Social Engineering, una guida introduttiva.

Versione 1.1

Andrea Ghirardini aka Pila

C.T.O. Pila's Security Services (http://www.pilasecurity.com)
Socio CLUSIT, Associazione Italiana Sicurezza Informatica (http://www.clusit.it)
Certificato CISSP, Certified Information System Security Professional (http://www.isc2.org)
pila@mclink.it

I N D I C E

Disclaimer

Le opinioni e le informazioni espresse nel presente documento appartengono agli autori e non ad aziende: esse non rappresentano in alcun modo idee, politiche aziendali o servizi specifici se non il pensiero e l'esperienza degli autori stessi.

Il disclaimer standard si applica al presente documento, in particolare modo per la non responsabilità degli autori, verso qualunque tipo di danni - causati direttamente o indirettamente – conseguenti alla lettura del presente documento e/o all'utilizzo illegale o fraudolento delle informazioni e/o funzionalità ivi contenute.

Gli autori non si assumono alcuna responsabilità per i contenuti di questo documento – così come di eventuali errori od omissioni – o di qualunque documento, prodotto o servizio da esso derivati, indirettamente o meno.

Il presente documento può essere liberamente distribuito, pubblicato o copiato con ogni mezzo disponibile a patto che lo stesso non venga modificato in alcun modo e previa autorizzazione scritta degli autori.

E' assolutamente vietato "appropriarsi" della proprietà intellettuale dell'opera, ovverosia spacciarsi per gli autori, tradurlo in altre lingue appropriandosene la paternità o estrapolare singoli paragrafi spacciandosi per l'autore degli stessi.

ABSTRACT

Lo scopo di questo paper è riassumibile in due punti fondamentali

1- Mostrare quali sono le reali possibilità della social engineering al fine di stimolare l'opinione pubblica a prendere in considerazione il fatto di dover adottare delle contromisure a questa forma di "information leaking"

2- Fornire un tutorial così che possa essere utilizzato dai penetration tester per compiere un controllo quanto più accurato e variegato possibile.

Come tutti i Technical Paper dell'Associazione Italiana Black Hats, anche questo documento può essere letto dal punto di vista dell'attaccante o del gestore del sistema stesso: vale in ambo i casi la regola "conosci il tuo nemico prima di"…

Ogni qualvolta se ne presenterà la possibilità il presente documento verrà aggiornato, con le nuove scoperte o gli update rilevati da ITBH: ovviamente invitiamo i lettori a comunicarci eventuali errori, imperfezioni o aggiornamenti dei quali siano a conoscenza, così come sistemi operativi non citati nel presente documento.

Buona lettura,

Andrea "Pila" Ghirardini

Introduzione

Tutti noi siamo abituati a pensare ad un hacker (white, gray o black hat che sia, la distinzione non è lo scopo di questa guida) nella sua forma più "romantica" dettataci dalla storia recente o dai media:

> *"...un ragazzo, al lavoro, al buio, chino sul computer, circondato da apparecchi tecnologici, da scarti di pizza, da tazze sporche di caffè, mozziconi di sigaretta e con ogni superficie piana occupata da manuali, documentazione o print-out di vario genere, intento a digitare comandi e a lanciare attacchi verso un bersaglio posto all'altro capo del mondo..."*

Siamo così ancorati a questa idea che non prediamo nemmeno in considerazione questa non sia corrispondente alla verità.

Così i wannabe hacker chiedono alle figure più carismatiche tool e nozioni per portare attacchi ai sistemi informativi più disparati. Allo stesso modo le compagnie (piccole, medie e grandi), gli enti pubblici, i centri di ricerca e chiunque si affacci ad internet per fornire un qualunque tipo di informazione o servizio si attrezzerà con una serie di dispositivi di sicurezza (siano essi firewall, appliance di vario genere, IDS o altro) con un unico scopo: tenere gli hacker fuori dai propri sistemi.

Porta sprangata... finestra aperta

Tutto questo porta a trastullarsi in un falso senso di sicurezza pensando di aver chiuso ogni possibile via d'entrata ai propri sistemi.
In realtà nulla potrebbe essere più lontano dalla realtà dato che un hacker ha decisamente altre frecce al proprio arco, altrettanto efficaci e decisamente più subdole. Questo paper mira a fornire una conoscenza piuttosto approfondita di una di queste arti, la social engineering.

CAPITOLO 1

1.1 Social Engineering

L'arte della social engineering è ancor più antica di quella dell'hacking come noi lo conosciamo. I primi che la utilizzarono estesamente furono i phreaker per riuscire a carpire informazioni vitali dalle compagnie telefoniche.

Come possiamo definire la social engineering? Potremmo dire che si tratta di "un metodo per ottenere informazioni mistificando la nostra reale identità durante la conversazione con un altro essere umano".

La social engineering si basa su due assiomi fondamentali:

1. **Gli esseri umani sono esseri molto fiduciosi nel prossimo e tendono a credere a ciò che si dice loro**

2. **Se un computer è decisamente meglio di un essere umano a memorizzare delle informazioni, quest'ultimo è indubbiamente il soggetto migliore per fornirle ad altri**

Un classico esempio è il vecchio proverbio "*l'abito non fa il monaco*" che, nella vita di tutti i giorni, si dimostra irrimediabilmente falso. Infatti, se per strada vedete un uomo con un saio, difficilmente penserete che che sia qualcosa di diverso da un frate francescano.

Nulla di nuovo quindi sotto il sole. Eppure la social engineering è sempre stata legata saldamente al mondo dell'hacking e del phreaking. Non solo ma molti hacker conosciuti e rispettati per i loro skill tecnici erano primariamente degli ottimi social engineering. Possiamo citare Kevin Mitnick oppure Mark Abene (aka *Phiber Optic*) e John Lee (aka *The Corruptor*) del gruppo dei "Master of Deception".

Teniamo infatti presente il fatto che nella maggior parte dei casi, per i motivi già spiegati nell'introduzione, le "vittime" della social engineering non sono assolutamente preparate.

CAPITOLO 2

2.1 Tool utilizzati

Un buon social engineer dispone di una serie di strumenti, che possono essere utilizzati per portare a termine il proprio lavoro e per migliorare l'efficacia dello stesso.

1) Uno o più telefoni. Un telefono cellulare, uno fisso e una buona connessione ad internet sono strumenti necessari. Anche un telefono pubblico può essere un buon surrogato in alcune occasioni.

2) Un Fax

3) Un computer munito di stampante e di un buon programma di Draw o DTP unito possibilmente ad uno scanner o a una stampante multi funzione (utile per produrre carte intestate o per copiare loghi o firme)

4) Un server di posta. E' molto utile avere una macchina Unix disponibile con installato un server SMTP da poter riprogrammare a seconda delle necessità senza dover passare per un server SMTP esterno (con le regole di antispam ed altri orpelli è meglio non appoggiarsi a server esterni)

5) Un ambiente consono: il che significa che se telefonate al call center della società dei telefoni dicendo loro che siete un tecnico in strada non potete farlo chiamando dallo studio di casa in perfetto silenzio, ne' tanto meno dire che siete un tecnico di un call center ad una vostra "vittima" chiamando dalla cucina mentre la mamma sta preparando la cena. Sembra scontato ma i particolari sono fondamentali quando si millantano credenziali altrui

6) Un blocco appunti o un buon programma per poter collegare ed organizzare le proprie idee. Non c'è nulla di peggio di inventare cose a caso (ivi compreso il proprio nome o la propria funzione) e di cambiarle in "corso d'opera" perché ce li siamo dimenticati. Il milgior programma per riuscire ad organizzare le proprie idée e per creare una “matrice di contatti” è *“The Brain”* , acquistabile al sito http://www.thebrain.com. Sfortunatamente è un’applicazione che ha un certo costo (75 $) e, purtroppo, funziona solo per la piattaforma Windows, ma, nel suo campo è una killer application. All’interno di The Brain le vostre idee vengono raffigurate tramite un albero tridimensionale in wireframe. Ad ogni nodo o ad ad ogni foglia potete aggiungere informazioni, sotto forma di note o di allegati, e/o collegamenti ad altri nodi/foglie. Descritto può sembrare complicato ma, con un minimo di assuefazione, permette di organizzare anche strutture aziendali molto complesse e navigabili in modo estremamente rapido, anche in tempo reale durante una telefonata con il nostro contatto.

CAPITOLO 3

3.1 Informazioni

Le informazioni sono la base del social engineer. E' impossibile riuscire a carpire le informazioni senza aver preparato un piano di "attacco" in maniera meticolosa e, perché no, scientifica.

3.2 Dove procurarsi le informazioni necessarie?

In questa fase si coincide con il lavoro di preparazione che fanno molti buoni hacker nel momento in cui devono controllare un sistema informativo.

3.2.1 Il dominio e i dns

Dalla registrazione del dominio possiamo dedurre una serie di particolari che ci potranno fornire le prime basi della nostra ricerca:

1) Il contatto tecnico, che, probabilmente, coinciderà con una figura di spicco del reparto IT

2) Il contatto amministrativo, che potrebbe coincidere con l'amministratore delegato o con una figura di responsabilità delle dirigenza.

3) Per entrambi dovrebbero essere forniti numeri di telefono e indirizzi di e-mail.

4) E' bene tenere conto di di due cose:

5) I record potrebbero non essere aggiornati (vedremo come verificare)

6) Il contatto tecnico potrebbe coincidere con una figura tecnica del manutentore del dominio, quindi una persona dello staff del provider piuttosto che della società proprietaria del dominio. Può comunque esserci utile in un secondo momento.

7) Dato che stiamo lavorando in quest'ambito è buona cosa procurarsi anche una serie di informazioni utili quali:

8) Il SOA record del DNS (si può capire chi gestisce i dns)

9) L'indirizzo del (o dei) mail server (utile per capire chi gestisce i server di posta)

3.2.2 Il server Web

Il server Web dell'azienda è una cornucopia di informazioni per il social engineering. In particolare è bene notare come nella maggior parte delle ditte medio/grandi il management sia oltremodo felice di includere nelle sue pagine una serie di informazioni

che il visitatore comune non guarderà mai ma che fanno sempre "molta scena". Nel nostro caso sono una vera panacea:

1. L'organigramma, spesso una delle cose più ambite dal social engineer
2. La lista dei partner della società
3. Tutti gli indirizzi di e-mail inseriti
4. Tutti i banner *"Powered by"*

   Con queste due informazioni possiamo costruirci una prima versione della nostra "matrice di contatti" capendo

5. Come è strutturata la società
6. Quali sono le persone chiave
7. Quali sono le relazioni tra i diversi reparti/dipartimenti
8. Quali sono le relazioni tra la società in esame e le consociate

   Inoltre si possono ricavare una serie di informazioni di corollario che ci possono essere utili:

9. Osservare il sorgente delle pagine web per capire con quale strumento sono state realizzate
10. Osservare le note di copyright così da capire se il sito è realizzato internamente alla società oppure da una ditta esterna. In questo caso trovare quanto prima l'indirizzo di e-mail del webmaster può esserci molto utile.

Se usate *"The Brain"*, create un nuovo brain e modellatelo sulle informazioni che avete ricavato in questa fase. Consolidatelo poi con quanto scoprirete nella fase di scanning. Da questo punto in poi il brain continuerà ad espandersi con quanto scopriremo nelle fasi successive.

3.2.3 Scanning

A questo punto prepariamoci ad affrontare una fase di verifica delle informazioni raccolte. Telefonate al centralino e chiedete di parlare con il contatto tecnico. Se ve lo passano riagganciate prima che quest'ultimo risponda. Nel caso la risposta sia un laconico:
"Il signor XXXX non lavora più per noi", chiedete, con gentilezza il nome della persona che ha preso il suo posto. Ripete ad libitum per tutti i contatti trovati (ovviamente non a raffica altrimenti la persona del centralino si potrebbe insospettire), tranne quello amministrativo (se è una figura di vertice l'iter può essere complesso).

CAPITOLO 4

4.1 Gli skill e i tool del social engineer

4.1.1 La voce

Non pretendiamo certo di possedere il dono che avevano le Bene Gesserit nel romanzo di Frank Herbert, Dune. Possiamo però affermare che una sonora "faccia di bronzo" è un requisito fondamentale, dato che ovviamente non ci si può mettere a ridere in faccia al nostro interlocutore. Chiarito questo ovvio passaggio è bene ricordarsi che il nostro tono di voce ed il nostro atteggiamento devono essere adeguati alla circostanza.

Può sembrare scontato ma ovviamente non useremo un tono arrogante se pretendiamo di essere un neo assunto che chiede al reparto IT la password per collegarsi ne', tantomeno, faremo gli umili se chiamiamo un impiegato pretendendo di essere il sysadmin alla ricerca di informazioni su un account.

Adeguiamoci al contesto e cerchiamo di aver chiaro l'organigramma aziendale e di conoscere la posizione del nostro interlocutore in relazione alla figura che noi stiamo interpretando.

Altre cose da tenere in considerazione sono le seguenti:

1) **Attenzione** a cercare di mistificare la propria voce: spesso la cosa "sa di falso" dopo le prime tre sillabe e quindi può essere più controproducente che efficace. Meglio un tono naturale e tranquillo che metterà a proprio agio il vostro interlocutore.
2) **Gentilezza** e sorrisi. Se avete mai fatto un corso per fare assistenza telefonica ricorderete una frase che veniva ripetuta alla nausea: un sorriso si percepisce anche per telefono. Niente di forzato ma una battuta un pizzico di humor e un sorriso cordiale sono tutti elementi che contribuiscono a distendere l'atmosfera. Questo non significa che dobbiamo trasformarci in cabarettisti al telefono
3) **Gli accenti**: fate molta attenzione a non voler dare "un tocco di classe" cercando di imitare un accento strettamente Barese se vivete in Val d'Aosta. Sembrereste più una parodia di Lino Banfi piuttosto che un tecnico che chiama dal Sud Italia. Lanciatevi in un tentativo di questo genere solamente:

1. Se è STRETTAMENTE NECESSARIO
2. Se avete vissuto nella zona della quale volete imitare l'accento
3. Se avete un genitore/nonno/parente-strettissimo di quella zona
4. Se la vostra vittima NON è di quel luogo

TIP: IMHO la miglior cosa è un accento totalmente neutro, possibilmente eviscerato da modi di dire ricorrenti che potrebbero farvi riconoscere. Fatevi ascoltare da un amico e ditegli di segnarsi i vostri "manierismi vocali" come l'intercalare di un "no", di un "you know" (tipico americano), di parolacce ripetute, strascicamento di vocali all'inizio/metà/fine parola, balbettii. Cercate poi di lavorare sui vostri difetti.

I toni: specialmente quando si parla con un comune utente è necessario assumere un tono di *"fredda competenza"* atto ad intimidire il più possibile il nostro interlocutore. Questo non significa assumere toni sprezzanti nei confronti della persona a cui parliamo, semplicemente la fredda cortesia tipica di colui che è immerso tutto il giorno *"in problemi tecnici troppo complessi".*

Il gergo: il gergo è una delle armi migliori e nel contempo un grosso problema per il social engineer. Un gergo tecnico molto criptico, intercalato da spiegazioni alla "amico idiota", è un ottimo metodo per intimidire un comune utente. Di contro è necessario particolare attenzione quando si parla con un responsabile IT fingendo di essere un neo assunto o un comune utente. Anni di esperienza possono aver radicato così profondamente un gergo molto tecnico all'interno del nostro linguaggio che potrebbe essere difficile tornare ad esprimersi con termini "non propri". Per chiarire:

Gergo	Termine da utilizzare
NT-1	"Scatola grigia sul muro" o "borchia"
Convertitore di interfaccia	"Scatola grigia"
Router	"Coso blu pieno di luci"
Bridge ADSL	"Modem"
	"Modem ISDN"
Collegamento HDSL	"Connessione ad Internet"

Inoltre resistete alla tentazione di spiegare eventuali errori che vi siete inventati per improvvisare una comunicazione con il reparto IT. La frase chiave, odiata da qualunque IT ma assolutamente diffusa, è "si è piantato tutto" o "non funziona niente". Questo copre qualunque tipo di errore, dalla stampante senza carta fino ad un crash del server dipartimentale.

Un corso di recitazione per principianti potrebbe essere un eccezionale investimento. Controllate nelle compagnie teatrali della zona (costano solitamente pochissimo) ma non trasformatevi in un Dario Fo' al telefono.

La naturalezza è la base di tutto, controllate quello che combinate quando siete costretti a parlare con un po' di nervosismo addosso. Niente fiumi di parole, niente pause eterne, niente uuuuh, ahhhh, ehm, ehhhh o altro. Ma state pure attenti ad una eccessiva scorrevolezza, che sa più di pavimento incerato che di una persona normale. e soprattutto..... niente panico.

Avete commesso un errore?
Non sapete cosa dire?

Respiro profondo e avanti come nulla fosse, altrimenti non farete altro che rimarcare il problema.

4.1.2 "La base comune"

Un buon social engineering oltre ad essere un discreto conoscitore della psiche umana deve necessariamente avere un panorama estremamente variegato e dettagliato dell'ambiente in cui lavora e si trova la sua "vittima".

Tutto questo è necessario per creare quel rapporto di fiducia sufficiente a far sì che si abbassino le difese inconscie che noi erigiamo quotidianamente nei nostri rapporti interpersonali. E' infatti assolutamente scontato che, ad esempio, siamo molto più propensi a fornire informazioni, anche banali come può essere l'ora attuale, ad un nostro collega di lavoro appena assunto piuttosto che ad uno sconosciuto per strada.

La differenza tra le due situazioni è infatti giustificabile da una cosa della massima importanza e che è un fondamento della social engineering: "la base comune". Una "base comune" tra due individui è in grado di far sì che la naturale (poca) diffidenza che esiste tra due estranei venga abbassata a livelli accettabili. La cosa interessante è che tale "base comune" non deve necessariamente essere qualcosa di concreto o di saldo come un'amicizia o un rapporto di parentela. Può essere qualcosa di assolutamente effimero, come una sensazione, un sorriso, una gentilezza, una passione comune, o l'impressione di appartenere ad uno stesso insieme di individui.

Per far questo quindi è necessario possedere molte informazioni sull'ambiente in cui è calato il nostro interlocutore. Dobbiamo conoscere per esempio la città in cui vive al punto da poter fare dei riferimenti così chiari da poter sembrare un concittadino, oppure la sua società in modo da passare, perlomeno, come un neo assunto da poche settimane.

4.1.2.1 Un esempio chiarificatore

Poniamo di voler estorcere delle informazioni dal signor Rossi che lavora nella filiale di Verona della "Pincopallo inc.". Prima di contattare la persona in questione con un qualunque media, dovremo cercare di conoscer per lo meno alcuni dei seguenti punti:

1. Cosa fa e cosa produce la "Pincopallo inc"
1. Dove ha le principali filiali
2. Quanti dipendenti possiede
3. Com'è organizzata
4. Le partnership che quest'ultima ha con altre aziende
5. Conoscere i principali fornitori della "Pincopallo inc"
6. La posizione in azienda del signor. Rossi

A seconda delle informazioni in nostro possesso potremo fingere di essere:

1. Un neo assunto della stessa filiale
2. Un dipendente di un'altra filiale
3. Un fornitore in cerca di spiegazioni
4. Un cliente
5. Un rappresentante di un'azienda partner

4.1.3 E-mail

L'e-mail è diventato probabilmente lo strumento principe per le comunicazioni aziendali. Rapido, informale, semplice da creare, veicola la maggior parte delle comunicazioni interne all'azienda.

Il social engineer deve quindi padroneggiare questo strumento nel migliore dei modi al fine di velocizzare i propri attacchi e rendere più incisive e precise le proprie richieste.

Ora è chiaro che chiunque è in grado di spedire un e-mail ma è bene tenere presente una serie di tip:

1) Lavorare per convincere un paio di persone all'interno dell'azienda,specialmente una persona del reparto IT a spedirvi una mail (i motivi possono essere i più svariati). Dagli header avremo l'accortezza di ricavare:
    1. Il nome del mailer utilizzato all'interno dell'azienda
    2. Il formato standard (testo ascii o html)
    3. Indirizzo ip del server di mail dell'azienda. Verificate la presenza di filtri antispam e cercate, se possibile, di utilizzare lo stesso server per spedire i vostri messaggi
    4. Le signature: controllate le signature delle mail che ricevete e controllate se sono standardizzate o se ognuno usa la propria. Fate sempre il grabbing delle signature delle persone delle quali volete assumere l'identità
2) Se qualcuno è abituato a segnare digitalmente le mail non preoccupatevene troppo. La maggior parte delle persone non controlla la signature digitale quindi potete usare una signature fake solo per fare la figura di metterla. Se volete buttare cenere negli occhi ai vostri interlocutori, mandatevi la mail che avete preparato e poi usate le funzioni del mailer per effettuare un forward presso i vostri interlocutori. Dato che il forward altera la mail aggiungendo dei > o altri segni a inizio riga è normale aspettarsi che la signature digitale non funzioni e quindi potete mascherare una signature totalmente fake. Ricordatevi comunque che la signature deve almeno essere un "cut & paste" di quella della persona che volete impersonare. Non corrisponderà con il testo che userete voi ma almeno l'identificativo del certificato o della chiave pgp sarà quello corretto.

4.2 Allenamento

Gli scherzi telefonici ai vostri amici possono essere degli ottimi allenamenti per riuscire a capire quanto siete preparati. Ingannare persone che conoscete è un'ottima prova delle vostre capacità di social engineering.

Chi vi scrive in Dicembre dello scorso anno combinò questo:

> *"... mia madre abita in una zona piuttosto impervia e fredda. Durante le festività natalizie il freddo fu così intenso da ghiacciare, e di conseguenza rompere, la condotta dell'acqua corrente che collega casa sua al paese e lasciare i miei genitori senza acqua per oltre 20 giorni.*

Poco dopo il recupero della piena funzionalità (30 Dicembre) dell'acquedotto mia madre ricevette la telefonata di un impiegato della società comunale che gestisce la distribuzione dell'acqua che le spiegò di aver trovato delle irregolarità nei pagamenti delle bollette e che, se non avesse ricevuto un fax con la copia delle ricevute, avrebbe dovuto sospendere la distribuzione fino a chiarimento avvenuto.

Mia madre, nota per il suo carattere battagliero alla Attila, e appena riavutasi dai disagi precedenti rimase a confabulare e questionare al telefono con l'impiegato per oltre 40 minuti Era così infervorata che "l'impiegato" dovette dirle un paio di volte "Mamma calmati, sono io!", prima che realizzasse che in realtà parlava con il "benamato" figliolo."

CAPITOLO 5

5.1 Un primo attacco: Il reparto IT

Il reparto IT è il primario bersaglio del social engineer dato che è quello che detiene sia il "potere" sia le conoscenze sul sistema informativo aziendale. Inoltre c'è un motivo molto più subdolo, sono coloro che meno si aspettano di essere considerati potenziali vittime, quindi la sorpresa è dalla nostra.
Per riuscire a conoscere un po' meglio i componenti del reparto IT ci sono dei metodi piuttosto collaudati:

1. **Il questionario**: Se avete capito che il vendor del server web è commerciale (ma anche che l'azienda utilizza un tool piuttosto che un altro od un so per i propri server interni o stazioni di lavoro) preparatevi una serie di domande inerenti al prodotto in questione (web server, DB o SO) e poi chiamate il centralino chiedendo di passarvi il contatto tecnico o chi lo sostituisce (IMHO il tutto risulta migliore se telefona una ragazza, gli informatici sono sempre poco corteggiati ;-P) Una volta che questo risponde fategli le domande preparate. Questo metodo ha il vantaggio di ottenere due risultati con una sola telefonata:

I. Verificare il contatto tecnico e chiedergli indirizzo, telefono ed altri dati personali
II. Carpire una nutrita serie di informazioni sul sistema informativo interno, a patto, ovviamente, che abbiate posto le domande in questione con un po' di "granum salis"

TIP: *Spesso sono tutti troppo occupati per dedicarvi dieci minuti, quindi siate così accorti da far presente al vostro contatto che tra tutti i partecipanti al sondaggio verrà estratto un premio (non troppo cospicuo, non dite un Cray-1, ma nemmeno troppo patetico tipo un euroconvertitore, piuttosto qualcosa di molto geeky tipo un Palm o un lettore di MP3)*

TIP 2: *Se chiamate per un sondaggio sulla piattaforma Microsoft, siate coerenti e non dite che il premio è un Apple iPod, anche se è molto geeky!*

2. **Il concorso**: Variante del questionario, ottenuto via e-mail e mandato a tutto lo staff IT. Fa decisamente più figura se mandato per snail-mail su carta intestata, ma il problema poi è l'indirizzo di ritorno che, per evitare che sia sospetto, deve essere necessariamente gestito attraverso una cassetta postale. Due considerazioni:
   I. Il concorso via e-mail può essere vanificato dal fatto che la nostra mail venga cestinata come una qualunque junk-mail.
   II. Di contro, in caso di risposta ci può fornire sia la "signature" di quella persona del reparto IT (utile per mandare mail fasulle) sia il PATH che la mail fa attraverso l'azienda che ci potrebbe quindi fornire qualche particolare in più rispetto ad eventuali mail server interni, oltre alla piattaforma client (benedetto Outlook Espress)

3. **Job Hunting**: Nessuno può resistere agli allettamenti di una società di ricerca del personale che telefona interessata per proporre una collaborazione o, meglio, un lavoro ben retribuito. Qualunque IT Manager non assolutamente "aziendalista" ci

fornirà tutte le notizie possibili sui progetti a cui ha partecipato all'interno dell'azienda, in barba a qualunque rapporto di riservatezza, pur di gonfiare opportunamente il proprio curriculum vitae in maniera da distinguersi dalla "massa". Sfruttate il più possibile questa opportunità, ricordandovi che è unica (nel senso che non potete chiamare ogni pochi giorni con questa scusa). Se avete veramente il ritegno di venditore d'auto usate, provate a chiedere al vostro interlocutore di segnalarvi altri nominativi, potreste trovarvi ad intervistare l'intero reparto IT!

TIP:
Chiamate la vittima in ufficio e fatevi dare il suo mumero di casa o di cellulare: sarà più propenso a parlare in un luogo isolato e lontano da "orecchi indiscreti"
Cercate di prepararvi una lista di domande che siano, al tempo stesso, rivelatrici ma non troppo sospette. Sfruttando ben l'occasione con qualcuno del reparto IT potrete ottenere una marea di informazioni. Se direte loro che state cercando "esperti di sicurezza" sarete legittimati a porre loro domande molto precise su come hanno implementato politiche di sicurezza interna.

5.2 Surfing on the Internet

E' il momento di correlare un po' di informazioni che abbiamo già ottenuto sul sistema informativo dell'azienda e su altri articolari così gentilmente forniti dal reparto IT.

In primis utilizzate un buon motore di ricerca (esiste altro oltre a Google?) e dategli in pasto i nomi e i cognomi di tutte le persone che avete reputato interessanti, seguiti subito dopo dal loro indirizzo di e-mail. Se siete fortunati troverete una valanga di informazioni utili:

1. News: Controllate tutti i newsgroup nei quali queste persone scrivono. Potreste trovare una panacea di info, rimaste nella memoria storica di internet. Tra questi monitorate con una certa cura i newsgroup tecnici dato che i membri del reparto IT potrebbero aver postato richieste di aiuto sul sistema informativo aziendale. Mi è capitato ben più di una volta di trovare marca/modello/versione del firewall aziendale, nonché stralci della configurazione. Non trascurate poi i newsgroup riguardanti argomenti non tecnici. Sapere che, ad esempio, Marco Romiti ha una passione per l'aereo modellismo vi tornerà utile (vedi capitolo "La base comune") per non parlare del fatto che bazzica su alt.sex.bondage ;-P
2. Maling list: vale tutto ciò che abbiamo scritto riguardo ai newsgroup con inoltre una serie di particolarità. Monitorate le mailing list di eventuali LUG locali e controllate a chi la nostra "vittima" risponde più frequentemente o con toni più familiari. Potrebbe tornare utile. Controllate inoltre il rapporto domande/risposte sull'argomento principale della mailing list. Se il tipo fa molte domande ma non risponde mai a nessuno potrebbe essere un indice di scarsa competenza che potrebbe riflettersi sulla qualità del suo lavoro all'interno dell'azienda. Infine fate il grabbing delle sue signature (utile per e-mail "spoofate") e cercate di analizzare lo stile con cui scrive (uso dei verbi, modi di dire, formalità del tono di scrittura, uso della punteggiatura)
3. Siti Web personali: Servono commenti? ;-P

5.3 L'utente

L'utente, creatura principe dei sistemi informativi aziendali, è per il social engineer l'equivalente di un'antilope per un leone africano. Attraverso le mani dell'utente si possono compiere i peggiori misfatti che possano passare per la mente dei security specialist, il tutto dalla posizione privilegiata dell'utente, ovvero di essere all'interno della rete, al di là del firewall eretto come unica barriera per tenere fuori dal sistema gli intrusi.

L'utente è quindi il tramite attraverso il quale carpire informazione, lanciare attacchi, compiere esplorazioni ed infine completare con successo il penetration test.

Dobbiamo quindi scegliere con cura la persona con la quale parlare.

5.3.1 La scelta

5.3.1.1 Le figure da evitare

L'amministratore delegato: sempre toppo impegnato e sicuramente poco propenso a farsi "comandare" a distanza.
Spesso e volentieri è meglio evitare anche figure di spicco come dirigenti e capi progetto, dato che sono figure di difficile gestione. Useremo il loro nome per legittimare invece richieste ai loro sottoposti.
Nessun altro. ;-P

5.3.1.2 Le figure migliori

La segretaria dell'amministratore delegato.
Solitamente la persona in azienda che ha gli stessi diritti dell'amministratore delegato e del quale legge gestisce posta, contatti, agenda e chissà che altro. Il suo computer è un repository di carte intestate, template e di una marea di documenti riservati. Inoltre la sua signature è in grado di legittimare anche le comunicazioni più strane. Se riuscite a convincerla a mandarvi una mail avrete tra le mani un'ottima chiave per tutti i livelli dell'azienda.

Il reparto IT
Più l'azienda è grande e più il reparto IT sarà un bersaglio ottimo per farsi fornire nuovi login e password, per farsi dare informazioni sulle procedure di gestione dei nuovi utenti e per farsi abilitare all'utilizzo di nuovi servizi. L'orario migliore per usufruire di questo "servizio" è prima delle nove del mattino (è piuttosto normale che un neo assunto sia zelante al punto di arrivare sul posto di lavoro piuttosto presto e nel contempo è probabile che chi sia al reparto IT non sia tra le figure di responsabilità) o dopo le diciotto.

Le persone al centralino/portineria

Hanno visibilità completa di chi entra e di chi esce dall'azienda, inoltre smistando tutto il giorno, visitatori, tecnici, trasportatori, manutentori sono dei veri esperti di dove si trovano depositi, apparati, sale server, contatori ed altro.

Personale amministrativo (o non produttivo)

Personale dell'amministrazione

Sono solitamente i meno avvezzi all'uso del computer e quindi i più facilmente intimoribili dal un tono alla "sysadmin" o da parole come "fault di rete", "virus", "trojan", "crash". Inoltre coloro che lavorano per l'amministrazione sono spesso coloro che hanno accesso ad una serie di informazioni riservate non disponibili ad altri reparti dell'azienda.

CAPITOLO 6

6.1 Esempi di attacco

Nota: gli esempi seguenti sono tutti reali, anche se ovviamente i nomi e i riferimenti più ovvi sono stati cambiati.

6.2 RAS e Trasferte

Durante il pen-test di un pubblico ufficio trovammo una situazione piuttosto positiva. I firewall erano ben configurati, i router blindati a dovere e i server Web patchati e configurati a dovere.
Durante una sessione di war-dialling trovammo però un numero al quale rispondeva un modem.
Telefonammo ad uno dei sistemisti spacciandoci per una azienda di sondaggi che lavorava per Microsoft e, applicando il metodo del sondaggio, apprendemmo che in ufficio era presente un server RAS per i dipendenti che lavoravano "sul campo".

Controllammo il server web e scoprimmo che l'ufficio possedeva alcuni geometri che spesso facevano rilevazioni sull'esterno. Telefonammo al centralino e chiedemmo di farci passare uno dei geometri. Quando rispose ci spacciammo per qualcuno dell'ufficio amministrativo che chiedeva alcuni chiarimenti rispetto alle ultime trasferte. Ci facemmo mandare via fax un elenco completo delle trasferte degli ultimi due mesi.

Avevamo ottenuto così sia una distribuzione statistica degli orari delle trasferte sia il nome dei geometri che le effettuavano. Passammo la settimana a cercare sui newsgroup i messaggi del reparto IT per fare il grabbing delle signature.

La settimana dopo mandammo un e-mail spoofata (con reply-to su un indirizzo creato ad hoc su yahoo) da parte di uno dei membri del reparto IT a tutti i geometri chiedendo di fornirci, per "implementazione di un nuovo sistema di sicurezza", username e password attuali. Ricevemmo i dati di tutte le persone a cui avevamo mandato la mail.

Con quelle ci collegammo al RAS durante dei periodi concidenti a quelli in cui i geometri uscivano e riuscimmo a fare un hack del file server principale bypassando il firewall aziendale.

6.3 Uno cattivissimo Worm

Durante un secondo pen-test, scoprimmo che i dipendenti, attraverso un sondaggio sugli utenti, potevano solamente utilizzare la posta elettronica e il web. Da un secondo sondaggio scoprimmo che il collegamento funzionava attraverso PAT ma che non era presente alcun proxy server. Scoprimmo inoltre che l'antivirus utilizzato era il Norton.

Osservammo l'edificio per un paio di giorni e scoprimmo così che la segretaria del direttore dell'ufficio si fermava fino a oltre le 18 molto spesso. Con un sucker facemmo il grabbing di alcune pagine del sito della Symantec e creammo un sito apposito con un annuncio fasullo su un nuovo tipo di Worm e relativo download di un programma di controllo.

Telefonammo al centralino e ci facemmo passare la segretaria. Le spiegammo che eravamo un sistemista di un altro ufficio collegato e che da un paio di giorni avevamo ricevuto una serie di mail contenenti il nuovo worm e provenienti specialmente dal suo computer. La segretaria andò nel pallone. La rassicurammo e la facemmo andare con il proprio browser sul sito fake e le facemmo fare il download del programma di controllo (un semplice netcat configurato con uno script per connettersi alla porta 80 di un server esterno dove ascoltava il listener e restituire una shell). Le facemmo lanciare lo script e le dicemmo di "lasciare il computer acceso tutta la notte così che potesse verificare che il worm non reinfettasse la macchina". Inoltre fummo così cortesi da dirle "che avremmo avvisato noi Mario Rossi (il sistemista dell'ufficio)" il giorno dopo.

Con il tunnel creato e una shell aperta effettuammo il nostro pen test con successo durante la notte.

6.4 La Biblioteca

Dal sito web dell'ufficio pubblico scoprimmo che l'ufficio in questione possedeva una biblioteca giuridica all'ultimo piano, aperta agli studenti di giurisprudenza dell'università.

Telefonammo al geometra dell'ufficio e, spacciandoci per un altro geometra di un ufficio vicino, chiedemmo il nome dell'azienda che aveva realizzato il cablaggio di rete, con la scusa di dover fare lo stesso lavoro.

Chiamammo la ditta in questione spacciandoci per il geometra con cui avevamo appena parlato e chiedemmo se fosse stato possibile ottenere copia dei progetti del cablaggio. Passammo a prenderli il giorno dopo e questi ci confermarono che in biblioteca erano presenti due connettori RJ-45 collegati alla rete aziendale.

Preparammo un libretto universitario con photoshop, ci presentammo all'usciere, salimmo in biblioteca, collegammo un portatile e trovammo che entrambi i connettori erano collegati agli switch. In un'ora il pen-test era concluso.

6.5 Virtual Public (?!?) Network

Penetration test in una filiale di una nota azienda meccanica. Chiamammo spacciandoci per una azienda di job-hunting e chiedemmo ad uno dei sistemisti del reparto IT se aveva esperienze con le VPN. Rispose in maniera affermativa ma fu così sincero da confermarci che nella ditta dove lavorava ora avevano comprato una soluzione da un noto operatore ex monopolista italiano ;-P.

Dalla descrizione capimmo che il sistema era più un Virtual PUBLIC Network, dato che era gestita in toto da dei router CISCO 2600 e non era nulla in più di un tunnel ip-over-ip, ovviamente non crittato.

Ottimo, conoscendo la configurazione, entrare da quella porta sarebbe stato semplice. Chiamammo così il call center del noto operatore.

Spiegammo alla gentile operatrice che necessitavamo della configurazione del router del centro stella per poter implementare una soluzione di back-up nel caso si fosse rotto il router in comodato. La signorina ci chiese subito la TGU della linea su cui si attestavano le VPN.

"... TGU? Ve la direi volentieri se il vostro tecnico non fosse stato così un genio da scriverla sull'etichetta posta di fronte alla finestra e che il sole ha scolorito!!"

La signorina si fece due risate, ci chiese il nome della società, l'indirizzo, e il nostro nome (ovviamente coincidente con quello del tecnico intervistato precedentemente). Trovò la linea, ci fornì la TGU ("Così ve la potete segnare per le prossime chiamate") e aprì il ticket. Il giorno dopo ci chiamò il tecnico, a dire il vero un po' seccato dato che era reticente a fornire la configurazione del loro router. Gli spiegammo che oramai sulla VPN transitavano dati talmente importanti che non potevamo permetterci un down maggiore di due ore e quindi necessitavano di una "soluzione tampone" nell'attesa di un loro intervento. Gli spiegammo che comunque gli avremmo mandato subito una richiesta via fax, cosa che facemmo prontamente, utilizzando una carta intestata falsificata. Ottenemmo alla fine la configurazione necessaria, la esaminammo e capimmo come intervenire. Seguì l'hack del router e, una volta intercettato e deviato il flusso attraverso la nostra rete, intervenimmo e concludemmo velocemente il pen-test.

6.6 Maledetto firewall

Una società informatica ci assunse per controllare il livello di security della propria rete. Prendemmo le nostre informazioni presso la camera di commercio e scoprimmo che la società si era ripresa da una piccola crisi finanziaria. Controllammo la registrazione del dominio e controllammo presso il centralino se il contatto tecnico fosse ancora assunto presso la società. La risposta fu negativa e quindi chiamammo il sostituto, spacciandoci per il RIPE e inventandoci un problema per il rinnovo del dominio. Il sostituto si rivelò un assunto alla seconda esperienza di lavoro (guarda caso). Ci fornì tutti i dati necessari.
Con la sua e-mail facemmo una ricerca su google e scoprimmo che il tizio in questione aveva chiesto a più riprese aiuto su un newsgroup riguardo al firewall aziendale dato che lui "non era pratico con quella architettura".

Tentammo un nuovo approccio. Comprammo un cellulare e affittammo una casella postale presso un ufficio postale. Creammo una carta intestata ad hoc e mandammo una bella lettera vergata in carta pregiata pubblicizzando una nuova azienda specializzata nell'assistenza su una serie di firewall commerciali tra i quali, guarda caso, quello dell'azienda in questione.

Lasciammo passare qualche giorno e cominciammo a lanciare una serie di Denial of Service verso il firewall. Dopo due giorni di "casini" squillò il nuovo cellulare :-D
Mandammo uno dei nostri a "fissare il problema" e, che cattivi, ad installare una backdoor sul firewall. Pen test finito....

6.7 Grafica 3D...

Eravamo in crisi nera. Dipendenti preparati, firewall ben chiuso, server web sistemati perfettamente, tizio alla portineria simile ad un Cerbero con l'emicrania.

Dopo due settimane di ricerche scoprimmo però che uno dei dipendenti del reparto di spedizioni aveva la segreta passione per la grafica 3D e certamente era un esperto in materia.

Riesumammo una vecchia copia di SolidThinking (sempre un programma divino) comprato ai tempi dell'università e cominciammo a contattare il tipo alla ricerca di consigli. Dopo qualche settimana di "corso online" e dopo aver comprato un paio di libri sull'argomento, preparammo un tutorial per principianti e chiedemmo al tipo se fosse stato così gentile da correggerci gli svarioni più grossi... benedetti oggetti embedded e macro di word. Gli mandammo nel documento un tunnel su http e creammo una macro per copiarlo, configurarlo e lanciarlo dalla sua macchina.

Entrati.

CAPITOLO 7

7.1 Conclusioni

Ciò che maggiormente ci auguriamo è di avervi fornito uno strumento che vi possa far capire le potenzialità della social engineering. Sia dagli hacker sia dagli esperti di sicurezza è una tecnica che troppo spesso viene sottovalutata o dimenticata e, specialmente per coloro che devono occuparsi della sicurezza di un sistema informativo, è una mancanza particolarmente grave dato che tramite questa è possibile ottenere informazioni vitali e ridurre drasticamente i tempi di un attacco informatico.

Questo potrebbe essere davvero un problema...