinen els arxius a què s'accedeix.
  El segon pas és dissenyar i fer els tests que permetin determinar si el maneig d'arxius està funcionant adequadament o si, per contra, aquest es veu afectat per problemes.

Problemes de directori transversal

Els problemes de directori transversal permeten l'accés a arxius del sistema mitjançant la manipulació dels paràmetres de la petició que governen el directori a què s'ha d'accedir. Aquest i altres problemes estan relacionats amb errors de validació de l'entrada de l'usuari.

Per a fer aquestes proves, es poden utilitzar les mateixes eines que es descriuen en el punt anterior.

- **Revisar el mecanisme de recuperació de contrasenya**. Si l'aplicació permet a l'usuari recuperar una contrasenya que ha oblidat, el mecanisme utilitzat no ha d'introduir cap vulnerabilitat en el marc d'autenticació. Per a això, s'ha d'estudiar si hi ha mecanismes perquè l'usuari recuperi la contrasenya, la manera com funcionen i si hi pot haver vulnerabilitats. Aquestes vulnerabilitats dependran dels mecanismes disposats i poden estar relacionades amb errors en la validació dels paràmetres d'entrada, o amb atacs d'enginyeria social (en cas que hi hagi un servei de suport a l'usuari). A partir d'aquest estudi, es determina el grau de robustesa del procés i les possibles vulnerabilitats que aquest mecanisme introdueix en el marc de l'autenticació.
  D'altra banda, l'aplicació ha de prevenir que l'usuari emmagatzemi la contrasenya en el navegador. Això implica verificar que el codi de client desactiva la propietat d'autocompletar del navegador.

- **Revisar el procés de final de sessió (*logout*)**. L'aplicació, en cas de tenir un marc d'autenticació, ha d'haver implementat un procés de final de sessió per a evitar que es reutilitzin sessions. També s'ha d'executar el procés de final de sessió automàticament després d'un cert temps d'inactivitat de l'usuari, per a evitar, per exemple, l'ús de la sessió en cas d'absència de l'usuari original.
  Durant el procés de revisió d'aquesta funcionalitat, s'ha de verificar que el procés de final de sessió elimina efectivament la sessió de l'usuari, que s'eliminen les galetes en el client, si és necessari, i que la sessió no es pot reutilitzar. Finalment, també s'ha d'estudiar el grau d'accessibilitat a la funció de final de sessió.
  Per a fer aquestes proves, és necessari l'ús d'un servidor intermediari web que permeti estudiar i alterar el flux d'informació entre el navegador i l'aplicació web. Les eines que es poden utilitzar són BURP i WebScarab.

- **Revisar la gestió de la memòria cau del navegador**. L'aplicació ha de controlar els continguts que es desen en la memòria cau del navegador, per a evitar que s'emmagatzemin continguts sensibles als quals es pugui accedir una vegada s'ha abandonat una sessió. D'aquesta manera, s'ha d'evitar la fugida d'informació sensible per mitjà de la memòria cau del navegador de l'usuari.
  Per a revisar que la memòria cau del navegador es gestiona correctament, es pot utilitzar l'eina WebScarab. Aquesta eina permet observar totes les respostes que ha produït l'aplicació web, i comprovar que, per a totes les que continguin informació sensible, s'han donat instruccions al navegador perquè no "oculti" les dades, mitjançant les capçaleres HTTP corresponents.

Revisió de la gestió de sessions

A causa que el protocol HTTP sobre el qual s'implementen les aplicacions web no emmagatzema informació d'estat, és molt important revisar la implementació que fa l'aplicació per a mantenir l'estat de la connexió i controlar la interacció amb l'usuari. En aquesta fase, s'han de fer les proves per a revisar la gestió de les sessions d'usuari.

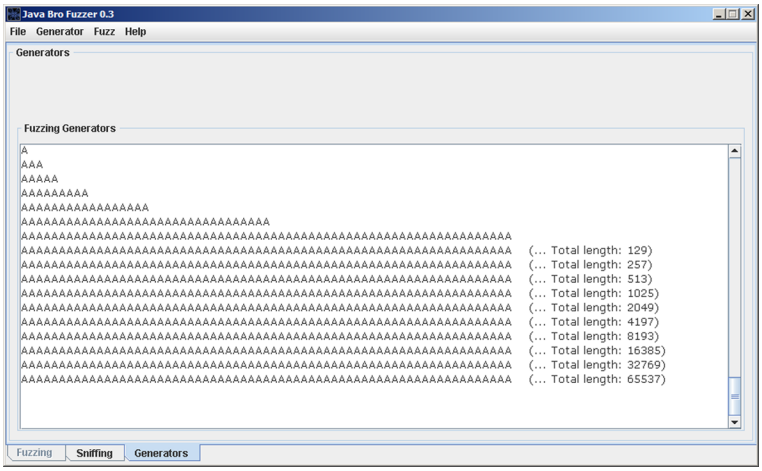
- **Estudi de l'esquema de sessions**. En una aplicació web amb un marc d'autenticació, és important mantenir sessions per a controlar la interacció de l'usuari. Per a gestionar una sessió, s'utilitzen *tokens* de sessió. Aquests *tokens* poden ser principalment de tres tipus: galetes, números de sessió transportats en paràmetres d'una petició GET, o paràmetres passats per una petició POST continguts en camps ocults de formularis. En tot cas, els *tokens* de sessió han de complir certes propietats –ser aleatoris, únics, resistents a anàlisis estadístiques o criptogràfiques– i evitar la fugida d'informació sensible.

  L'estudi de l'esquema de sessions requereix, en primer lloc, determinar l'estructura dels *tokens* de sessió i la possibilitat que aquests puguin donar lloc a una fugida d'informació. Per a això, s'ha d'examinar una mostra significativa de *tokens* en cerca de patrons o informació sensible (fins i tot ofuscada), i revisar les condicions sota les quals es reutilitzen els *tokens*. Aquesta mateixa prova serveix per a determinar si els *tokens* de sessió es generen d'una manera predictible i si són valors realment aleatoris. En els casos en què es consideri adequat i factible, s'han d'intentar fer atacs de força bruta per a intentar obtenir ID de sessió vàlids.

  Per a recollir *tokens* de sessió i examinar-ne les característiques, es pot utilitzar l'eina WebScarab, que també permet manipular els *tokens* de sessió que ofereix l'aplicació i fer estudis sobre la seva aleatorietat. En el cas d'intentar atacs de força bruta per a obtenir *tokens* de sessió vàlids, s'ha d'utilitzar alguna eina de *fuzzing* amb fonts de dades personalitzades.

  Eines de *fuzzing*

  Les eines que s'utilitzen per a aquest propòsit són els mòduls de *fuzzing* de WebScarab o BURP, o bé el *fuzzer jbrofuzz*.



Eina JBroFuzz

- **Estudi de l'exposició dels *tokens* de sessió**. L'aplicació ha de prevenir que els *tokens* de sessió siguin visibles durant el seu enviament des del client fins al servidor. En cas contrari, les sessions dels usuaris es poden veure compromeses. Per a assegurar que els *tokens* no són visibles, s'ha de comprovar que aquests s'envien sempre xifrats amb cada petició HTTP, i que a més s'utilitza un canal segur per a l'enviament (HTTPS).
  A continuació, s'ha de validar que l'aplicació implementi el control adequat, mitjançant directives, per a evitar que servidors cau intermedis emmagatzemin *tokens* de sessió. També s'ha de controlar que l'enviament dels *tokens* de sessió no es faci mitjançant peticions GET, i verificar que el servidor no els accepta en una petició GET. Per a la realització d'aquestes proves, s'utilitzarà una eina de tipus servidor intermediari com WebScarab o BURP.

- **Prevenció d'atacs de *session riding* o *cross site request forgery* (CSRF)**. Un atac de CSRF és aquell en què es força un usuari d'una aplicació web a fer una petició HTTP que ell no ha sol·licitat expressament (seguint un enllaç o fent clic en un botó d'un formulari). Aquesta petició pot tenir un impacte rellevant, com podria ser, per exemple, un canvi de contrasenya, una ordre de comanda, etc. Normalment, es requereix que la víctima ja tingui establerta la sessió en l'aplicació web vulnerable.
  L'aplicació web ha de prevenir que es facin accions importants i rellevants sense la intervenció de l'usuari o confiant únicament en informació predictible (encara que sigui dins del marc d'una sessió autenticada). Sense aquest tipus de precaució, la petició que causa l'acció es podria preconstruir i amagar, de tal manera que l'usuari l'executés sense el seu coneixement i sense adonar-se de l'efecte que s'ha causat. El problema d'aquesta vulnerabilitat és que pot ser explotada sense atacar realment l'aplicació, ja que en realitat s'està aprofitant un error en el disseny.

Maneres d'ocultar i forçar la petició

Hi ha diverses maneres d'ocultar i forçar la petició. Per exemple, es pot inserir en qualsevol pàgina que hagi de visitar la víctima (no ha de ser en l'aplicació atacada) una imatge que en realitat conté una petició construïda per a llançar l'atac. També es podria aprofitar una vulnerabilitat de *cross-site scripting* en un lloc web que la víctima visiti i, mitjançant codi javascript inserit en el navegador de la víctima, llançar la petició. Quan la víctima visita el

lloc web que conté el contingut maliciós, automàticament i sense el seu coneixement es llança una petició contra l'aplicació web amb tots els paràmetres necessaris per a fer l'atac.

Per a evitar aquest tipus d'atacs, l'aplicació ha d'implementar mesures com afegir informació específica de la sessió en les peticions que executen alguna acció.

Mesures de seguretat

Utilitzar camps ocults en formularis que siguin aleatoris i diferents per a cada petició (encara que l'acció executada en l'aplicació sigui exactament la mateixa). A més, l'aplicació ha de comprovar que els paràmetres rebuts són els que s'esperava per a la sessió, i que s'han rebut en el moment exacte.

Una altra mesura pot ser demanar confirmació a l'usuari abans de fer qualsevol acció rellevant. L'objectiu final d'aquestes mesures és evitar l'execució d'accions en el context d'un usuari sense el seu coneixement ni consentiment.

L'auditor pot estudiar la vulnerabilitat de l'aplicació web a aquest tipus d'atacs utilitzant una aplicació de tipus servidor intermediari com WebScarab o BURP. Aquestes aplicacions permeten observar quin tipus de peticions s'utilitzen per a consultar informació de l'aplicació web o executar accions rellevants. De la mateixa manera, permeten estudiar quina informació cal enviar en la petició, si es confia únicament en informació que té el navegador (com una galeta) i si es demana confirmació de les accions. Finalment, aquestes aplicacions també permeten manipular les peticions.

Revisió de la validació de les dades d'entrada

Probablement, els problemes de seguretat més greus en una aplicació web es deriven d'errors en la validació de l'entrada. Així, doncs, no s'ha de confiar en les dades externes que es reben, ja que són sempre susceptibles de ser alterades per un atacant. Les proves que es facin en aquest àmbit determinen el tractament correcte de l'entrada de l'usuari, especialment quan aquesta pot conduir a vulnerabilitats en l'aplicació.

- **Problemes d'injecció**. Quan l'entrada d'un usuari ha de ser finalment utilitzada per un *backend* o intèrpret, és necessari validar-la correctament per a evitar l'execució d'instruccions o ordres. Per a això, de primer se seleccionen els vectors d'entrada de dades que siguin susceptibles de ser interpretats. Els vectors d'entrada susceptibles són els que seran interpretats per un *backend* (un servidor LDAP, un gestor de bases de dades relacionals o un intèrpret d'ordres) o fins i tot pel mateix navegador web de l'usuari (injecció de contingut en la capa de presentació).
  Una vegada identificats els intèrprets susceptibles de tractar determinades dades d'entrada, s'han de fer bateries de proves per a trobar injeccions de diferent tipus[10].

(10)Consultar OWASP *Testing Guide* i OWASP *Development Guide*.

Injeccions

Alguns exemples d'injeccions:

- Cross Site Scripting
- Injecció SQL

- Injecció LDAP
- Injecció ORM
- Injecció XML
- Injecció SSI
- Injecció XPath
- Injecció IMAP/SMTP
- Injecció de codi
- Injecció d'ordres

Per a fer aquestes proves, és necessari observar i modificar el flux d'informació entre el client i l'aplicació. Per a això, s'utilitza una aplicació de tipus servidor intermediari com WebScarab o BURP. També es pot utilitzar una eina de *fuzzing* amb fonts de dades personalitzades.

Exemples de les eines que s'utilitzen per a aquest propòsit són els mòduls de *fuzzing* de WebScarab o BURP, o bé el *fuzzer jbrofuzz*.

- **Corrupció de memòria.** Les entrades de l'usuari s'han de tractar de manera adequada, per a evitar que les aplicacions que tractaran després les dades es puguin veure afectades per problemes de corrupció de memòria, com desbordaments de memòries intermèdies o *bugs* de format.
  Els desbordaments de memòria són causats per problemes de falta de verificació de les dades d'entrada. Les variables que contenen aquestes dades es passen als processos per mitjà de memòries intermèdies (en la pila o *heap*). Si no es controla la longitud que tenen aquestes dades, es pot provocar un mal funcionament en el procés que els rep.
  Per a comprovar la possibilitat de fer aquest tipus d'atacs en l'aplicació web, s'utilitzarà una bateria de proves contra els diferents vectors d'entrada prioritzats. Cadascuna d'aquestes proves s'ha de centrar en un paràmetre d'entrada, i s'han de fer proves del funcionament del procés donant diferents valors al paràmetre amb longituds diferents. En el moment en què es detecta un funcionament anòmal del procés, es tindrà identificat un punt potencial de desbordament de memòria intermèdia.
  Per a l'execució de les bateries de proves, també es pot utilitzar alguna eina de *fuzzing* amb fonts de dades personalitzades; posteriorment, s'hauran d'emprar eines de depuració per a identificar l'origen del mal funcionament. Això permetrà determinar si l'error es deu o no a un desbordament de memòria intermèdia.
  Aquest tipus de proves són les més complicades de fer i podríem considerar que el treball de l'auditor es converteix en una investigació de seguretat d'un producte de programari concret.

Totes les fases i tècniques descrites anteriorment són automatitzables fins a cert punt i per això al mercat hi ha eines disponibles per als auditors especialitzades en la cerca de vulnerabilitats en aplicacions web (Acunetix, Netsparker, Nessus, Nexpose, Qualys, etc.) que automatitzen pràcticament totes les fases. Facilitant credencials a l'escàner, l'eina realitza per si sola el recorregut de l'aplicació (*web spidering* o *web crawling*) i, sobre cadascuna de les pàgines i paràmetres detectats, és capaç de passar tota una bateria de proves. No obstant això, aquestes eines poden generar falsos positius, no aconseguir completament totes les parts de l'aplicació o no ser capaces de detectar problemes lligats

a la lògica de negoci que realitza l'aplicació. Per aquest motiu, aquestes eines constitueixen un element molt important de l'arsenal de tècniques disponibles per a l'auditor, però en cap cas un substitut total de la feina professional, diligent i intel·ligent d'un auditor experimentat.