Enginyeria social

Sergi Robles Martínez
Sergio Castillo Pérez

PID_00178951

Universitat Oberta de Catalunya
www.uoc.edu

Índex

Introducció

Hi ha un gran nombre de vulnerabilitats de naturalesa molt variada que permeten una gran diversitat d'atacs. Això fa difícil el disseny d'una política de prevenció completa i dóna lloc a la necessitat de tenir experts en seguretat de la informació amb un ampli coneixement sobre el tema. Les vulnerabilitats, els atacs i els mecanismes de prevenció vistos fins ara són de naturalesa tecnològica, la qual cosa en permet fer una anàlisi completa, amb les puntualitzacions remarcades en els mòduls anteriors.

No obstant això, s'ha obviat fins ara un element comú a tots els sistemes d'informació i que precisament és el més vulnerable i fàcil d'atacar, i que dificulta en gran manera l'anàlisi de seguretat dels sistemes. Ens referim als humans. Darrere d'un sistema d'informació sempre hi ha persones, com els usuaris, els administradors, o el personal de desenvolupament i manteniment.

Si incloem les persones com a part integrant d'aquests sistemes d'informació, aspecte que desgraciadament apareix moltes vegades descurat en les anàlisis de seguretat, resulta que sol ser, amb diferència, la baula més feble de tota la cadena de seguretat. Encara que la consideració d'aquest factor humà en l'estudi de les vulnerabilitats d'un sistema sembla obvi, hi ha circumstàncies que n'afavoreixen l'exclusió. El primer impediment es troba en la naturalesa mateixa del problema, ja que es pot pensar que està fora del domini de les tecnologies de la informació i de les comunicacions i descartar-lo en comptes de buscar-ne la integració. Sens cap dubte, considerar les persones com a part del sistema en dificulta enormement l'anàlisi. Es pot pensar que en molts aspectes aquesta anàlisi de l'activitat humana entorn dels sistemes d'informació pertany més al domini de la psicologia social.

En aquest mòdul veurem que és possible analitzar el que denominarem *enginyeria social* des d'un punt de vista metodològic. Identificarem les estratègies, les tècniques i els mitjans utilitzats per l'enginyeria social, i de quina manera es relacionen per a aconseguir atacar vulnerabilitats del sistema. Aprendrem també a detectar els elements més vulnerables a partir dels diagrames d'atac d'enginyeria social i per mitjà de casos pràctics, i també a incloure estratègies per a la prevenció en les solucions de seguretat. D'aquesta manera, s'aconseguirà una visió més holística de les vulnerabilitats de seguretat dels sistemes d'informació que permetrà no solament ampliar i complementar els mecanismes de prevenció vistos fins ara, sinó a més enfocar de manera diferent el disseny mateix dels sistemes. S'estudiaran també altres instàncies d'enginyeria social que tenen especial rellevància per la seva quotidianitat, com els atacs de *phishing*, *scareware* i *hoaxes*.

Objectius

Els objectius que l'estudiant ha d'haver aconseguit després d'estudiar els continguts d'aquest mòdul són els següents:

1. Saber identificar les estratègies, les tècniques i els mitjans més comuns utilitzats per l'enginyeria social.
2. Aprendre a fer diagrames d'atacs d'enginyeria social (DAES).
3. Identificar els elements més vulnerables d'un sistema a partir del DAES.
4. Dissenyar estratègies per a la prevenció dels atacs d'enginyeria social.
5. Tenir una visió més completa de les vulnerabilitats d'un sistema d'informació.

1. El procés de l'enginyeria social

Una de les claus per a afrontar amb èxit el problema de la inclusió del factor humà en l'anàlisi de seguretat d'un sistema d'informació és la identificació de manera precisa de tots els elements que hi intervenen, i el seguiment d'una metodologia concreta. Si no es fa d'aquesta manera, és fàcil endinsar-se massa en l'àmbit de la psicologia social, en particular en l'anàlisi de la confiança humana, o el de la persuasió, que augmenta la complexitat i fa més difícil el disseny de solucions pràctiques per a la detecció i prevenció d'atacs. Una part important del treball d'investigació fet sobre aquest tema no es troba en el domini de la informàtica, sinó en el de les ciències socials.

En aquest apartat es presenta un enfocament pràctic i simple per a l'anàlisi de la intervenció humana en la seguretat d'un sistema, que permet la detecció i prevenció d'atacs que utilitzen les persones. El primer pas serà definir els conceptes bàsics que usarem.

Anàlisi de casos concrets

Molts dels treballs fets sobre el tema de l'enginyeria social fins ara es basen en l'anàlisi de casos concrets, com el de Mitnick i Simon (2002).

En el context de la seguretat informàtica, anomenarem **enginyeria social** la seqüència d'accions que tenen com a finalitat l'obtenció d'informació, el frau o l'accés no autoritzat a sistemes informàtics, i que ha implicat en algun moment la manipulació psicològica de persones.

Un sistema **vulnerable a atacs d'enginyeria social** serà, per tant, aquell susceptible a ser atacat mitjançant aquestes tècniques. El punt que fa diferents els atacs d'enginyeria social d'altres atacs és la manipulació psicològica de les persones que es fa en algun moment.

Altres col·lectius

Fora del domini de la informàtica, la policia, els detectius privats i els periodistes, entre altres col·lectius, utilitzen també de vegades l'enginyeria social per a aconseguir informació.

Així doncs, un aspecte bàsic en l'enginyeria social serà la manipulació psicològica de persones. En el subapartat següent es veurà de quines maneres es pot fer aquesta manipulació.

1.1. Aspectes explotables

La base de l'enginyeria social és l'aplicació de tècniques de psicologia per a aconseguir, per mitjà de la manipulació, que les persones facin certes accions o desvetllin la informació que volem. Trobem la base teòrica d'aquestes tècniques en la psicologia social.

Hi ha tres aspectes de la psicologia social que seran importants per als propòsits de l'enginyeria social: les tècniques per a la persuasió i la influència, les actituds i creences que afecten la interacció social, i la falsa confiança.

Lectura complementària

La psicologia social engloba l'estudi de com les persones pensen, influeixen i es relacionen entre elles. Es pot trobar més informació sobre la psicologia social en l'obra de Myers (1994).

1.1.1. Tècniques de persuasió i influència

En la psicologia social s'identifiquen dues maneres que es poden utilitzar per a persuadir. D'una banda, utilitzant arguments sistèmics i lògics per a estimular una resposta favorable, induint la persona a pensar detingudament i donar un consentiment. D'una altra, d'una manera més lateral, basada en indicacions perifèriques i dreceres mentals per a eludir l'argument lògic i la contraargumentació per a intentar provocar l'acceptació, sense pensar en profunditat sobre el tema. Una manera com es pot fer una persona més susceptible a aquesta persuasió perifèrica és per mitjà de missatges o accions en l'inici de la interacció que provoquin reaccions emocionals, com excitació o por. Aquestes reaccions, i també altres formes de distracció, serveixen per a interferir en la capacitat de pensament lògic de la víctima i permetre explotar aquesta persuasió perifèrica per a fer atacs d'enginyeria social.

Una gran part de la bibliografia de la psicologia social reconeix almenys set factors que es basen en la persuasió perifèrica que són afectius en la persuasió i influència de persones (Cialdini, 2008):

1) Autoritat. La majoria de les persones són molt receptives a l'autoritat. En les condicions adequades, l'autoritat es qüestiona poc, i la tendència a obeir instruccions d'algú que diu tenir-ne és molt alta, fins i tot quan es reben de manera indirecta (per exemple, per mitjà del telèfon).

Exemple d'autoritat

Un exemple de recurs a l'autoritat és demanar que obrin una porta fent-se passar per un agent de policia.

2) Parquedat. Quan hi ha escassetat d'un bé o servei en el qual es podria estar interessat, o la disponibilitat és solament per un període de temps limitat, les persones ho tendeixen a voler més. Saber que aquesta disponibilitat limitada pot crear competència entre altres persones per a adquirir-ho incrementa més encara el desig d'adquirir-ho.

Exemple de parquedat

Un exemple de recurs a la parquedat és anunciar que solament queden tres unitats de llapis USB per a les primeres persones que contestin una enquesta.

3) Similitud. Hi ha una innegable tendència humana que ens agradi allò que és similar a nosaltres mateixos. Tenir elements en comú, com per exemple aficions, gustos musicals o artístics, o fins i tot compartir els mateixos problemes, crea un fort incentiu per a tractar algú d'una manera especial, més favorable.

Exemple de similitud

Un exemple de recurs a la similitud és comentar casualment que hem nascut a la mateixa ciutat per a demanar posteriorment una informació no pública.

4) Reciprocitat. Quan algú dóna alguna cosa, o promet que ho farà, les persones sentim una forta tendència a retornar alguna cosa a canvi, fins i tot si el que s'ha rebut mai va ser sol·licitat. Aquesta regla bàsica de la interacció humana és innata a les persones i funciona tot i que el cost del donat i rebut sigui molt diferent.

Exemple de reciprocitat

Un exemple de recurs a la reciprocitat és desconnectar distretament a algú el cable d'accés a la xarxa d'un ordinador simulant una avaria per solucionar el problema després i demanar un favor a canvi.

5) Compromís. Si s'incompleixen les promeses, les persones tenen la certesa que seran considerades de poca confiança per altres persones. Això provoca que les persones facin un gran esforç per complir amb els compromisos adquirits.

Exemple de compromís

Si es convenç a una persona que va fer una promesa, quan en realitat no en va fer cap, aquesta s'esforçarà per complir-la.

6) Consistència. Les persones tenen tendència a actuar de manera consistent amb les seves accions passades, encara que en la situació actual mantenir aquesta coherència ja no tingui sentit, ja que creuen que en no fer-ho seran considerades de poca confiança (Cacioppo i altres, 1986).

Exemple de consistència

Es pot predir la reacció d'una persona a partir de les seves accions passades.

7) Prova social. Davant el dubte sobre si fer o no una acció, o quina és la més apropiada, les persones decideixen segons el comportament d'altres persones properes. Això pot portar a fer accions que van contra els interessos de les persones sense que s'arribin a pensar detingudament.

Exemple de prova social

Si tres persones conxorxades mostren el DNI a un fals porter, la persona següent també el mostrarà.

1.1.2. Actitud i creences

Un altre aspecte de la psicologia social important en l'enginyeria social són les creences i actituds. Les persones generalment pensen que els altres comparteixen els seus mateixos sentiments i idees, la qual cosa es denomina l'efecte del fals consens. L'enginyer social pot utilitzar aquestes creences per a manipular la víctima i aconseguir que faci alguna acció.

Experiments de psicologia social mostren que fins i tot algunes de les persones que analitzen detingudament els missatges persuasius ho deixen de fer quan perceben que l'origen és més honest. Així, algunes víctimes d'enginyeria social tendeixen a confiar més en les seves creences o impressions personals sobre l'honestedat que els ofereix algú que en l'anàlisi objectiva del contingut del missatge mateix. Un atac, per exemple, podria estar precedit d'una estratègia de millorar la percepció de l'honestedat de l'atacant per part de la víctima.

1.1.3. Falsa confiança

Per defecte, les persones tenen una tendència natural a confiar en els seus congèneres, encara que no hi hagi un historial d'interaccions que avali aquesta confiança. És més, ser desconfiat d'entrada sol ser mal vist socialment i representa una percepció negativa de les persones. Quan no hi ha una percepció elevada de risc, es concedeix d'entrada el benefici del dubte en contra del que aconsellaria un pensament racional detingut, fins a certs límits (no se solen deixar la claus de casa al primer desconegut que ens les demana, per

exemple). Fins i tot si d'entrada una persona decideix no confiar, sol ser senzill fer-li canviar d'idea simplement fent-li veure que està desconfiant.

A més de la confiança natural directa, resulta fàcil fer accions que es perceben com a indicadors que augmentaran la confiança que es diposita en algú. Estaríem parlant, per exemple, de les tècniques de persuasió perifèriques vistes anteriorment amb l'objectiu d'incrementar la confiança que es té en l'atacant o de la seva credibilitat. Sense arribar a la persuasió, el simple contacte continuat en el temps augmenta automàticament la percepció de confiança. Per exemple, confiarem més en algú que hem vist cada matí al metro durant l'últim mes que en algú que acabem de conèixer, encara que racionalment no hi hagi cap raó per a això.

El pretext és una de les tècniques més conegudes per a guanyar confiança. Establir contacte amb una persona per mitjà d'una història falsa sol ser suficient perquè aquesta persona dipositi confiança sobre l'atacant i redueixi la seva reticència a oferir informació privada. Aquesta percepció de confiança és un dels punts explotables de les persones més utilitzats en l'enginyeria social i que sol ser més efectiu.

1.1.4. Altres aspectes explotables

A part dels aspectes ja vistos, hi ha altres qualitats humanes que són explotables des del punt de vista de l'enginyeria social. A continuació trobem alguns exemples:

Curiositat	Ignorància	Cortesia	Avarícia	Apatia
Paranoia	Luxúria	Inseguretat	Amabilitat	Caritat
Recel	Orgull	Enveja	Empatia	Compassió
Consol	Solidaritat	Ira	Indulgència	Amor

Aquestes qualitats humanes, no sempre presents en totes les persones, representen punts febles que faciliten l'engany i la manipulació. La curiositat, per posar un cas, és una qualitat humana molt comuna. Qui es pot resistir, per exemple, a veure el contingut d'un llapis USB trobat accidentalment al carrer? Molts atacs d'enginyeria social utilitzen aquest tret humà d'una manera o una altra.

Unes altres es perceben com a qualitats desitjables en una bona persona, i són fins i tot inculcades en algunes religions, com la caritat, la compassió o l'amabilitat. Moltes persones haurien de fer un gran esforç per resistir l'impuls d'oferir ajuda al necessitat o d'alleujar el sofriment del que pateix. No us saltaríeu alguna norma de la política de seguretat de l'empresa per cobrir l'error d'algú amb una família a càrrec, parar els seus plors, i treure-li la por de l'acomiadament?

Moltes d'aquestes qualitats són part de l'educació que es rep. Mancar-ne, en alguns casos, pot fer titllar les persones de "mal educades". En general, qualsevol aspecte que faci que les persones estiguin per sobre de qualsevol regla és explotable per part de l'enginyeria social per a saltar mecanismes de seguretat.

1.2. El procés de l'enginyeria social

En el subapartat anterior hem vist maneres de manipular les persones per mitjà de tècniques estudiades en la psicologia social. Els atacs d'enginyeria social tenen en comú la utilització d'alguna tècnica d'aquest tipus, en un moment o un altre, per a complir els seus objectius. En general, aquests atacs no usen exclusivament aquestes tècniques, sinó que les combinen amb altres atacs d'índole més tecnològica i amb altres tipus d'accions.

Generalment, els atacs d'enginyeria social es basen en la realització d'accions d'aquest tipus per a aconseguir resultats parcials, que es podran combinar per a poder fer noves accions, i així reiteradament fins a aconseguir l'objectiu final. És el que denominem el procés de l'enginyeria social. La representació gràfica d'aquest procés per a casos concrets ens permetrà estudiar les seves característiques i fer una anàlisi per a determinar quins són els punts crítics del sistema o dissenyar estratègies de prevenció.

Cadascuna de les accions particulars que es fan en aquests atacs estarà caracteritzada en tres nivells:

1) Estratègia. Determina el tipus de l'acció i els objectius que persegueix. Hi ha tres possibles estratègies: recollida d'informació, forçar una acció i atac directe. Totes les accions pertanyeran a una d'aquestes categories o una altra.

2) Tècnica. Per a cada estratègia hi ha diverses tècniques concretes per a aconseguir els objectius. Aquestes tècniques poden ser molt variades i en poden anar apareixent de noves a mesura que es desenvolupin noves tecnologies.

3) Via. La via identifica exactament el mitjà pel qual s'utilitza una certa tècnica en una acció. Una mateixa tècnica es pot aplicar per mitjà de vies diferents.

En la representació gràfica dels atacs d'enginyeria social, cada acció s'identifica mitjançant l'estratègia a la qual pertany, la tècnica utilitzada i la via d'aplicació, i està representada en un node.

Dins del procés de l'enginyeria social, les accions es faran seqüencialment fins a aconseguir la finalitat de l'atac. En alguns casos seran necessàries diverses accions prèvies per a fer-ne unes altres, o hi haurà accions alternatives per a aconseguir un mateix resultat parcial. Els diagrames DAES (diagrames d'atacs

d'enginyeria social) ens permetran representar gràficament aquestes relacions de seqüencialitat entre les accions.

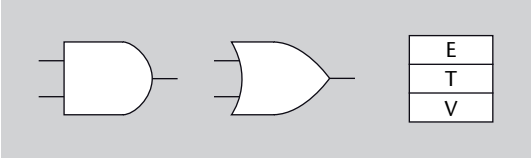
1.2.1. Diagrames DAES

Una vegada vistos els components bàsics de l'enginyeria social, presentem ara els diagrames d'atacs d'enginyeria social (DAES), que ens permetran veure de manera gràfica les accions que intervenen en un determinat atac d'enginyeria social, quina és la seva seqüencialitat, i podrem fer una anàlisi de l'atac. Encara que en la bibliografia hi ha algunes maneres similars de representar atacs, cap considera especialment el cas de l'enginyeria social. Els diagrames DAES estan especialment indicats per a la representació i l'anàlisi d'aquest tipus d'atacs.

Un **diagrama d'atacs d'enginyeria social (DAES)** és una representació gràfica de les accions, i les seves relacions, que poden intervenir en un atac d'enginyeria social.

En els diagrames DAES els principals nodes són les accions de l'atac, i estan representades per una caixa amb la identificació de l'estratègia, de la tècnica que utilitza, i també de la via per la qual s'aplica. Les accions estan relacionades entre elles o bé per mitjà d'una relació directa, o bé per mitjà de nodes conjunt o alternativa. Finalment, l'objectiu final de l'atac s'especifica amb un node objectiu. La figura 1 mostra els principals components dels diagrames DAES. Les relacions es representen com a fletxes, i el sentit n'indica la seqüència.

Figura 1. Elements clàssics del DAES



1.2.2. Accions

Les accions es representen amb una caixa de tres seccions: estratègia, tècnica i via. L'estratègia pot ser o recollir informació o forçar una acció o atac directe, que en la representació gràfica es representen amb les sigles RI, FA o AD, respectivament, en la secció superior de la caixa. La secció central indica la tècnica utilitzada, i la secció inferior, la via. En l'apartat 2 es detallaran diverses tècniques i vies utilitzades en cada estratègia. En aquest subapartat utilitzarem únicament l'identificador de l'estratègia en la representació de les accions per introduir els diagrames DAES.

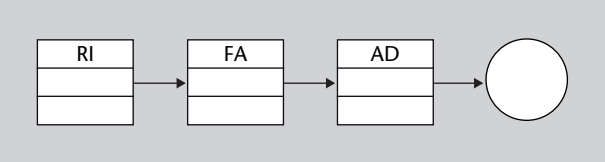
1.2.3. Relacions seqüencials

Les accions estan connectades per mitjà de relacions directes, expressades com a fletxes en el diagrama, que representen la seva seqüencialitat, és a dir, quina acció s'ha de fer abans que una altra.

Exemple

En l'exemple de la figura 2 veiem com tres accions s'han de fer una abans que l'altra. El resultat de l'última acció és necessari per a l'objectiu final de l'atac d'enginyeria social, que apareix representat amb un cercle en el diagrama DAES. Per a fer una acció és imprescindible haver fet abans les accions que la precedeixen.

Figura 2. Exemple de diagrama DAES amb tres accions



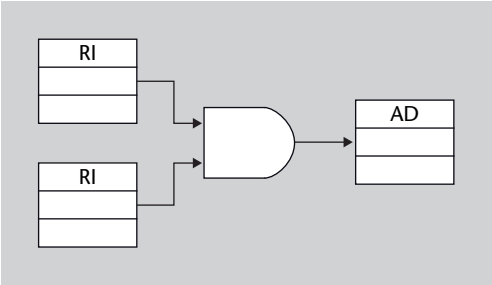
En aquest cas, hi ha una acció de recollida d'informació. Aquesta informació ha estat utilitzada per a forçar una acció. Finalment, aquesta acció ha permès fer un atac directe i completar l'objectiu inicial de l'atac d'enginyeria social.

Una acció pot requerir que s'hagi fet no solament una acció prèvia, sinó més d'una. En aquest cas, el diagrama DAES permet especificar per mitjà d'un node conjunt que cal fer diverses accions per a poder-ne dur a terme una altra. El node conjunt actua aquí com una "i" lògica. Per a poder fer l'acció següent a un node conjunt, totes i cadascuna de les accions connectades a aquest s'han d'haver completat amb èxit.

Exemple

En l'exemple de la figura 3 es pot observar com per a la realització d'una acció d'atac directe és necessària l'obtenció d'informació per mitjà de dues accions de recollida d'informació.

Figura 3. Exemple de node conjunt



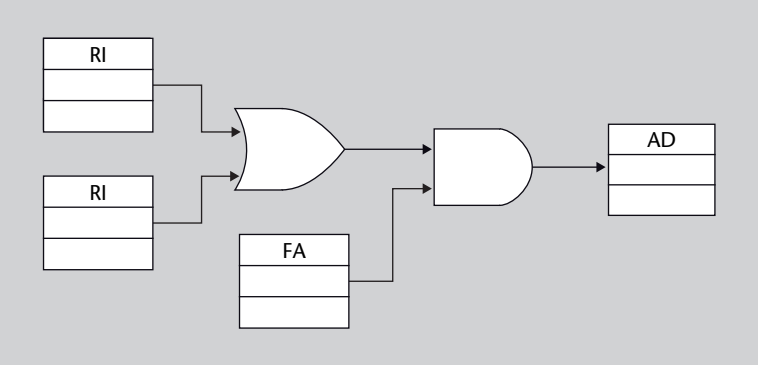
De manera similar, els diagrames poden expressar alternatives d'accions, és a dir, diferents opcions que permeten una certa acció. En aquest cas, s'utilitzaran els nodes alternativa, que actuaran com la "o" lògica. Si almenys una de les

accions connectades a un node alternativa s'ha aconseguit fer amb èxit, encara que cap altra no l'hagi fet, és suficient per a fer l'acció següent en la seqüència.

Exemple

La figura 4 mostra un exemple en què aconseguint una informació per mitjà d'una acció o d'una altra, i forçant una altra acció, es pot dur a terme un atac directe.

Figura 4. Exemple amb node conjunt i alternativa



No és necessari cap altre tipus de node per a representar les possibles dependències entre les accions, ja que qualsevol combinació pot ser representada utilitzant únicament les seqüències, les alternatives i els conjunts.

1.2.4. Normalització

Un mateix atac d'enginyeria social, exactament amb les mateixes accions i relacions seqüencials entre elles, es pot expressar de multitud de maneres usant diagrames DAES. Això es deu al fet que hi ha moltes maneres equivalents de combinar els nodes alternativa i conjunt sense variar la relació final entre les accions que connecten. Aquesta flexibilitat es converteix en un inconvenient quan, per exemple, volem comparar els DAES de dos atacs. Malgrat ser dues instàncies del mateix atac, la representació en DAES diferents, encara que equivalents, en pot obstaculitzar l'anàlisi comparativa.

Per a solucionar aquest problema s'utilitza el DAES normalitzat, en el qual les combinacions de diferents nodes conjunt i alternativa es fixen en una única possibilitat. En concret, les relacions complexes es mostraran en aquesta normalització solament com a alternativa de conjunts.

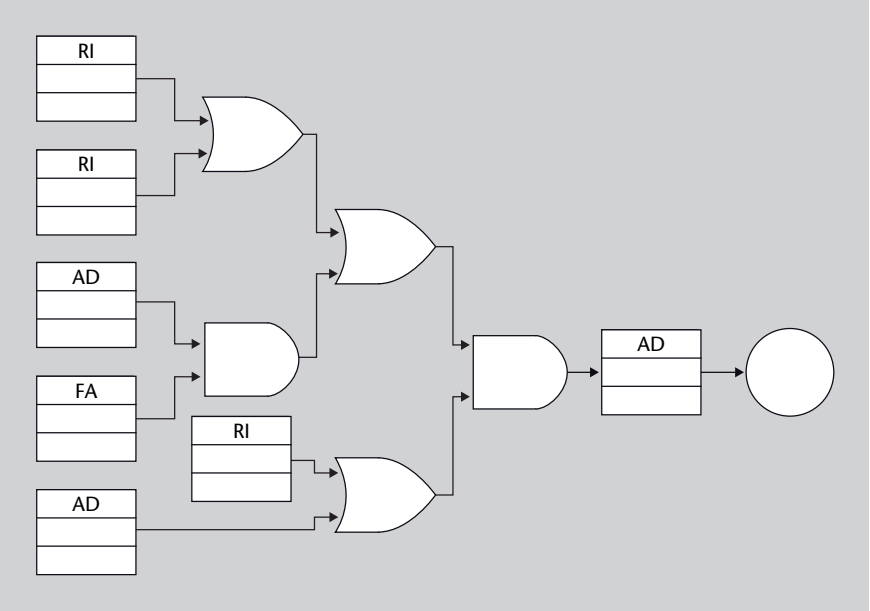
Un **diagrama d'atacs d'enginyeria social (DAES) normalitzat** és un DAES en el qual els nodes alternativa i conjunts solament s'utilitzen de manera combinada com a alternativa de conjunts.

Això no limita l'expressivitat dels diagrames DAES, ja que qualsevol combinació d'aquests nodes té un equivalent en la forma normalitzada. Ho podem veure més clarament si considerem que cada acció té un resultat positiu o negatiu depenent de si s'ha fet amb èxit o no. D'aquesta manera, podem considerar que tenim una estructura algebraica amb dues operacions internes, "+" i "*", les dues sense invers però amb element neutre, amb les propietats associativa, distributiva i commutativa. Així doncs, podem fer operacions sobre aquesta estructura per a aconseguir la forma normalitzada.

Exemple

En l'exemple de la figura 5 es mostra el DAES corresponent a un atac en què hi ha una sola combinació de nodes alternativa i conjunt.

Figura 5. DAES corresponent a un atac



Si expressem el diagrama DAES d'aquesta figura representant el node alternativa com l'operador "+", el node conjunt com l'operador "$*$", i les accions com els operands A_i, tenim una expressió:

$$[(A_1 + A_2) + (A_3 * A_4)] * (A_5 + A_6)$$

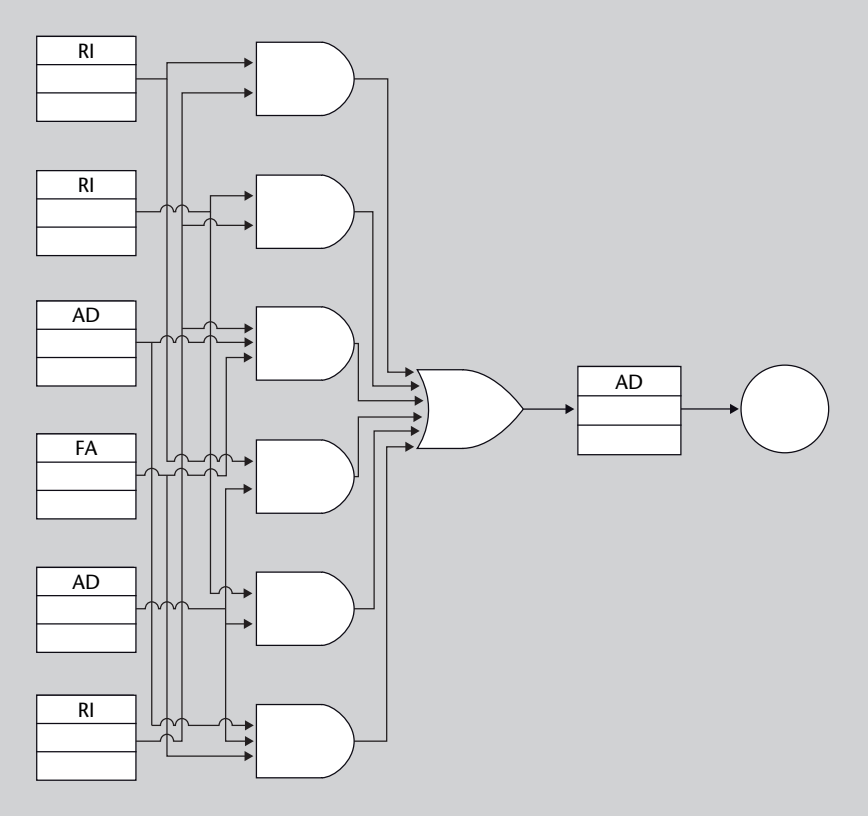
Per a convertir aquesta expressió en la seva forma normalitzada l'expandiríem fins a aconseguir aquesta altra:

$$(A_1 * A_5) + (A_2 * A_5) + (A_3 * A_4 * A_5) + (A_1 * A_6) + (A_2 * A_6) + (A_3 * A_4 * A_6)$$

Després del procés de normalització (figura 6), s'observa com sense canviar la seqüència d'accions de l'atac, aquest es representa de manera equivalent com una alternativa de conjunts. Aquesta manera normalitzada permetrà la comparació directa amb altres diagrames DAES.

Aquest exemple de normalització correspon a una relació molt complexa d'accions. En els atacs més habituals, tal com es veurà en l'apartat 3 de casos pràctics, les relacions solen ser més senzilles.

Figura 6. DAES equivalent normalitzat



2. Estratègies i tècniques

Com hem vist, el procés de l'enginyeria social comprèn un conjunt d'estratègies, tècniques i vies per a aconseguir un objectiu final. D'acord amb això, en aquest apartat presentem una taxonomia d'aquestes estratègies segons tres categories principals:

1) recollida d'informació,

2) forçar una acció i

3) atac directe.

A continuació es descriuran cadascuna de manera més detallada, mostrant també alguns exemples de tècniques i vies associades. És important remarcar que, a diferència de la categorització que es fa per a les estratègies, que és tancada, tant les tècniques com les vies associades que s'exposen aquí no són úniques. És a dir, les tècniques i vies aquí presentades han de ser considerades com a exemples particulars. De fet, tant les tècniques com les vies són suficientment obertes perquè no sigui possible fer-ne una classificació i fins i tot, en un futur, és possible que n'apareguin noves que desconeixem. Per tant, és possible que pugueu trobar altres tècniques associades a cadascuna de les estratègies diferents de les exposades aquí.

2.1. Recollida d'informació

L'estratègia de **recollida d'informació** té com a finalitat captar informació útil per a l'atacant, i per a la qual no hauria de tenir accés hipotèticament.

Es tracta de l'estratègia més senzilla que un atacant pot emprar. La raó d'això és que en la majoria dels contextos en els quals l'enginyer social pot actuar, sempre hi sol haver una certa fuga d'informació.

Aquesta fuga d'informació pot obeir a dos patrons possibles. En primer lloc, la informació pot ser obtinguda en ser exposada de manera inconscient pels usuaris. Aquí, el concepte d'inconsciència l'expressem en relació amb les con-

seqüències que pot tenir des d'un punt de vista de l'enginyeria social. Cal destacar que aquest primer patró sempre implica l'existència d'algun component social o humà. Per tant, la utilització, per exemple, d'un detector de xarxa de manera aïllada no és considerat com a part de l'estratègia de recollida d'informació. En segon lloc, el patró següent se sustenta a obtenir la informació mitjançant la interacció de l'enginyer social amb altres persones. Cadascun d'aquests patrons els denominarem *fuga d'informació sense interacció humana* i *fuga d'informació per interacció humana*, respectivament.

2.1.1. Patró de fuga d'informació sense interacció humana

Dins de la fuga d'informació sense interacció humana trobem diverses tècniques. En concret, n'hi ha tres possibles:

1) cerca a Internet,

2) obtenció física d'informació i

3) l'observació.

En relació amb la tècnica de **cerca a Internet**, un usuari malintencionat pot trobar una gran quantitat d'informació que li pot ser d'utilitat simplement explorant per la Xarxa de xarxes. Per a això, l'atacant pot utilitzar algun cercador web emprant filtres dissenyats específicament, o explorant directament webs conegudes. Alguns tipus de vies per a aquesta estratègia poden ser les xarxes socials, els fòrums o les pàgines web corporatives. En aquests entorns la quantitat d'informació que es pot aconseguir és considerable i molt dispar. Alguns exemples de tal informació poden ser: relacions entre persones, informació sobre la xarxa o els sistemes d'una empresa, persones associades a càrrecs, o números de telèfon, entre altres.

La tècnica de **obtenció física d'informació** es basa en l'apropiació no autoritzada d'elements físics que contenen informació, i dels quals l'enginyer social extraurà les dades interessants posteriorment. Alguns exemples d'aquest tipus d'informació poden ser noms, adreces, números de telèfon, comptes bancaris, comptes de correu, etc. Aquesta categoria la podem subdividir en dues subcategories segons si el tipus d'element físic és d'un sol ús o no. En el primer cas, l'apropiació es farà en sistemes destinats a l'emmagatzematge de deixalles per a la recollida i tractament posteriors (figura 7). Així, algunes de les possibles vies associades són papereres, contenidors d'escombraries, contenidors de paper per al reciclatge, màquines destructores de documents, etc.

Figura 7. Recollida d'informació

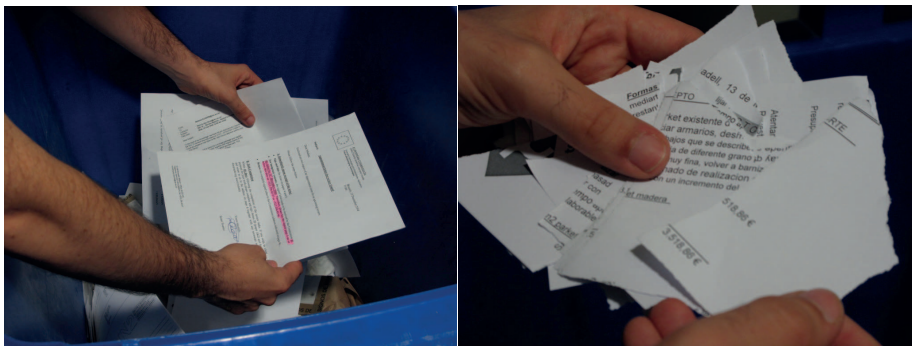


Figura 7

Exemple real de cerca d'informació en un contenidor de paper reciclat. Es poden observar a l'esquerra documents sense destruir, i a la dreta un document en fragments que pot ser reconstruït manualment.

Encara que això pugui semblar inversemblant, la realitat mostra que hi ha una certa despreocupació per part d'organitzacions i empreses per la destrucció efectiva d'elements que contenen informació. Ja no solament d'informació en paper, sinó també en dispositius com ara discos durs o llapis USB. En aquest context, hi ha fins i tot empreses especialitzades en la destrucció de components que contenen informació. Quant a la segona subcategoria, els elements físics no seran d'un sol ús, i l'apropiació es pot fer en qualsevol lloc freqüentat per usuaris. Aquesta subcategoria inclou vies com poden ser agendes, documents, cartes, telèfons mòbils, portàtils, llapis USB, etc.

Figura 8. Trituradora de documents

Figura 8

Exemple de trituradora. Es pot observar a dalt a l'esquerra l'aspecte d'aquesta oberta, i a la seva esquerra el detall del patró de tall del paper. A baix a l'esquerra, una imatge de la mateixa destructora triturant un disc compacte al costat del detall de les fulles encarregades del tall.

Finalment, la tècnica d'**observació** se centra en l'obtenció d'informació basant-se exclusivament a examinar el comportament de persones, fets o objectes. Així mateix, sobre aquesta observació es poden aplicar raonaments lògics basats en relacions entre elements visualitzats per a extreure conclusions. Alguna de les vies possibles que pot utilitzar un enginyer social són les càmeres ocultes, les relacions o els comportaments socials, el seguiment de persones, etc.

A aquesta categoria també pertany la via que denominem *shoulder surfing* (figura 9). Aquesta es basa a observar detingudament les pulsació de les tecles fetes per un usuari en el procés d'entrada a un sistema. Durant aquest procés, l'usuari maliciós captarà visualment les pulsacions tant per al nom d'usuari com per a la seva contrasenya.

Figura 9. *Shoulder surfing*

Figura 9

Simulació d'un atac de *shoulder surf*. A la foto de l'esquerra es pot veure com la víctima introdueix, sense adonar-se del perill, les seves credencials pel teclat. Mentrestant, l'atacant, des d'una posició privilegiada observa la contrasenya introduïda. A la foto de l'esquerra, l'atacant, amb unes ulleres de sol que incorporen una càmera oculta, grava les pulsacions per a analitzar posteriorment el vídeo amb deteniment.

2.1.2. Patró de fuga d'informació per interacció humana

Aquest patró inclou dos tipus de tècniques. La primera la denominem *interacció directa*, i la segona, *interacció mitjançant un mitjà de comunicació*.

La **interacció directa** és aquella tècnica en la qual l'acció recíproca de comunicació entre l'enginyer social i la víctima es fa de manera personal i directa, és a dir, sense l'ús de cap mitjà de comunicació entre totes dues persones.

Aquesta tècnica pot afectar tantes persones com hi pugui haver en una corporació o organisme. Alguns exemples poden ser vigilants, repartidors, recepcionistes, etc. En aquest cas, la via utilitzada és la mateixa conversa que s'estableix entre l'enginyer social i les persones implicades.

La tècnica d'**interacció mitjançant un mitjà de comunicació** és l'homòloga a la interacció directa, amb la diferència que hi ha un mitjà de comunicació entre l'enginyer social i la víctima.

En aquest cas, la via vinculada té multitud de formes, com ara telèfon, carta, correu electrònic, fax, aplicacions de missatgeria instantània, programari de VoIP, etc.

2.2. Forçar una acció

L'estratègia de forçar una acció és aquella que empra algun dels aspectes explotables presentats en el subapartat 1.1., i la finalitat de la qual és la d'aconseguir –de manera directa o indirecta– que algú faci una acció en benefici de l'enginyer social.

Així, una tècnica que explotés l'autoritat podria ser la suplantació d'algú que ocupés un càrrec superior a la víctima, i a la qual persuadiria perquè modifiqués la regla d'un tallafocs amenaçant-li amb un possible acomiadament en el cas de no cooperar. En aquest cas, la via emprada podria ser, per exemple, el telèfon.

Figura 10. Estratègia de forçar una acció

Figura 10

Exemple de l'estratègia de forçar una acció. Un llapis USB amb un enregistrador de teclat especialment preparat és deixat en un lloc comú com pot ser una fotocopiadora. Si alguna persona té la curiositat de conèixer el contingut del llapis USB, pot ser infectada en introduir-lo en la seva màquina. A partir d'aquest moment les seves contrasenyes poden ser compromeses.

Enregistrador de teclat

Un exemple diferent de tècnica podria ser la captura de la contrasenya d'un usuari utilitzant un enregistrador de teclat. Associat a aquesta tècnica es podria emprar un llapis USB preparat com a via que contindria l'enregistrador de teclat camuflat i que seria posat en un lloc proper a la víctima. La víctima, en veure el llapis USB i desconèixer-ne el propietari, el podria agafar i introduir-lo en la seva màquina influïda per la curiositat de conèixer-ne el contingut. A partir d'aquí, el programari maliciós es podria instal·lar de manera automàtica emprant algun tipus de vulnerabilitat (Larimer, 2011) i, posteriorment, enviar les pulsacions de tecles per mitjà de la xarxa.

Explotar l'empatia

Un altre exemple de tècnica estaria basat a explotar l'empatia. En particular, l'atacant podria "donar pena" a una víctima perquè aquesta proporcionés ajuda a l'enginyer social i li facilités, per exemple, informació sobre l'arquitectura d'una xarxa amb l'excusa que li han amenaçat d'acomiadar-lo si no soluciona un problema. Aquí la via emprada seria la mateixa conversa que mantindrien l'atacant i la víctima.

2.3. Atac directe

L'estratègia d'atac directe comprèn aquells atacs de caràcter tècnic que formen part d'un procés d'enginyeria social. Com ja hem vist, aquests tipus d'atac poden ser finals o intermedis respecte al procés d'enginyeria social. Aquests atacs exploten alguna de les vulnerabilitats que hem anat veient al llarg d'aquesta assignatura. Alguns exemples particulars de tècnica empleada en aquest tipus d'estratègia podrien ser un atac de denegació de servei via un SYN *flooding* o una escalada de privilegis via un desbordament de memòria intermèdia.

Figura 11. Atac directe

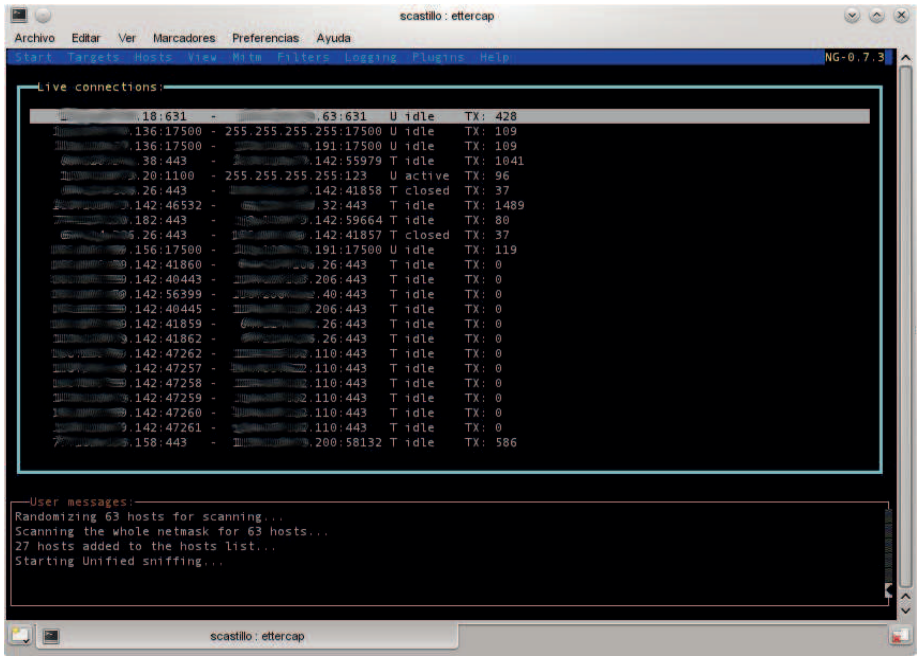


Figura 11

Ús de l'aplicació *ettercap* per a fer un atac directe de tipus ARP *poisoning*.

3. Casos pràctics

En aquest apartat incloem una sèrie d'exemples pràctics d'atacs d'enginyeria social. L'objectiu és consolidar els coneixements vistos en els apartats anteriors. Cadascun dels casos que s'exposen han estat estructurats de la mateixa manera. En primer lloc, s'exposarà quin és l'objectiu final que persegueix l'usuari maliciós. Seguidament, es relatarà quin és el procés de l'atac enumerant els diferents passos que es fan fins que s'aconsegueix l'objectiu final. Per concloure, per a cada exemple es dibuixarà el seu diagrama DAES i es comentarà breument cadascun.

Lectura recomanada

Us animem també a consultar la referència *The Art of Deception: Controlling the Human Element of Security* (2000) de Kevin Mitnick, on podreu trobar altres exemples que us permetran complementar els exposats aquí.

Observació

Aquests casos són totalment ficticis i qualsevol semblança amb la realitat és pura coincidència.

3.1. Cas 1: robatori a un banc electrònic

3.1.1. Objectiu

Fer un robatori en un banc que opera per Internet. És a dir, fer una transferència monetària a un compte remot.

3.1.2. Escenari

A la sala de juntes d'e-Calers, SA, un conegut banc que opera per Internet, es respira un aire tibant. La directora general està explicant que durant l'absència del cap de seguretat hi ha hagut un robatori important (de fet, una transferència irrevocable no autoritzada de molts euros a un compte de les illes Caiman). Les fortes mesures de seguretat informàtica no semblen haver estat efectives, però encara no saben què ha fallat. De sobte, en Carles, que escoltava amb atenció els fets, obre molt els ulls i es comença a ruboritzar.

Fa uns dies, en Carles rebia una trucada. Era d'un tècnic dels serveis d'informàtica de l'empresa que li trucava en relació amb un canvi de programari que s'havia de produir en breu. En Carles ja sabia d'aquest canvi per una circular interna (recordava haver-la tirat a la paperera). El tècnic li va explicar que havia parlat amb el cap de seguretat, Roque Sierra, abans que marxés, i havien acordat que li passarien el codi de seguretat per a l'administració de comptes. Això era, li va explicar, per a comprovar que tot funcionés correctament en la nova versió abans de posar-la en producció. La clau era diferent cada dia, i per això no la hi havia donat en Roque mateix abans d'anar-se'n. A en Carles no li feia gaire gràcia donar aquella clau, però ho va fer finalment considerant racionalment la situació: el tècnic sabia on era el cap, sabia que ell estava a càrrec ara, i, com li va fer veure, no donar-la-hi implicaria retardar el canvi del

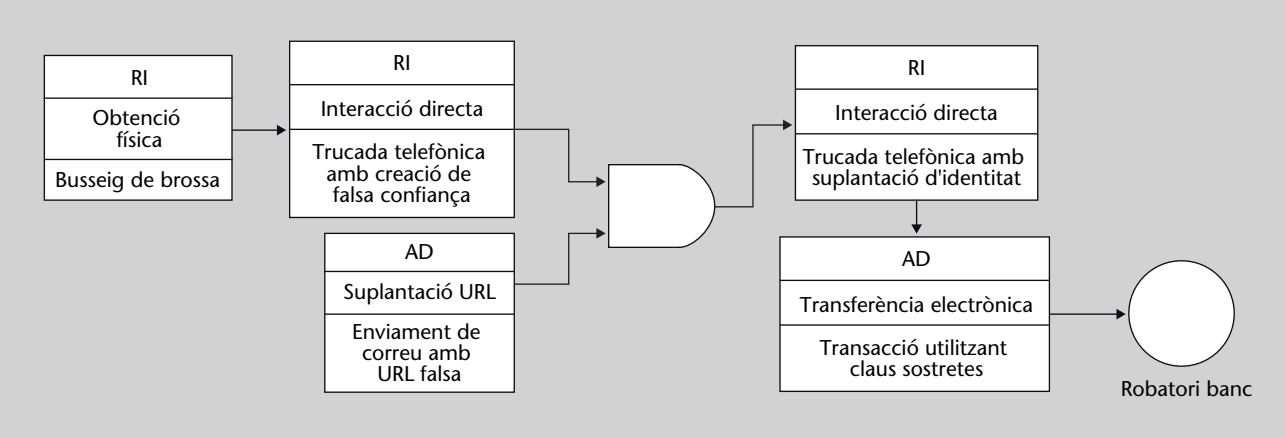
programari per culpa seva i, molt probablement, una reprimenda d'en Roque. A més, en connectar-se des del seu navegador a l'URL que li va donar el tècnic va poder validar la veracitat del que li deia: sota el logotip corporatiu hi havia el full de seguiment del procés de canvi, i en la tasca 16 deia que ell mateix havia de proporcionar el codi en rebre aquesta trucada.

Unes setmanes abans, algú "bussejava" les escombraries en els contenidors de paper d'e-Calers. Alguns empleats que el van veure van pensar que era algun indigent buscant cartró per vendre'l. Res més lluny de la realitat. Aquest personatge estava molt content perquè havia trobat una circular on s'avisava d'un canvi de programari, un resguard d'una reserva d'un bitllet d'avió a nom de Roque Sierra Arán, i algunes còpies de factures de proveïdors de serveis. No li va costar gaire establir certa confiança amb la recepcionista de matins de l'empresa: després de moltes trucades fent veure que era d'una de les empreses proveïdores, ja eren gairebé amics! Sense gaire esforç li va sostreure quina posició ocupava en l'empresa en Roque ("per cert, no coneixeràs un tal Roque Sierra que treballa allí, que és cosí llunyà de la meva cunyada?"), i qui el substituïa.

3.1.3. Diagrama DAES

En la figura 12 es mostra el diagrama DAES d'aquest escenari.

Figura 12. Diagrama DAES cas 1



En aquest cas tenim un únic node de relació de conjunt, que defineix dos conjunts d'accions per fer: d'una banda, l'obtenció de la informació sobre qui és el substitut del responsable de seguretat; i, d'una altra, la preparació d'un lloc web que serà necessari en la part següent de l'atac. A partir d'aquí vindrà el punt més difícil, aconseguir les claus d'accés per mitjà de la persuasió i l'engany, i finalment culminar l'atac amb la substracció econòmica per mitjà del desviament a un compte estranger.

3.2. Cas 2: modificació de la pàgina web d'un portal

3.2.1. Objectiu

Modificar la pàgina web principal d'un portal de venda de llibres com a mesura per a desacreditar-lo.

3.2.2. Escenari

La tenda online e-Books, una tenda que ven llibres per mitjà d'Internet, sap com és d'important tenir una bona imatge des del punt de vista de la seguretat. Aquesta és conscient que les notícies sobre atacs en els quals es compromet la seguretat de portals que ofereixen venda de productes perjudiquen seriosament les vendes, ja que aquest tipus de situacions genera desconfiança en els usuaris compradors.

Des de fa uns mesos, les vendes d'e-Books han descendit considerablement després de l'aparició del portal CheapBooks, que fa ofertes molt competitives i contra les quals e-Books no pot competir. Després d'aquest període de temps de crisi per a e-Books, i en vista de la imminent fallida de l'empresa, el directiu de l'empresa decideix posar en pràctica una campanya de desacreditació de CheapBooks. Per a això, decideix contractar en BlackMan –un individu experimentat a comprometre la seguretat de sistemes– amb la finalitat de modificar la web principal del portal de la competència.

Després de fer en BlackMan una anàlisi de la seguretat del portal de CheapBooks, conclou que aparentment no hi ha cap escletxa remota per explotar de manera senzilla i que li permeti comprometre el sistema. Així mateix, determina que la màquina remota és un sistema GNU/Linux corrent un servidor web Apache. També descobreix que el mateix portal conté un *frontend* d'administració per al qual es requereix un nom d'usuari i contrasenya.

En aquesta situació, i atès que en BlackMan sap que moltes vegades la baula més feble en seguretat és l'home mateix, decideix emprar tècniques d'enginyeria social. Després de buscar per la web de CheapBooks, troba el nom i el telèfon tant del responsable IT com de l'administrador de la xarxa, i també el correu electrònic d'aquest últim, al qual cal dirigir-se en el cas d'haver-hi algun problema amb la pàgina web.

En primer lloc, en BlackMan decideix intentar trucar per telèfon a l'administrador de la xarxa per aconseguir la contrasenya del *frontend* que li doni accés a la part restringida del portal. Per aconseguir això, s'intenta fer passar pel responsable d'IT i li exigeix que li proporcioni la contrasenya per modificar una configuració urgentment. Malgrat això, l'administrador de la xarxa, amb una dilatada experiència en seguretat, reconeix ràpidament l'intent d'atac en

no coincidir el timbre de veu amb la del seu immediat superior. Seguidament l'administrador de la xarxa informa al seu cap de l'intent d'enginyeria social.

Després d'aquest fracàs, en BlackMan decideix deixar passar un temps com a mesura preventiva per no aixecar sospites que algú està intentant comprometre la seguretat de CheapBooks. Transcorregut un mes, decideix emprar una estratègia d'enginyeria social més elaborada. En aquesta ocasió truca per telèfon al responsable d'IT fent-se passar per un proveïdor de maquinari. En aquesta conversa, en BlackMan convenç el responsable d'IT per a mantenir una reunió i poder presentar-li així suposades ofertes d'interès per a l'empresa. Abans de mantenir la reunió, en BlackMan prepara un llapis USB amb un enregistrador de teclat programat per ell mateix, i que no és detectable per cap programari antivirus actual, ja que implementa diferents mecanismes d'ofuscació. Aquest programari maliciós és emmagatzemat en el llapis USB amb aparença de ser un document de nòmines, quan en realitat es tracta d'un executable. En concret, es denomina "Nomines.doc_____.exe". Durant la reunió, feta al despatx del responsable d'IT, en BlackMan deixa caure el llapis USB sense que ningú no se n'adoni. Durant el temps que dura la presentació de productes, en BlackMan intenta ser el més convincent possible i presentar dades reals que ha aconseguit prèviament. En acomiadar-se, demana el correu electrònic al responsable d'IT amb el pretext que li enviarà més informació.

Al cap d'uns dies, el servei de neteja troba el llapis USB en el despatx del responsable d'IT i, pensant que seria d'ell, l'hi deixen damunt de la taula. En arribar aquell dia al despatx el responsable d'IT i veure el llapis USB té la curiositat de saber què conté i el connecta el seu portàtil. En inspeccionar el contingut veu un suposat document amb el nom "Nomines", sense adonar-se que en realitat és un executable. Després d'això, decideix obrir-lo sense ser conscient del perill que representa. Procedeix llavors a fer un doble clic en l'arxiu i, seguidament, l'executable maliciós mateix mostra una finestra dient que el document està corrupte. Després d'això, el responsable d'IT pensa que per algun motiu aquell document està incomplet o és erroni i no presta més atenció a l'ocorregut. Després d'això, el portàtil del responsable queda infectat per l'enregistrador de teclat que va preparar en BlackMan i, a partir de llavors, totes les pulsacions de tecles són enviades per la xarxa a en BlackMan. Gràcies a això, no porta més d'una hora a en BlackMan tenir en poder seu les credencials d'accés com a administrador a una màquina de la xarxa interna denominada `neptuno`.

En adonar-se en BlackMan que la màquina `neptuno` forma part de la xarxa interna de CheapBooks i que, per tant, té una IP d'un rang privat, decideix procedir de la manera següent. En haver obtingut el correu electrònic del responsable d'IT durant la reunió, i conèixer el de l'administrador de la xarxa, envia a aquest últim un correu falsejant el remitent i fent-se passar pel seu superior. Això és possible, ja que el sistema de correu electrònic de CheapBooks

no implementa cap tecnologia com podria ser OpenSPF o DKIM. El contingut d'aquest correu és el següent:

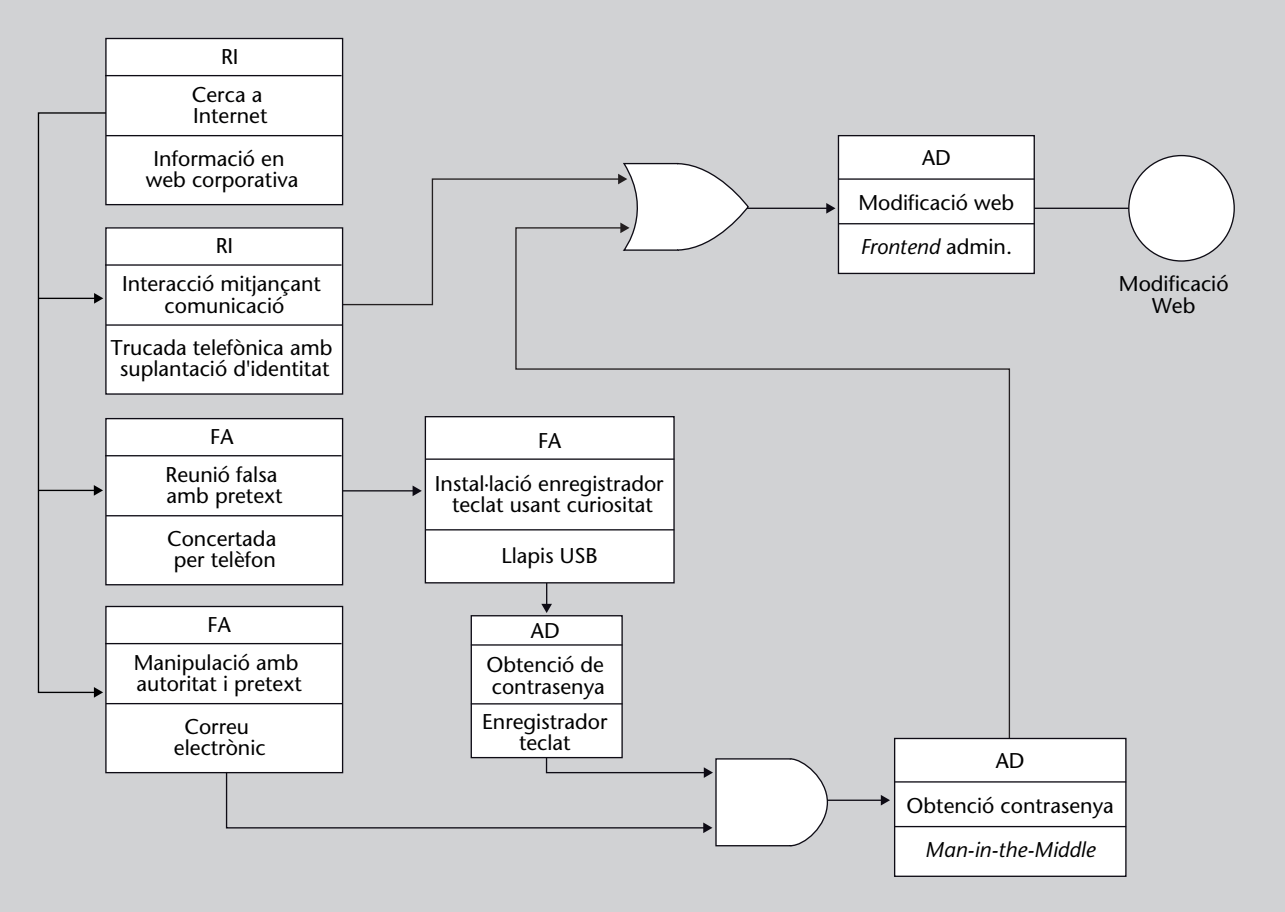
```
Subject: Habilitar NAT cap a neptuno!
From: Juan Sánchez Hipólito <JSanchez@cheapbooks.com>
To: webadmin@cheapbooks.com
Date: 01-06-11 13:50

Hola Toni!
Aquest cap de setmana vinent necessitaria poder accedir
a la màquina neptuno des de casa. Si us plau, afegeix una
regla en el tallafocs per a fer NAT redirigint el port
2222 cap al 22 de la màquina neptuno.
Bon cap de setmana!
```

En rebre el responsable de la xarxa el correu procedeix a fer la petició que li ordenen. Durant aquest cap de setmana en BlackMan es connecta a la màquina `neptuno` des de l'exterior, i s'adona que des d'aquesta no pot accedir directament al servidor web per modificar-ne el contingut. No obstant això, en l'arxiu `/etc/hosts` de `neptuno` descobreix que la IP del servidor web és 10.0.0.10. Després d'una ràpida anàlisi del servidor web des de la xarxa interna, conclou que l'única manera d'accés a aquest servidor és físicament o per mitjà del *frontend* que ja coneixia de feia temps. Llavors, decideix esperar al dilluns, moment en el qual llança un atac de tipus *man-in-the-middle* emprant *ARP-spoofing* que li permet capturar les credencials de l'administrador de la xarxa que l'autentiquen cap al *frontend*. En aquest moment, en BlackMan, amb ple accés al servidor web, modifica la pàgina web principal. En aquesta deixa un missatge en què es proclama que la seguretat de CheapBooks és deficient i que els clients no s'haurien de fiar de les compres que hi fan.

3.2.3. Diagrama DAES

El diagrama DAES de la figura 13 correspon a aquest cas d'estudi. A partir d'informació obtinguda del web corporatiu, s'inicien una sèrie d'accions que es poden fer en paral·lel. En aquest punt no hi ha cap relació d'alternativa ni de conjunt. A partir d'aquí, s'hauran de completar les accions d'instal·lació de l'enregistrador de teclat i l'obtenció de la contrasenya per a poder continuar (seqüència de conjunt) i obtenir la contrasenya amb un atac de *man-in-the-middle*. Una vegada es disposa d'aquesta contrasenya, o si ha resultat amb èxit una recollida d'informació per mitjà de trucada telefònica (seqüència alternativa), ja es podrà fer l'atac final: la modificació de la web per mitjà del *frontend* d'administració.

Figura 13. Diagrama DAES cas 2



3.3. Cas 3: modificació de notes en una universitat

3.3.1. Objectiu

Alterar la nota d'una assignatura en l'expedient electrònic d'un alumne en una universitat.

3.3.2. Escenari

No podia ser que a ella, que es considerava bona en seguretat computacional, li suspenguessin *Criptografia* només per haver tingut un mal dia quan van fer l'examen final. Havia d'actuar per posar els punts sobre les is: es modificaria ella mateixa el 4 que li havia posat el professor, per un 9, una nota més concorde al seu nivell, segons ella.

Després d'esbrinar més o menys com funcionava el procés d'introducció de qualificacions finals en l'expedient electrònic i tancament d'actes, per mitjà dels manuals d'ajuda per a professors publicats a la pàgina web de la universitat, ja podia començar a tramar el seu pla d'atac basat, com no, en l'enginyeria

social. Després de tot, estudiar el criptosistema utilitzat per a trobar-hi vulnerabilitats tampoc no acabava de ser el seu fort.

Intentar aconseguir directament la contrasenya del professor estava descartat. Era un professor de seguretat, de manera que el risc era gran. El primer objectiu, per tant, seria saber en quina màquina hi havia el servidor central d'LDAP. Si comprometia aquesta màquina, podria conèixer, probablement, la contrasenya del seu professor, i llavors entrar utilitzant la seva identitat i fer el canvi de nota.

Després d'algunes trucades per a intentar esbrinar quin ordinador albergava el servidor, va decidir canviar d'estratègia. El personal de la universitat es mostrava molt recelós a revelar detalls tan tècnics. Va pensar en una alternativa enginyosa, i en unes poques trucades telefòniques va esbrinar aviat on enviaven els equips obsolets quan eren substituïts per altres de més nous. No li va ser difícil obtenir, en la planta de reciclatge on enviaven els ordinadors vells, alguns discos durs que venien de la universitat. Encara que el contingut dels discos havia estat esborrat, amb l'ajuda de programari especialitzat va aconseguir recuperar molta de la informació que contenien. En el segon disc va trobar el que buscava: un fitxer de configuració amb l'adreça IP del servidor d'LDAP i la seva contrasenya d'autenticació.

No seria senzill entrar en el servidor d'LDAP des de fora, de manera que hauria de fer una intrusió en un dels ordinadors interns. Després de preparar un programa troià, el va enviar per correu electrònic a diverses persones de l'administració de la universitat. El correu semblava un missatge típic que s'envien entre amics, amb una multitud de destinataris, i feia referència a un vídeo que s'incloïa i semblava molt graciós. Una de les víctimes va seleccionar el vídeo per visualitzar-lo, la qual cosa, a més, va instal·lar un petit programa que donaria accés remot a l'ordinador. Una vegada dins, va aconseguir entrar en el servidor d'LDAP i tenir accés al *hash* SHA1 de la contrasenya del professor. Utilitzant un programa de trencar contrasenyes basat en paraules de diccionari va trobar després d'unes hores la paraula de pas que buscava. Aconseguit!

Amb la contrasenya d'accés ja podia entrar al portal web d'introducció de qualificacions fent-se passar pel seu professor, però encara necessitava una altra contrasenya, la de traspàs de qualificacions a l'acta de l'assignatura. Tenint ja la contrasenya d'accés i les dades bàsiques del professor (número d'identificació a la universitat, nom complet, DNI, etc.) va aconseguir canviar aquesta segona contrasenya per telèfon al·legant que l'havia oblidat.

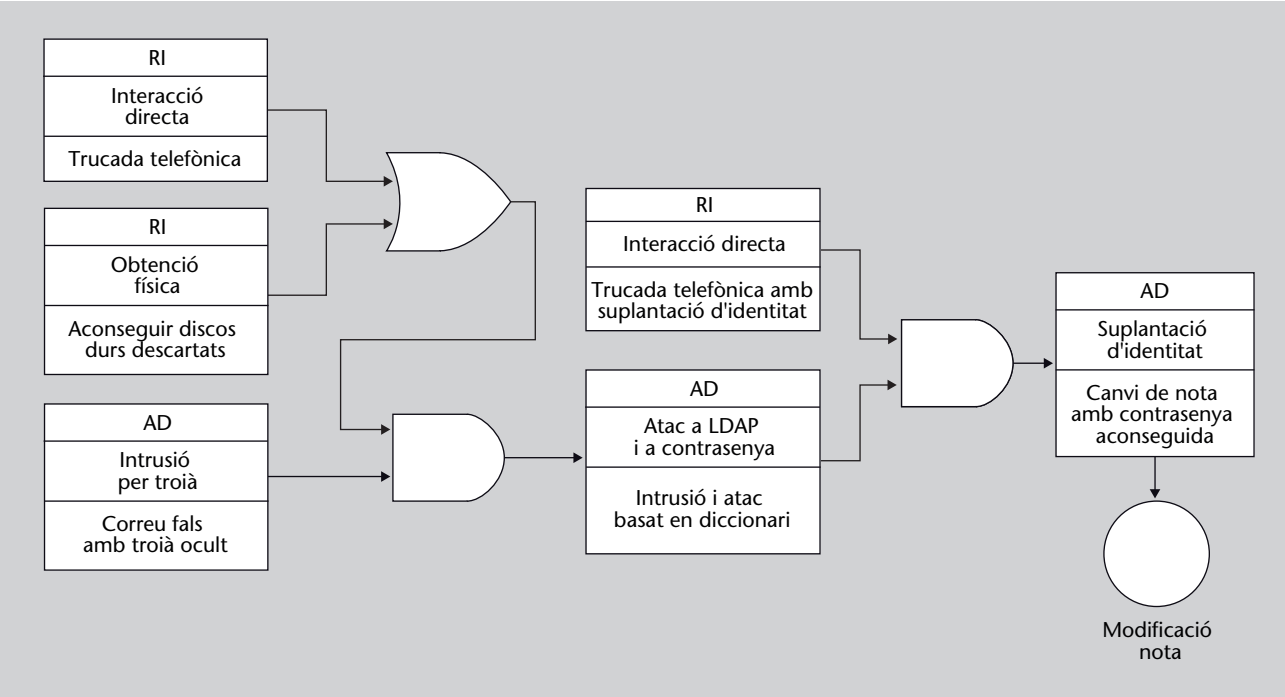
Ara ja ho tenia tot, i solament faltava l'estocada final. Des d'un navegador de la biblioteca, va accedir al portal de notes, es va canviar el 4 a un 9, i va transferir les notes a l'acta. Ja ho havia aconseguit; s'havia fet justícia! L'alegria, no obstant això, li va durar poc. Després d'uns dies, el professor va detectar el canvi quan estava repassant els excel·lents per a decidir qui rebria matrícules

d'honor. Encara que durant tot l'atac no va deixar cap traça que la inculpés, estava clar qui era l'única interessada a modificar aquesta nota en concret.

3.3.3. Diagrama DAES

El diagrama DAES corresponent a aquest cas es mostra en la figura 14.

Figura 14. Diagrama DAES cas 3



En aquest cas veiem les sis accions més importants en aquest atac d'enginyeria social organitzades per mitjà de dues relacions de conjunt i una d'alternativa. En les accions de l'alternativa, començant cronològicament, s'intenta primer obtenir informació per mitjà d'una trucada i, en no aconseguir-ho, s'opta per buscar aquesta informació en un disc dur desinventariat. Amb la informació de la localització del servidor d'LDAP, juntament (relació conjunt) amb el control d'una màquina interna aconseguit mitjançant un troià, ja es pot fer l'atac a LDAP i al *hash* de la contrasenya del professor que hi és. Amb una altra trucada telefònica s'aconsegueix l'altra contrasenya necessària per a fer l'últim atac, que és el canvi de la nota.

4. Casos especials d'enginyeria social

En el context de l'enginyeria social podem trobar multitud d'atacs amb característiques diferents. Aquesta afirmació cobra sentit si recordem que aquests atacs estan definits com un procés compost per un conjunt d'accions relacionades seqüencialment. Entre tot el ventall de diferents possibilitats, hi ha una sèrie d'atacs d'enginyeria social que tenen una especial rellevància per la seva quotidianitat. En aquest apartat tractarem breument cinc casos d'enginyeria social que són familiars per a la majoria dels usuaris, i el denominador comú dels quals és que, a excepció del *SMiShing*, es produeixen en el context d'Internet. Aquests casos especials d'enginyeria social són el *phishing*, el *vishing*, el *SMiShing*, l'*scareware* i els *hoaxes*.

4.1. *Phishing*

El *phishing* és un atac d'enginyeria social l'objectiu final del qual és el d'obtenir dades bancàries d'una víctima amb una finalitat fraudulenta. Per a aconseguir-ho, l'enginyer social suplanta la identitat d'una entitat financera i convenç a un usuari per a fer una acció que li permet captar aquestes dades.

Per a fer phishing, l'enginyer social utilitza el correu electrònic com a via. De vegaes aquest tipus d'enviament es fa de manera massiva a comptes de correu que han pogut ser obtinguts per diferents mitjans. L'enviament indiscriminat de correus es fa amb l'objectiu de maximitzar les probabilitats d'èxit de l'atac. En aquest correu se sol·licita a la víctima que visiti la web de l'entitat, on posteriorment se li demana que introdueixi les seves dades personals al costat de les seves credencials. L'engany en aquest procés es troba en el correu mateix, on se sol incloure un enllaç a la suposada web legítima; no obstant això, aquest enllaç apunta en realitat a un servidor especialment preparat per l'atacant, on és capaç de recollir les dades que li interessen. Depenent de l'habilitat de l'enginyer social per a preparar un correu electrònic convincent, i com sembli de creïble a la víctima, l'atac tindrà èxit o no.

4.2. *SMiShing*

L'*SMiShing* és una variant del *phishing*, amb la diferència que es fa utilitzant missatges de telefonia mòbil de tipus SMS (*short message service*).

Aquí, l'usuari rep un SMS procedent d'una suposada entitat bancària i en el qual se li força, mitjançant enginyeria social, a fer una trucada a un número particular, o a enviar una resposta al missatge amb dades sol·licitades.

Figura 15. Exemple de *phishing*

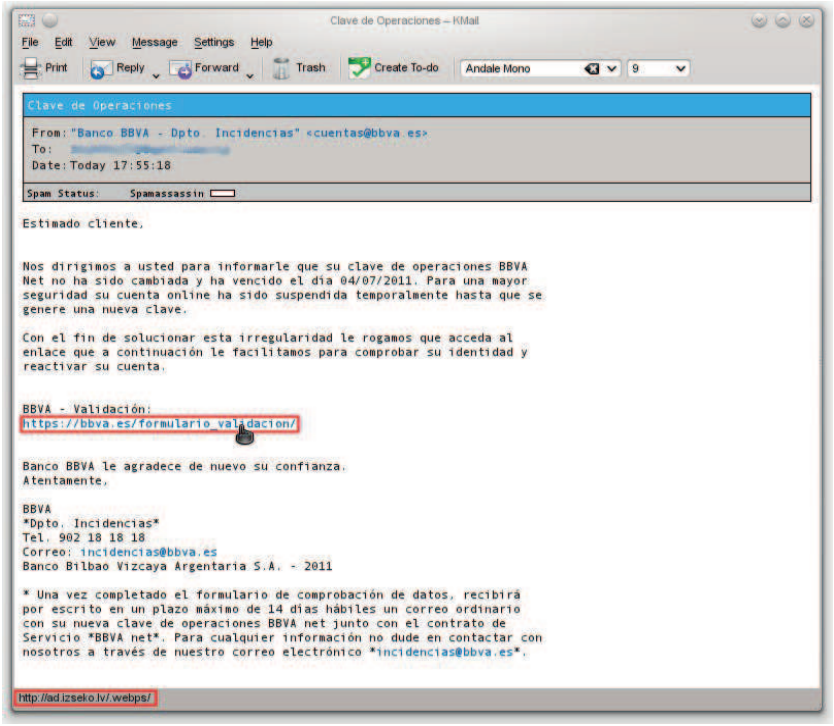


Figura 15

Exemple de *phishing* per correu electrònic. Noteu que l'URL mostrada en el cos del correu no coincideix amb l'apuntada per l'enllaç en la part inferior esquerra de la imatge.

4.3. *Vishing*

El *vishing* és també una variant del *phishing*. En aquest cas, la diferència és que es fa per veu utilitzant el sistema de telefonia tradicional, o de vegades l'enginyer social sol usar els serveis oferts per la telefonia sobre IP (VoIP).

L'atac es basa a utilitzar un sistema automàtic que fa trucades a números de telèfon. Quan detecta que en l'altre extrem hi ha una persona, se li comunica que hi ha algun tipus de problema amb la seva targeta de crèdit i es convenç perquè proporcioni certes dades, entre els quals figura el número de la seva targeta, la data de caducitat i el codi de seguretat.

4.4. *Scareware*

L'*scareware* és una forma de programari maliciós per a obtenir beneficis emprant enginyeria social. En concret, explota l'engany, la persuasió, la coacció o la por mitjançant missatges d'alarma o d'amenaça per forçar la víctima a fer un pagament. L'exemple més comú és el de suposades solucions de seguretat que s'instal·len i ens adverteixen que el sistema està infectat per algun tipus de codi maliciós. A partir d'aquí, l'*scareware* brinda la possibilitat a l'usuari d'eliminar l'hipotètic programari maliciós fent un pagament, ja sigui mitjançant una targeta de crèdit o fins i tot via SMS.

Una alternativa quant al mètode utilitzat és el programari maliciós identificat per alguns antivirus com a *W32/CardPay.A*, *Win32/DotTorrent.A* o *FraudTool.W32*, */Fakecopyright*, entre altres. Es basa a explotar el sentiment de culpa i la por que poden sentir usuaris en descarregar programari il·legal. En particular, una vegada instal·lat mostra missatges d'advertiment indicant que s'estan violant les lleis del *copyright* i que es té identificada la IP de l'usuari. Seguidament, proposa evitar un judici fent un pagament com a manera de solucionar la situació.

Figura 16. Exemple de *scareware*

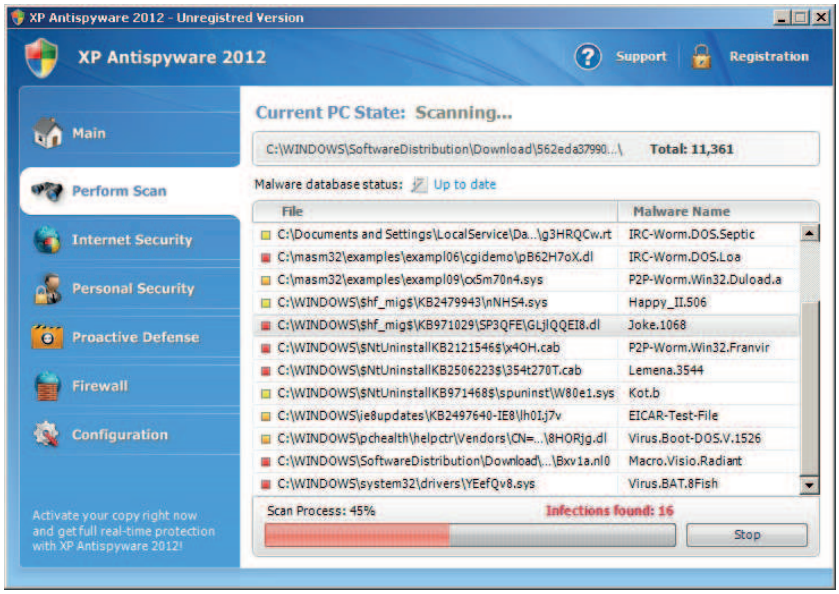


Figura 16

Exemple de *scareware*. La suposada aplicació antivirus mostra que el sistema està infectat per una gran quantitat de programari maliciós, quan en realitat no és així. Posteriorment ofereix la possible compra del producte per desinfectar el sistema.

4.5. *Hoaxes*

Un *hoax* és un tipus d'enginyeria social que es dóna en l'àmbit del correu electrònic. Es basa a crear una notícia o un rumor totalment fals en forma de correu electrònic, en el qual es força el destinatari, utilitzant alguns aspectes explotables barrejats vistos en el subapartat 1.1., a la reexpedició del correu perquè es propagui i distribueixi en cadena.

Darrere els *hoaxes* hi pot haver diferents interessos, com ara causar alarma social, confondre o modificar l'opinió pública, desprestigiar una empresa o la recollida d'adreces electròniques per a utilitzar-les posteriorment com a destinataris de correu brossa. Per això la necessitat d'explotar aspectes com són l'engany, la parquedat, la prova social, l'amabilitat o l'empatia entre altres. Així mateix, la temàtica d'aquests sol ser molt variada, com per exemple: virus informàtics, llegendes urbanes, cadenes de solidaritat, etc. Serveixi d'exemple el correu següent, considerat com un *hoax*:

ATENCIÓ, AQUEST MISSATGE ÉS VERÍDIC!

Saps que la llet en cartró que no es ven dins del termini de caducitat torna a la fàbrica per a ser repasteuritzada i torna al supermercat de nou?. Increïble, veritat?. Doncs la llei permet a les centrals lleteres repetir aquest cicle fins a 5 vegades, la qual cosa acaba deixant la llet gairebé sense sabor i amb una significativa reducció de la seva qualitat i valor nutricional.

Quan la llet arriba al supermercat per a la venda al consumidor final, el cartró ha d'exhibir un petit nombre que està marcat a la part inferior. Aquest nombre varia de l'1 al 5. Com a molt s'ha de tolerar comprar llet fins al número 3, és a dir, llet que ha estat repasteuritzada 2 vegades, i es recomana no comprar cartrons de llet amb nombre 4 o 5, ja que això significa que la qualitat de la llet estarà degradada. Si compres una caixa tancada, n'hi ha prou de verificar el nombre de la caixa, ja que tots els cartrons de dins tindran la mateixa numeració. Per exemple, si un cartró té el nombre 1, significa que és la primera vegada que surt de la fàbrica i arriba al supermercat per a vendre'l, però si té el nombre 4, significa que va caducar 3 vegades i que va ser repasteuritzada 3 vegades i va tornar al supermercat per a tractar de ser venuda i així successivament...

Així és que, ja saps, quan compris llet, mira el fons del cartró i no compris caixes que tinguin els nombres 4 o 5, i per als més escrupolosos, ni tan sols el 3.

En l'arxiu adjunt podreu veure el nombre en qüestió. Aneu al supermercat, agafeu una caixa de llet i comproveu el nombre; dubto que hi trobeu l'1 o el 2.

SI TENS CONSCIÈNCIA CIUTADANA, DIVULGA AQUEST MISSATGE!!

5. Anàlisi

Tradicionalment, les recomanacions que s'han suggerit per a la lluita contra l'enginyeria social han estat enfocades a la formació del personal i les auditories. Aquest tipus de formació té una forta dependència en funció de cada persona, el seu càrrec dins d'una organització i el nivell d'accés que té a informació crítica. Així, la formació que s'ha de donar a una persona de manteniment no hauria de ser la mateixa que a una altra que treballa com a administrador de sistemes. De vegades, aquesta formació és nul·la o tan genèrica que no té en compte les característiques de cada individu. Malgrat això, fins i tot persones amb formació adequada rebuda no s'escapen dels factors humans tan explotats per l'enginyeria social. Hi ha, per tant, la necessitat d'una metodologia que permeti determinar les persones crítiques, i també els requisits de formació de cadascuna d'elles. D'aquesta manera, es podrà fer una èmfasi especial en la conscienciació que han de prendre determinades persones dins d'una organització.

Tal com s'ha pogut comprovar en l'apartat anterior per mitjà de diferents casos, la utilització del diagrama DAES permet obtenir una visió global d'un atac d'enginyeria social. També s'ha pogut verificar com el diagrama es pot construir des de la perspectiva de l'enginyer social abans de fer l'atac, o des del punt de vista d'una auditoria de seguretat després d'haver-se perpetrat l'atac. Com es veurà en aquest apartat, l'ús d'aquest tipus de diagrames va més enllà de la simple comprensió de quina ha estat la planificació o l'evolució d'un atac d'aquest tipus. Concretament, es presenta aquí una metodologia que, partint d'un diagrama DAES, permet analitzar la seguretat dels sistemes d'informació des de la perspectiva de l'enginyeria social. En particular, l'estratègia que es mostra permet analitzar i detectar d'una manera evolutiva els factors de risc que poden intervenir en un possible atac d'enginyeria social. D'aquesta manera, no solament és possible ser conscient de quines mesures tècniques podrien ser incorporades per a millorar la seguretat, sinó també de com cal determinar quines persones crítiques requereixen una formació específica, atesa la seva criticitat davant atacs d'aquest tipus.

Aquesta metodologia es denomina *retroampliació inversa del diagrama DAES*. A continuació descriurem aquesta estratègia, enumerant els passos que s'han de seguir i fent recalcament especial en els elements crítics que ens permet identificar.

5.1. Retroampliació inversa del diagrama DAES

La retroampliació inversa del diagrama DAES és una metodologia iterativa i evolutiva que permet determinar elements crítics en una organització des de la visió de l'enginyeria social. Com el seu nom suggereix, està basada en els diagrames DAES ja presentats anteriorment. Com s'ha pogut comprovar, el diagrama DAES pot ser construït des de diferents punts de vista. Fins ara solament s'han mostrat dos tipus: el diagrama DAES construït per un enginyer social abans d'un atac i el diagrama DAES construït per un especialista de seguretat després de perpetrar-se un atac.

La retroampliació inversa del diagrama DAES parteix de l'atac final del diagrama DAES. A partir d'aquí, l'expert en seguretat haurà d'analitzar i identificar totes les possibles accions de l'enginyeria social predecessores que han conduït a aquest atac final. Cadascuna d'aquestes accions és considerada llavors com un factor de risc. A partir d'això, per cada acció predecessora s'aplica de manera recursiva la mateixa idea. És a dir, es buscaran les accions predecessores d'aquestes ultimes i així successivament.

Estratègia preventiva

La retroampliació inversa treballa amb els diagrames DAES després de perpetrar-se un atac com a mètode correctiu. No obstant això, també pot ser aplicada com una estratègia preventiva partint de potencials atacs finals que es podrien dur a terme en una empresa o entitat, i el denominador comú dels quals és l'ús de l'enginyeria social.

De manera més formal, podem definir la retroampliació inversa del diagrama DAES de la manera següent:

1) Obtenir el diagrama DAES associat a un procés d'enginyeria social.

2) Normalitzar el diagrama DAES.

3) Considerar com a **acció actual** l'objectiu del diagrama DAES normalitzat. Notarem l'acció actual mitjançant l'expressió A_C.

4) Per a l'acció actual A_C, identificar i determinar les accions predecessores A_i ($i = 1...n$) tals que hi ha una relació seqüencial entre cada A_i i A_C.

5) Si algun A_i no forma part del diagrama DAES, afegir-lo al costat de la seva relació seqüencial respecte a A_C en forma normalitzada.

6) Considerar cada A_i com un factor de risc.

7) Per cada A_i, considerar $A_C := A_i$ i repetir de manera recursiva el pas 4 fins que no s'identifiquin més accions predecessores.

És important destacar que el concepte d'identificació i determinació d'accions predecessores que apareix en el pas 4 depèn exclusivament del coneixement que tingui l'expert en seguretat sobre l'organització que estigui fent l'anàlisi. Aquest tipus de coneixement no serà exclusivament social, sinó també tècnic. El motiu d'això és que, tal com hem vist anteriorment, en un atac d'enginyeria social apareixen accions tant de caràcter social com tècnic. Per tant, l'expert de seguretat haurà de conèixer aspectes no solament tecnològics, sinó també organitzatius, el personal que forma part de l'empresa, els nivells d'accés a

informació que té cada individu, etc. Com es pot desprendre d'això, aquest tipus d'anàlisi no és exhaustiva i completa, ja que la quantitat d'accions que poden intervenir en un atac d'enginyeria social és incomptable. Malgrat això, la retroampliació inversa del diagrama DAES ha de ser entesa com una eina d'ajuda per a millorar la seguretat global d'una organització.

Després del procés d'ampliació del DAES, i mitjançant la visualització del nou diagrama, es poden identificar gràficament aspectes rellevants en relació amb l'atac sobre el qual s'està treballant. Així, com ja hem vist en el pseudocodi anterior, una vegada que ha finalitzat l'execució de l'algorisme, tindrem identificats els factors de risc tant humans com tecnològics. No obstant això, el nou diagrama ens permet obtenir més informació. En concret, podem emprar aquesta representació de l'atac per a obtenir les dades útils següents:

- Accions crítiques (tant de caràcter tecnològic com social). Aquestes accions seran aquelles que, eliminant-les, l'atac es veu mitigat considerablement o fins i tot eliminat.

- Conjunt d'accions mínimes perquè un atac tingui èxit.

- Probabilitat d'èxit en cas que es dugui a terme un atac. Això es pot obtenir si introduïm probabilitat en cada relació seqüencial i calculem la probabilitat d'èxit final.

- Nivell de risc de l'atac respecte a la seguretat global. De manera similar al cas anterior, es pot calcular assignant a cada relació seqüencial un valor numèric associat al risc.

Aquesta forma d'anàlisi fins i tot ens permetria establir un conjunt de diagrames DAES que podríem definir com a *patrons tipus de l'enginyeria social*. Això possibilita fer taxonomies i categoritzacions d'atacs, de manera que, conegut un patró i la solució que s'ha d'aplicar, es pot extrapolar a aquell atac que contingui el mateix patró.

5.2. Exemple d'anàlisi mitjançant retroampliació inversa

Amb l'objectiu que us familiaritzeu amb el procediment que s'ha de seguir en la retroampliació inversa del diagrama DAES, presentem en aquest subapartat un cas fictici d'atac d'enginyeria social. En aquest exemple, després d'estudiar el cas i obtenir el diagrama DAES corresponent, procedirem a fer una anàlisi segons la retroampliació del diagrama, la qual cosa ens permetrà deduir els aspectes destacables de l'atac, com ara elements crítics, accions mínimes per a dur a terme l'atac, etc.

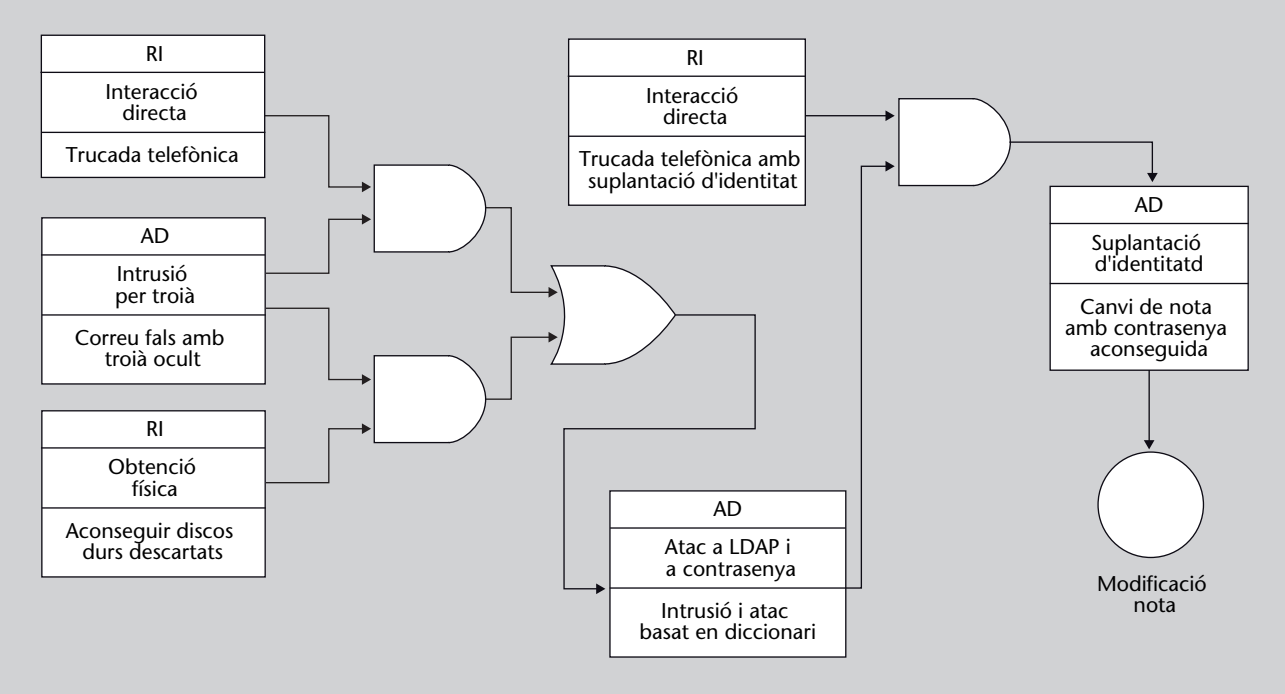
5.2.1. Descripció de l'escenari

Per a fer aquest exemple d'anàlisi s'utilitzarà l'escenari de modificació de notes en una universitat descrit en el subapartat 3.3. d'exemples pràctics.

5.2.2. Retroampliació inversa del diagrama DAES

Els primers passos per a fer l'anàlisi és obtenir el diagrama DAES i normalitzar-lo. El diagrama DAES s'observa en la figura 14, i la versió normalitzada en la figura 17.

Figura 17. Diagrama DAES normalitzat del cas 2



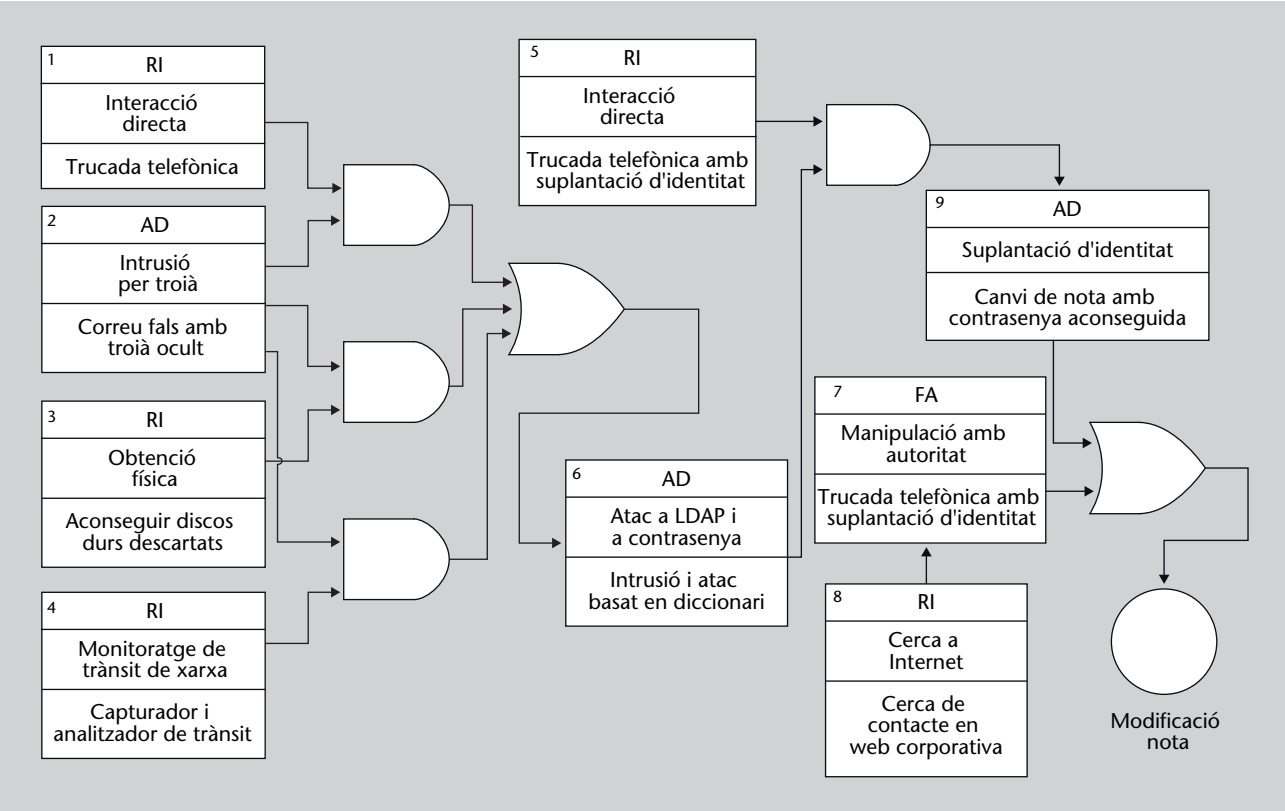
Després de la normalització del diagrama DAES, l'analista de seguretat pot procedir a identificar i determinar accions predecessores, i també les seves relacions de seqüencialitat, partint de l'objectiu final. En el nostre cas, aquest procés no el farem de manera exhaustiva, atesa l'existència d'una estreta relació entre les accions que s'han d'afegir en el diagrama retroampliat i el context en el qual ens trobem.

En l'escenari que ens ocupa, l'analista partiria de l'objectiu final, és a dir, del canvi d'una nota per suplantació d'identitat mitjançant una contrasenya obtinguda. Per a aconseguir aquesta modificació, una alternativa seria forçar una acció. En concret, aquesta consistiria a convèncer, via telèfon, algú de gestió acadèmica que l'enginyer social és el professor responsable mateix de l'assignatura i que la nota d'un alumne particular ha de ser modificada. Analitzant les possibles maneres d'aconseguir el telèfon de contacte de gestió acadèmica, l'analista de seguretat s'adona que en la web de la universitat apareix aquest

número (estratègia de tipus obtenció d'informació). Per tant, la relació de seqüència entre totes dues accions (recollida d'informació primer, i forçar una acció, segon) conduirien al mateix objectiu final.

Prosseguint amb l'anàlisi, l'expert en seguretat, en estimar quins són els predecessors de l'atac directe a LDAP i a la contrasenya del professor, podria adonar-se que l'autenticació contra el servidor d'LDAP es fa amb un protocol en clar. És a dir, en el procés d'autenticació contra el servidor la contrasenya corresponent viatja sense xifrar. La combinació d'usar un troià al costat de la captura de trànsit a la xarxa interna podria permetre a un potencial usuari malintencionat aconseguir la contrasenya d'autenticació cap a aquest servidor. A partir de llavors, aconseguir la contrasenya emmagatzemada en SHA1 seria un pas trivial. En la figura 18 podem observar el diagrama ampliat resultant.

Figura 18. Diagrama DAES normalitzat i ampliat del cas 2



Després de l'obtenció del diagrama DAES ampliat, podem deduir directament que les accions crítiques són la 2, 6, 7 i 9. D'altra banda, els conjunts mínims d'accions per a aconseguir l'objectiu són {1,2,5,6,9}, {2,3,5,6,9}, {2,4,5,6,9} i {7,8}.

6. Prevenció i reflexions

El procés de l'enginyeria social és ben conegut, i les seves bases han estat utilitzades durant segles per a fer accions fraudulentes de diversa índole. Amb l'aparició dels sistemes computacionals d'informació, l'enginyeria social ha cobrat una especial rellevància en no aplicar-se ja únicament al món físic, sinó al món digital. Al llarg d'aquest mòdul hem vist com des del punt de vista de la seguretat informàtica les vulnerabilitats que permeten atacs d'aquest tipus estan molt lligades a les tecnologies disponibles.

No obstant això, les solucions per a evitar atacs d'enginyeria social són un tema molt més complicat i, malgrat ser un aspecte fonamental en la seguretat dels sistemes d'informació, el trobem gairebé marginat en la bibliografia i exclòs en molts tractats de seguretat. El motiu és la complexitat associada a aquest problema. Encara que hi ha algunes mesures per a minimitzar la probabilitat d'èxit dels atacs d'enginyeria social, veurem en aquest apartat que no hi ha una manera d'eradicar completament aquestes greus vulnerabilitats.

Les maneres d'afrontar el problema es basen en la formació i sensibilització, i també en la definició i aplicació de polítiques de seguretat.

6.1. Formació i sensibilització

La formació del personal en una organització sobre l'enginyeria social és un element bàsic per a la lluita contra aquesta. No obstant això, no és clar qui han de ser els receptors d'aquesta formació, ja que tot el personal relacionat amb l'organització d'una manera o una altra és susceptible de ser víctima de l'enginyeria social. Això inclou des del personal de neteja i manteniment, fins als alts càrrecs de gerència.

Per a ser efectiva, l'aprofitament de la formació s'ha de validar freqüentment, normalment mitjançant auditories especialitzades. Així mateix, una mesura que sol ajudar a millorar els resultats d'aquest procés de formació és la utilització d'esquemes d'incentiu/penalització, que recompensin el personal que utilitzi de manera adequada els coneixements adquirits i que penalitzi, econòmicament o d'una altra manera, el qui demostri no haver aprofitat aquesta formació. D'aquesta manera s'incentiva el personal a considerar seriosament els problemes de seguretat associats a l'enginyeria social.

El problema més greu del procés de formació és el cost elevat, ja que ha d'estar dirigit a un col·lectiu molt nombrós; es tracta d'una docència molt espe-

cialitzada i requereix una validació constant generalment per mitjà d'auditories. Una alternativa molt més econòmica són les campanyes de sensibilització. L'objectiu d'aquestes campanyes és conscienciar els membres d'una organització sobre els mètodes utilitzats per l'enginyeria social per a poder identificar-los quan es presenten i poder així evitar-los. La sensibilització pot ser complementària a la formació, i reservar aquesta última per als col·lectius més sensibles.

Figura 19. Exemple campanya de sensibilització

Figura 19

Esquerra: exemple de pòster d'una campanya de conscienciació sobre el problema de l'enginyeria social. Conté consells bàsics per a evitar els atacs més freqüents. Dreta: samarreta de sensibilització de l'enginyeria social.

6.2. Polítiques de seguretat i auditories

A més de la formació, és molt important incloure punts específics sobre l'enginyeria social en les polítiques de seguretat de l'organització. La figura 20 mostra alguns exemples de punts que s'haurien de tenir en compte en les polítiques de seguretat d'una organització.

Figura 20. Exemple de campanya de sensibilització

- L'abast de la informació sensible no ha d'anar més enllà del cercle de persones estrictament necessari.
- Els documents amb informació sensible estaran sempre desats sota clau quan ningú els custodiï.
- En cap concepte es facilitaran claus d'accés per telèfon o correu electrònic, encara que qui les sol·liciti proclami ser un administrador.
- La presència de persones desconegudes s'ha de reportar sempre al responsable de seguretat.
- Tots els documents seran destruïts quan acabi la seva vida útil, sense importar si contenen informació sensible o no.
- Cal desconfiar sistemàticament dels missatges rebuts per correu electrònic i de les trucades telefòniques.
- Sempre que sigui possible, retornar les trucades o correus electrònics per a assegurarnos que no hi ha una suplantació de personal.
- Utilitzar criptografia per a garantir l'autenticitat i el secret del correu electrònic.
- Mai no seguir enllaços proporcionats per correu electrònic o telèfon; en lloc d'això, buscar l'enllaç d'altres fonts.
- No utilitzar dispositius d'emmagatzematge (com llapis USB o discos durs, per exemple) que han tingut contacte amb l'exterior de l'organització.

Per a validar l'aplicació correcta de les polítiques de seguretat, és convenient fer auditories especialitzades en enginyeria social de manera periòdica. Les auditories permeten detectar també noves vulnerabilitats, amb l'actualització corresponent de les polítiques. El cicle de definir polítiques de seguretat i auditar s'hauria de repetir de manera contínua.

6.3. Enginyeria social, psicologia i humanitat

La majoria de les vulnerabilitats explotades per l'enginyeria social, tal com s'ha vist en el primer apartat d'aquest mòdul, estan derivades de qualitats humanes com la facilitat d'establir certa confiança entre individus després d'un període d'interacció. Algunes d'aquestes qualitats, com la caritat o la cortesia, són generalment considerades aspectes positius en la nostra societat. D'altres, com l'empatia o el desig d'ajudar, responen a reaccions més instintives. Fins i tot els aspectes més racionalment controlables, com la reacció davant l'autoritat o l'avarícia, es poden usar per a manipular psicològicament l'individu i exercir una influència per a la realització d'accions induïdes.

Si considerem un ordinador immune als atacs d'enginyeria social és precisament perquè manca de totes aquestes qualitats que ens acaben fent, precisament, humans. Si una persona es comporta de tal manera que no sigui possible manipular-la d'alguna manera utilitzant les tècniques descrites, serà molt difícil que estigui integrada en la societat, ja que la percepció que se'n tindrà és molt negativa. Ho podem veure clarament amb un exemple. Si al tercer intent d'introduir una contrasenya en un ordinador que utilitzem habitualment, aquest ens bloqueja l'accés fins que un supervisor no el torni a habilitar, ens conformarem resignadament. Si, en canvi, una persona ens demana la identificació per a entrar a la feina i un dia l'hem oblidada, no entendrem per què ens bloqueja l'accés, i li exigirem flexibilitat apel·lant, precisament, a la seva humanitat. És difícil comprendre en el moment que aquesta mateixa flexibilitat podria permetre l'accés a un atacant.

Evitar el problema, per tant, és molt difícil, si no impossible. Les estratègies de formació i conscienciació són clarament útils i necessàries, però no eludeixen totalment els atacs d'enginyeria social. Per a evitar l'atac cal focalitzar en la part final del diagrama DAES estès, és a dir, en les amenaces directes, per a bloquejar els atacs assumint que l'enginyer social té a la seva disposició tota la informació.

Resum

Sens dubte, la seguretat computacional és una disciplina complexa a causa de la gran quantitat d'àrees interrelacionades que abasta. Moltes vegades s'incorre en l'error de considerar aquestes àrees des d'una perspectiva exclusivament tecnològica, quan la realitat va molt més allà. Un clar exemple d'això és l'enginyeria social, un dels components de la seguretat que moltes vegades passa desapercebut o al qual no es dóna la importància que mereix. La realitat ha demostrat, en més d'una ocasió, que en seguretat la baula més feble de la cadena continua essent el component humà i, per tant, l'enginyeria social no ha de ser menyspreada com a font de possibles atacs.

Al llarg d'aquest mòdul hem dissecat l'enginyeria social fins a concebre-la com un procés, compost per un conjunt d'accions i relacions seqüencials entre elles. En tot atac d'enginyeria social, el denominador comú sempre serà l'existència d'alguna acció basada en la manipulació psicològica de les persones. Darrere d'aquesta manipulació s'amaguen múltiples aspectes explotables, i que l'atacant pot usar a favor seu per aconseguir el seu objectiu final.

L'existència d'aquests aspectes humans explotables, més propis de la psicologia social, no ens han de fer caure en l'error de pensar que no formen part del domini de la seguretat computacional. Per tant, els hem d'integrar en tot procés d'anàlisi i de millora de la seguretat dels sistemes d'informació. En aquest sentit, hem vist com els diagrames DAES són una eina que permet establir una metodologia analítica de gran utilitat. Així, els diagrames DAES ens permeten representar atacs d'enginyeria social d'una manera gràfica, al mateix temps que són la base per a detectar elements crítics en una organització per mitjà de la retroampliació inversa.

Finalment, no hem d'oblidar quines estratègies preventives han de ser utilitzades per a evitar atacs d'enginyeria social. Aquestes estratègies impliquen una formació adequada del personal, considerant la seva posició dins de l'organització jeràrquica, així com el nivell de privilegis d'accés que tingui a sistemes i informació. Així mateix, la definició de polítiques clares de seguretat per a evitar atacs d'enginyeria social ha de ser imposada. Com a mesura per a garantir que aquestes polítiques de seguretat són conegudes i posades en pràctica per tot el personal, les auditories de seguretat han de ser utilitzades com a manera de validar-ne el compliment.

Activitats

1. Busqueu a la vostra paperera física informació que podria ser utilitzada per a fer un atac d'enginyeria social. A partir de les dades individuals que obtingueu, intenteu pensar en com les relacionaríeu i en trauríeu possibles conclusions.

2. Busqueu en el vostre correu electrònic un cas de *phishing* i de *hoax*.

3. Trobeu a Internet exemples de *hoaxes* i raoneu quines accions s'haurien de prendre si en rebem algun.

4. Busqueu exemples de *hoax* a Internet i redacteu-ne un de nou tenint en compte els aspectes explotables vistos en aquest mòdul. No l'arribeu a enviar.

5. Simulem que, com a enginyer social, heu aconseguit un llapis USB del qual voleu extreure informació. Per a això, demaneu a algú que hi copiï cinc arxius qualssevol. Després d'això, indiqueu a aquesta persona que elimini dos d'aquests arxius. A continuació, simuleu que heu aconseguit el llapis USB sense el seu consentiment. Seguidament, descarregueu l'eina TestDisk* i intenteu recuperar els arxius eliminats. Creieu que els usuaris són conscients de la possibilitat de recuperació de dades? Com relacioneu això amb l'enginyeria social?

6. Penseu un possible atac d'enginyeria social que es podria donar al vostre lloc de treball o estudi habitual. Dibuixeu-ne el diagrama de DAES corresponent i normalitzeu-lo. Intenteu aplicar-li la retroampliació inversa perquè sigui més complet.

7. Busqueu alguna notícia real en la qual l'ús de l'enginyeria social hagi estat present d'alguna manera.

8. Feu una petita enquesta en el vostre lloc d'estudi o treball sobre el coneixement i la conscienciació de les persones davant els atacs d'enginyeria social. Quina proporció d'enquestats creieu que saben què és l'enginyeria social? Compareu la vostra previsió amb els resultats que heu obtingut.

Atenció!

Aquest exercici podria causar la pèrdua d'informació! Feu aquesta activitat amb la màxima cautela possible. Llegiu amb deteniment la documentació del TestDisk abans de fer-la. Assegureu-vos que la recuperació l'apliqueu sobre el llapis USB amb el qual treballeu.

***http://www.cgsecurity.org/wiki/TestDisk**

Exercicis d'autoavaluació

1. Quina afirmació és certa sobre els diagrames DAES?
- **a**) Són una representació exhaustiva d'un atac d'enginyeria social que preveu totes les accions possibles.
- **b**) La seva versió normalitzada no permet la comparació amb altres diagrames.
- **c**) Poden ser expressats a partir d'una estructura algebraica amb dues operacions internes.
- **d**) Cap de les anteriors.

2. Quin dels aspectes següents no s'explota directament en l'enginyeria social?
- **a**) Receptivitat a l'autoritat
- **b**) Fàcil establiment de confiança
- **c**) Inundació per amplificació de peticions DNS
- **d**) Recuperació de dades d'un disc dur

3. L'ús d'un llapis USB amb un enregistrador de teclat pot ser emprat en un atac d'enginyeria social mitjançant una estratègia de tipus...
- **a**) recollida d'informació.
- **b**) forçar una acció.
- **c**) atac directe.
- **d**) Cap de les anteriors.

4. Un atac d'enginyeria social...
- **a**) empra els aspectes explotables humans.
- **b**) és l'acció amb la qual finalitza tot procés d'enginyeria social.
- **c**) pot ser contrarestat amb mesures tecnològiques.
- **d**) a) i c)

5. Un programa instal·lat en un sistema que identifica una gran quantitat de virus i que ens suggereix comprar-lo per a desinfectar la màquina és un tipus de...
- **a**) *phishing*.
- **b**) *hoax*.
- **c**) *scareware*.
- **d**) Totes les anteriors.

6. El *phishing* explota...
a) la falsa confiança.
b) la reciprocitat.
c) la similitud.
d) Totes les anteriors.

7. La retroampliació inversa...
a) no requereix un diagrama DAES normalitzat.
b) no és útil si no s'ha produït un atac d'enginyeria social.
c) condueix a un DAES que conté accions de l'atac encara que aquestes no hagin estat identificades per l'analista de seguretat.
d) Cap de les anteriors.

8. En la retroampliació inversa l'analista de seguretat...
a) ha de tenir un coneixement social i jeràrquic respecte a les persones de l'empresa implicada.
b) no és necessari que conegui els mecanismes de seguretat tecnològics implantats en l'empresa.
c) és capaç d'identificar tots els elements crítics.
d) Cap de les anteriors.

9. Quina afirmació és certa sobre l'enginyeria social?
a) No és necessari conscienciar els usuaris sobre mesures per a evitar ser víctimes d'aquests atacs.
b) No es pot evitar solament amb mesures tecnològiques.
c) No afecta els sistemes de tipus Unix.
d) Totes les anteriors.

10. Per minimitzar la probabilitat d'èxit dels atacs d'enginyeria social, una organització pot...
a) ampliar la política de seguretat.
b) oferir un pla de formació específica.
c) iniciar una campanya de conscienciació.
d) Totes les anteriors.

Solucionari

1. c; **2.** c; **3.** b; **4.** a; **5.** c; **6.** a; **7.** d; **8.** a; **9.** b; **10.** d.

Bibliografia

Cacioppo, J. T.; Petty, R. E.; Kao, C. F.; Rodriquez, R. (1986). «Central and peripheral routes to persuasion: An individual difference perspective». *Journal of Personality and Social Psychology*, (núm. 51, pàgs. 1032–1043).

Cialdini, R. B. (2008). *Influence: Science and Practice*. (5a. ed.). Pearson Education.

Larimer, J. (2011). «Beyond Autorun: Exploiting vulnerabilities with removable storage». BlackHat, Washington (USA): IBM X-Force Advanced Research.

Mitnick, K. D.; Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security*. (1a. ed.). Nueva York: John Wiley & Sons, Inc.

Myers, D. G. (1994). *Exploring social psychology*. Nueva York: McGraw-Hill.