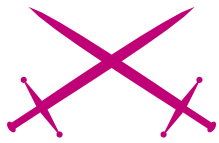



Social engineering



Attacco

Pierpaolo Palazzoli, Matteo Valenza 

Grado di difficoltà



Le tecniche di attacco oggi a disposizione sono innumerevoli e molto complesse. Generalmente sempre legate alle imperfezioni dei software. Come tutti sanno i programmi sono scritti dall'uomo e l'errore è intrinseco nella natura dell'uomo stesso, quindi viene da se la conclusione.

Esattamente come nei software anche nei comportamenti, reazioni, comunicazioni l'uomo è imperfetto, quindi vulnerabile. La natura fisiologica ci rende condizionabili da migliaia di agenti esterni e interni, come cambi climatici, emozioni e malattie. Questa componente ci rende condizionabili, assecondabili e scontrosi....

Il ragionamento quindi ci porta a considerare che a capo dei sistemi, software e programmi c'è la figura umana in tutte le sue sfaccettature e vulnerabilità.

Le tecniche finalizzate allo sfruttamento delle vulnerabilità sociali/umane si chiama Social engineering. La finalità di questo metodo è lo studio del comportamento individuale di una persona ai fini di carpirne delle informazioni o condizionarla a fare delle azioni.

Un'altro motivo che ha spinto l'hacking a spostarsi su queste tipologie di tecniche di attacco è l'aumento di sistemi di sicurezza evoluti.

Le basi fondamentali di questo metodo sono le stesse che si trovano alla base della comunicazione sociale. Quindi comunicazione verbale e non verbale. Tipicamente quelli tecnologici sono mezzi di comunicazione verbale, dove le parole sono alla base della comuni-

cazione. Esistono anche la sotto distinzione tra comunicazione scritta e comunicazione vocale. Tipicamente chat, blog da una parte e telefono voip dall'altra. Per quanto riguarda la comunicazione non verbale si intende tutto quello che è espressione umana in una comunicazione: gesticolare, espressioni visive, sguardi, contatto, ecc.

La distinzione di questi concetti servirà per chiarire i prerequisiti di un social engineering.

Molto probabilmente il social engineering è sempre esistito all'interno della società, ma non

Dall'articolo imparerai...

- A comportarti in contesti professionali come utente,
- Tecniche di raggio,
- Metodologia di approccio sociale.

Cosa dovresti sapere...

- Sistemi di assistenza telefonica ed helpdesk,
- Tipologie di problematiche IT,
- Focalizzazione degli obiettivi,
- Capacità di improvvisazione.

aveva mai focalizzato la sua attività sul furto di informazioni finalizzate a crimini informatici.

La figura della persona astuta, è sempre esistita facendo anche la storia di intere popolazioni. Le capacità comunicative in molti casi sono in grado di supplire enormi lacune nelle argomentazioni trattate.

Tutti questi concetti/comportamenti fanno parte del quotidiano di ognuno di noi, molte volte pensare a questi argomenti ci permette di focalizzare gli obiettivi e quindi agire di conseguenza.

Introduzione e contesti sociali

L'inventore di questo metodo di attacco è senza dubbio Kevin Mitnick, e la base di questa tecnica è di sicuro lo spionaggio. Mitnick ha strutturato un metodo di social engineering basandosi su un contesto sociale/culturale americano. Questo particolare non è indifferente, perché il contesto socioculturale europeo è completamente diverso. Partendo dal presupposto che l'Europa ha una storia molto più complessa, la popolazione ha maturato una coscienza storica differente. Il territorio europeo è altamente eterogeneo come religioni, nazioni, lingue e culture, questo porta prima di tutto ad incomprensioni legate a modi di dire, di fare, lingua, esternazione delle emozioni e tutte quelle componenti che caratterizzano la popolazione. Il livello di fiducia tra le persone è molto più basso rispetto a quello americano. Tutte queste componenti non rendono trasportabile completamente il modello di social engineering americano.

Alcune tecniche si potrebbero usare, altre invece darebbero di sicuro risultati negativi. Un esempio di non applicabilità, raccontato da Mitnick, è quello che racconta di se stesso, grazie ad una penna regalata ad un bigliettaio di treni, ottiene la password utente sul sistema di bigliettazione. Penso che questo tipo di attività non sia applicabile in un contesto europeo. Una tecnica applicabile invece, ma assolutamente

non banale, è spacciarsi per un'altra persona.

Prerequisiti

Come nelle tecniche di hacking su servizi di rete, anche il social engineering pretende dei prerequisiti. Questi sono da una parte tecnici: dotazioni hardware e software, ma soprattutto sociali, legati al carattere, il modo di parlare, la facilità di espressione, la capacità di leggere le risposte codificate nella comunicazione non verbale dell'interlocutore. L'aspetto fisico e la portanza sono fondamentali nel caso di comunicazione faccia a faccia. Il carattere del social engineer deve essere estremamente aperto, tollerante, forte. La capacità di mentire è fondamentale, anche il controllo delle emozioni è una condizione necessaria.

Dal punto di vista comunicativo, è necessaria una buona capacità di intrattenimento, una giusta dose di interventi all'interno di una discussione. Frasi grammaticalmente corrette, concetti semplici ma focali.

Un'aspetto difficilmente catalogabile è la capacità di percepire le emozioni rilasciate dalla persona con la quale si parla. In molti casi parlare degli argomenti più cari all'interlocutore permette di ottenere il massimo risultato.

Se la finalità è l'accesso ad un sistema, il giusto punto di partenza è colui che lo gestisce, in questi casi è necessario capire l'interlocutore come creatore e capo indiscusso di quel sistema, tentando di ottenere informazioni complimentandosi sull'operato. Non bisogna assolutamente innescare competizioni di conoscenza, perché siamo noi a voler ottenere informazioni.

Le capacità da sviluppare, molto difficili, sono le metodologie di convincimento. Di difficile applicazione queste tecniche devono essere ponderate, in caso contrario si risulterà troppo opprimenti. Al contrario assecondando continuamente l'interlocutore si arriverà ad essere considerati senza carattere.

Il giusto equilibrio di tutti questi (e molti altri non citati) prerequisiti sono

necessari se si vuole intraprendere la strada dell'attacco sociale.

La finalità del social engineering è di sicuro quella tecnica, ma non dimentichiamoci che è utilizzabile per qualsiasi finalità. Di sicuro il social engineering è sempre esistito come base di corteggiamenti, rapporti di affari, rapporti gerarchici...

Analisi degli obiettivi

Come in tutti gli attacchi che si rispettano, esiste un piano su cui basarsi. Il piano è dettato dall'obiettivo. L'obiettivo può essere cambiato durante l'attacco ma tenendo sempre conto del rischio che si sta correndo.

Quando si da una finalità ad una attività, questa diventa il traguardo da raggiungere, ci permette di mantenere costante e focalizzato l'obiettivo. Gli obiettivi sono sempre delle persone, è la base del social engineering ed è molto differente se queste rappresentino una società o se stesse.

Le differenze sostanziali si trovano negli individui che rappresentano una società, tipicamente dipendenti. Alla base del loro comportamento professionale esistono motivazioni lavorative, mansione coperta, numero di anni di operatività in quel contesto. Nelle aziende di grandi dimensioni, i sistemi di controllo sono spesso inefficienti, quindi le politiche di pareggiamento degli stipendi porta ad un malcontento generale. Unito al trattamento delle persone come numero, non valorizzando meriti e capacità.

Per quanto riguarda la persona che rappresenta se stessa e i propri interessi è molto più complesso, dato che questo individuo tutela la propria proprietà, quindi la sua posizione sarà estremamente diffidente, per poter fare breccia in questo caso è necessario definire socialmente la sua posizione di superiorità e potere. Successivamente tentare di addentrarsi nelle argomentazioni di maggiore interesse per l'interlocutore tipicamente hobby.

Creare degli schemi predefiniti non è sempre vincente, ma analizza-



re i comportamenti e schematizzare la personalità a volte lo è.

Preparazione

La preparazione del campo in gergo tecnico viene chiamata footprinting. È il tentativo, tramite mezzi tecnologici, di ottenere il maggior numero di informazioni sull'obiettivo.

L'obiettivo come abbiamo detto, è una organizzazione o persona, la conoscenza del nome di tale società/persona, è banale dirlo, ma è necessaria.

La capacità necessaria qui è l'uso avanzato di strumenti per le query sui database quali: motori di ricerca, enti per la registrazione dei domini, enti per la registrazione degli indirizzi ip, elenchi telefonici online, portali socialnet (tipicamente per persone fisiche).

Prima di tutto inserire il nome della società in un motore di ricerca per ottenere le info riguardanti: recapito telefonico, call center, numero reclami e struttura organizzativa quali (nomi dei manager).

Ottenuti i nomi dominio è necessario identificare tramite il comando whois, l'Admin Contact e la *Technical Contacts*. Questi tipicamente sono l'amministratore delegato e il secondo è lo staff tecnico. Da qui otteniamo l'indirizzo della sede amministrativa e la scadenza del dominio (data molto utile).

Risolvendo il dominio otterremo l'indirizzo ip, dove è hostato, il sito/posta, informazioni fondamentali, gli indirizzi mail di segnalazione pubblicati, responsabili degli ip e i soliti dati: indirizzo, città, ecc.

Da questa prima analisi dovremmo ottenere le informazioni necessarie per iniziare a contattare l'obiettivo.

Gli elenchi telefonici on-line possono avvalorare o completare i dati ricavati precedentemente, nell'eventualità avessimo anche dei nominativi specifici, si potrebbe tentare la ricerca nelle socialnet di qualche blog, sito personale, utilissimi per conoscere gli interessi degli individui.

Lo strumento e-mail è molto potente e dinamico, basti pensare

che è possibile falsificare la propria provenienza (spoofing del mittente), tentare di rubare informazioni (phishing), o semplicemente farsi conoscere.

Ricognizione e Attacco

La prima fase dell'attacco consiste nella ricognizione che anticipa immediatamente l'attacco. Questa fase richiede uno spostamento fisico verso il target. Le informazioni di localizzazione sono già in possesso. Ormai la maggior parte delle aziende/privati possiede connettività wireless, quindi è consigliabile setacciare la zona dell'azienda obiettivo e controllare l'eventuale presenza di access point. È risaputo che le chiavi wep sono craccabili, il wpa-psk è già più difficoltoso. Nella maggior parte dei casi le reti sono aperte. Se l'access point fosse direttamente interconnesso alla rete interna avremmo accessibilità a tutte le informazioni necessarie per potere combinare azioni di social engineering. Nel caso la finalità fosse l'accesso alla rete, saremmo arrivati al risultato. Comunque l'accesso alla rete non garantisce la conoscenza di password, sistemi, reti ed interconnessioni.

Le fasi di ricognizione più strutturate sul social engineer sono di sicuro al chiamata telefonica e il contatto faccia a faccia.

Nella maggior parte delle aziende che offrono servizi esistono i call center. Tipicamente sono luoghi degradati sia dal punto lavorativo che sociale. Sono posti di passaggio, lavori momentanei (interinali).

Il profilo professionale è tipicamente basso, bassa considerazione del lavoro, sfruttamento e quindi luogo propizio per ottenere informazione e pieno di vulnerabilità. Bisogna aggiungere che fino ad ora solo alcuni call center hanno sistemi di autenticazione (*user* e *password*). La maggior parte delle aziende di servizi hanno il codice cliente, che in taluni casi, è bypassabile tramite alterazione della voce e necessità di intervento immediato. Esistono aziende che addirittura si affidano

alla buona fede dell'utente che deve dichiarare, se il telefono non fosse quello su quale vuole avere assistenza, il numero sul quale vuole per esempio cambiare il piano tariffario o togliere e aggiungere i servizi.

Qualche telefonata potrebbe essere necessaria, segnandosi nomi degli operatori. La chiamata deve accompagnare o un guasto o un reclamo, e se è possibile, tentare di scalare ad un livello di assistenza superiore, gestore di un numero maggiore di risorse e quindi maggiori informazioni. Esistono numeri raggiungibili dall'esterno. Tipicamente i centralini collegati a linee primarie hanno una numerazione principale (prima parte) e il numero di interno (seconda parte). Fare delle telefonate su interni casuali sarebbe utile se eventualmente, grazie alla raccolta dei nominativi, si avesse l'interno diretto di qualche responsabile/capo, di modo da potersi far conoscere (sotto falsa copertura).

Questi contatti telefonici devono essere documentati e finalizzati a loro volta ad affinare le informazioni collezionate. Sapere che standard ha la creazione delle mail aziendale per esempio è un'ottima informazione, per esempio *nome.cognome@dominio.xx* oppure *cognome@dominio* e così via.

Facendo esempi potremmo impersonificarci o in un fornitore o in un cliente. Questi due metodi sono differenti ma entrambi efficaci. Se si vuole colpire una persona prendiamo la sua identità, nel caso dell'azienda diventiamo fornitore.

Con le informazioni ottenute sino ad ora è possibile tentare di prendere appuntamento per una visita durante la quale, preparandoci adeguatamente, si proporranno dei servizi/dispositivi del tutto inerenti al business dell'azienda stessa. Non capita mai che il contatto interno controlli la veridicità del commerciale/venditore.

I sistemi di sicurezza fisici delle aziende richiedono: dichiarazione di nome e cognome, biglietto da visita

(riproducibile), firma, e tesserino temporaneo consegnato.

Le videocamere sono ormai presenti in tutte le strutture, l'uso di un cappello potrebbe essere una buona scelta. Tutte queste soluzioni devono essere pianificate precedentemente. Una volta entrato in un'azienda abbiamo a disposizione un numero altissimo di attività:

- Collegamento alla rete interna (*sniffing*),
- Inserimento di un access point,
- Creare disservizi per avere un diversivo (sistemi anticendi ecc).

Una volta a contatto con la parte aziendale con la quale avete preso l'appuntamento, dopo aver sostenuto discorsi attinenti, bisogna con fare sicuro chiedere accesso alla rete per scaricare la posta o meglio, ad una domanda specifica chiedete di poter consultare in vpn le risorse in ufficio. All'atto di connessione alla lan potrebbe essere necessario avere a disposizione gli script già pronti per arp poisoning e sniffing, nonché enumerazione delle porte aperte, una sorta di sonda. Di fondamentale importanza è l'aspetto formale (vestiario e cura della persona).

Per quanto riguarda una persona fisica, sono più efficaci gli attacchi indiretti. Quindi tentare di modificare, contratti di servizi spacciandosi per la persona che si vuole attaccare. La

localizzazione fisica dell'abitazione è un possibile accesso tramite wireless insicure o non protette. Il furto di identità applicabile con phishing, oppure le telefonate, spacciandosi per l'operatore di servizi di telecomunicazioni, facendo fare test e facendosi comunicare i piani di indirizzamento pubblici in quel momento assegnati. La capacità di combinare qualità discorsive a quelle tecniche possono dare i risultati attesi. Conoscere le tecnologie utilizzate dai vari operatori permettono di focalizzare le domande e capire meglio le risposte.

La sezione di ricognizione è fondamentale ai fini del risultato ma potrebbe essere molto lunga, la capacità di relazionarsi risulta fondamentale ai fini di non farsi mai scoprire.

Persuasione

La fase di persuasione è sia all'interno della fase di ricognizione che di attacco, infatti è possibile che le domande che ponete non abbiano delle risposte dirette oppure nei momenti di difficoltà potrebbe essere un buon diversivo.

Le tecniche di persuasione sono innumerevoli, ma la legge di base è dare la sensazione di essere fortemente sicuri di se e in grado di dimostrare ciò che si racconta. Il condizionamento non deve essere mai diretto, perché tipicamente

quando c'è diffidenza ogni costrizione potrebbe essere dannosa. L'obiettivo è di tentare di condizionare una scelta di modo che si abbia deciso il percorso ma che l'interlocutore pensa di avere lui stesso intrapreso.

Persuadere una persona significa tentare di entrare in sintonia con lei, quindi ascoltarla e rispondere quello che lei si attende, nello stesso tempo avvicinarsi ad argomenti e concetti focali per il nostro obiettivo.

Conclusioni

Le conclusioni possono essere sia a favore che contro alla reale efficacia di questa tecnica. Il dato di fatto è che il social engineering non è assolutamente niente di nuovo, sono principi che regolamentano il quotidiano di molti ambienti professionali europei, l'unica differenza è nella finalità tecnologica. Questo non significa che non debba essere considerato pericoloso, ma di sicuro è l'ultima fase di messa in sicurezza per una azienda.

Infatti la sua nascita è giustificata da sistemi di sicurezza evoluti (ids, ips, firewall layer7). L'applicazione maggiore in questo momento di tecniche di questo tipo è il phishing, perché applicabile ad un modello massivo.

In prima fase vale la pena di risolvere i problemi reali di sicurezza e poi pensare alle filosofie di comportamento. ●

In Rete

- [http://en.wikipedia.org/wiki/Social_engineering_\(computer_security\)](http://en.wikipedia.org/wiki/Social_engineering_(computer_security)) – WIKIPEDIA,
- <http://www.securityfocus.com/infocus/1527> – Securityfocus,
- <http://www.mitnicksecurity.com/> - Sito di riferimento di Kevin Mitnick.

Cenni sugli autori

Snortattack.org, Portale orientato alla sicurezza, è il risultato della fusione di conoscenze e collaborazione del team. Le tipologie di argomenti trattati spaziano a 360 gradi su tutti gli ambiti di sicurezza: attacco/difesa.

Grande punto di forza è l'uso di Snort come soluzione alle innumerevoli problematiche di intrusione. Un forum e mailinglist che concorrono a tenere aggiornati gli utenti sulle nuove problematiche. Con Snortattack.org, il team, intende creare uno Snort User Group finalizzato alla collaborazione tra gli utenti di Snort dell'Italia e tutto il Mondo, e la missione di trattare le problematiche di sicurezza.