

Introduzione

Che cosa si intende con “hacking non tecnologico”?

Quando ho intrapreso questa attività, ero preparato al fatto che la curva di apprendimento sarebbe stata lunga e ripida. Ho trascorso molte notti insonni a elaborare worm nella mia rete domestica, tentando di partire dalle basi. Tutta questa pratica ha ripagato. Dopo anni di duro lavoro e studi intensi, ho fondato un piccolo, ma agguerrito, team di intrusione. Sono stato bravo, il mio spirito è stato forte. Le reti si prostravano davanti a me. I miei collaboratori contavano su di me e mi ero convinto di essere “quello giusto”. Poi ha incontrato Vince.

Con il suo aspetto di quarantenne, con l’occhio vigile e un’aria vagamente europea, Vince si è presentato con un abbigliamento classico: normalmente invece indossava un trench di pelle nera, una bella camicia, pantaloni scuri, scarpe nere e talvolta un cappello nero. Aveva decisamente un look affascinante. I racconti sui risultati che aveva conseguito erano leggendari. Alcuni dicono che sia stato un federale e che si occupasse di progetti segreti per il governo. Altri sostengono che sia stato un mercenario, intento a vendere i propri oscuri segreti al miglior offerente.

Certamente era brillante. Sapeva fare cose straordinarie e apparentemente impossibili. Sapeva aprire serrature, mettere in corto circuito sistemi elettronici, trarre informazioni dall’etere con qualche strano aggeggio elettronico. Un giorno mi ha mostrato un sistema da lui creato chiamato “van Eck” (http://en.wikipedia.org/wiki/Van_Eck_phreaking). Era in grado di assorbire le radiazioni elettromagnetiche prodotte da un monitor a tubo catodico e riassemblarle, consentendogli di leggere il contenuto di un monitor a mezzo chilometro di distanza. Mi ha insegnato che una TV in bianco e nero può essere utilizzata per spiare le conversazioni dei telefoni cellulari sui 900 MHz. Mi ricordo ancora di come, curvo su un tavolo della mia cantina, alimentava il tuner UHF di un vecchio TV in bianco e nero con una coppia di sottili pinze. Quando ho sentito una conversazione telefonica provenire dalle casse del vecchio TV, ho deciso che avrei dovuto apprendere il più possibile da Vince.

Ero incredibilmente intimidito alla nostra prima impresa insieme. Fortunatamente avevamo compiti differenti. Dovevo svolgere una valutazione interna, che simulava un’intrusione. Un dipendente maldestro può causare innumerevoli danni a una rete. Per perfezionare la simulazione, il cliente ci ha fornito uno spazio di lavoro, una connessione

di rete e il nome-utente e la password di un utente legittimo, ma non amministrativo. Ero incaricato di sfruttare queste credenziali per ottenere il controllo amministrativo dei sistemi critici della rete. Per esempio, se riuscivo a ottenere l'accesso ai record riservati conservati nel database aziendale, il tentativo poteva ritenersi concluso con successo. Vantavo un record quasi perfetto in tema di valutazione della sicurezza interna ed ero fiducioso delle mie capacità.

Vince doveva svolgere una valutazione fisica che simulava una minaccia esterna. La sede vantava una sicurezza fisica di alto livello. Avevano speso un sacco di soldi in serrature, sensori e apparecchi di sorveglianza. Sapevo che Vince li avrebbe aggirati con i suoi superpoteri ipertecnologici. L'incarico sembrava essere alla nostra portata, con lui che si occupava della sicurezza fisica e io che lavoravo dall'interno. Eravamo un "dream-team" della sicurezza.

Quando Vince ha insistito perché lo aiutassi nella parte fisica di questa valutazione non stavo nella pelle. Mi immaginavo in un film di 007, con Vince nei panni di "Q" e me stesso (naturalmente) in quelli di James Bond in una tuta da assalto ninja. Vince avrebbe fornito tutto il necessario, come il van Eck, e io mi sarei infiltrato nel perimetro e avrei spiato i monitor di sorveglianza o qualcosa del genere. Mi immaginavo le tecniche straordinarie che avremmo impiegato per aggirare i sistemi a tastiera elettronica o le chiusure a prossimità. Mi immaginavo lo sguardo delle guardie, mentre li legavamo con il nastro adesivo alle loro poltroncine, dopo esserci calati silenziosamente dal soffitto della sala di sorveglianza.

Non vedevo l'ora di iniziare. Ho detto a Vince di mostrarmi gli strani gadget che avremmo utilizzato per infrangere la sicurezza. Quando mi ha detto che non aveva alcun gadget con sé, mi sono messo a ridere e non ci credevo. Non sapevo che Vince fosse un burlesco. Quando mi ha ripetuto che veramente non aveva portato nulla, per un attimo ho pensato di rompergli il muso, ma avevo sentito dire che era cintura nera in sei diverse arti marziali e quindi gli ho chiesto gentilmente cosa diavolo aveva in mente. Disse che avremo agito in modo creativo. Un genio mercenario, una leggenda vivente e non aveva portato nulla? Gli ho chiesto come poteva sperare di attaccare un edificio ad alta sicurezza senza nulla in mano tranne la creatività. Mi ha risposto guardandomi con un ghigno, che non ho mai dimenticato.

Abbiamo passato l'intera mattina semplicemente a controllare il sito. Era costituito da svariati edifici di più piani, con alcuni parcheggi per i dipendenti, il tutto racchiuso da una cancellata. Ogni movimento doveva svolgersi dal cancello principale. Fortunatamente il cancello era aperto e senza guardie. Vince guidava e abbiamo girato attorno a un edificio e parcheggiato sul retro, dove si potevano osservare i banchi di carico.

"Là", mi ha detto.

"Dove?", gli ho domandato.

"Là", ha ripetuto.

Vince ha un pessimo senso dell'umorismo. Ho seguito il dito e ho visto il piano di carico. Appena dietro i portoni, c'erano vari operai intenti a maneggiare grossi pacchi.

"Il piano di carico?", ho chiesto.

"Entrerai da lì".

Ho risposto con un "See...".

"Esattamente. È facile!", mi ha risposto.

“Non ho detto ‘Seee...’ per dire che è facile. Intendevo dire: con tutta quella gente, come posso entrare?”.

“Ci sono loro e ci sarai anche tu”, mi ha risposto. Vince ha proseguito in questo modo. “Comportati con naturalezza. Saluta gli altri. Sii amichevole. Fai commenti sul tempo”.

Ho fatto tutto quello che mi ha detto ed effettivamente mi sono trovato all’interno. Ho passeggiato qua e là, ho preso alcuni progetti di veicoli corazzati e altra roba militare, li ho fotocopiati e me ne sono andato. Tutto qui. Evito naturalmente di descrivere il mio cuore che batteva all’impazzata, il pensiero della prigionia militare in cui mi avrebbero sbattuto e se era vero tutto quello che si racconta sulle attenzioni dei compagni di cella, ma ce l’ho fatta. Ed è stata un’avventura incredibile. Era la forma più semplice di ingegneria sociale, ma aveva funzionato a meraviglia. Nessuno mi ha mai domandato nulla. Probabilmente era semplicemente fuori dai loro normali schemi mentali. Non riesco a celare il mio ghigno mentre tornavo alla macchina. Ma Vince non c’era più.

È uscito dall’edificio qualche minuto più tardi, con una piccola pila di fogli.

“Come ci sei riuscito?”, gli ho chiesto.

“Come hai fatto tu!”.

“Allora perché non hai fatto tutto da solo?”, gli ho chiesto.

“Volevo essere sicuro che funzionasse”.

Bene, ero stato la cavia da laboratorio di Vince, ma in realtà non mi importava molto. Era stato emozionante ed ero pronto per proseguire.

L’altro edificio che abbiamo preso di mira sembrava una vera e propria fortezza. Non c’erano piani di carico e l’unico ingresso visibile era quello frontale. Il portone era di legno e acciaio (sembrava quasi il portone di un castello) e aveva uno spessore approssimativo di 15 centimetri, con un lettore di tesserini a prossimità. Abbiamo osservato i dipendenti che gli sventolavano davanti il tesserino, al che il portone si apriva e permetteva l’ingresso. Ho suggerito la tecnica del tailgating. Ormai ero lanciato. Ma Vince ha scosso la testa. Ovviamente aveva in mente qualche altra idea. Ha camminato verso l’edificio e poi ha rallentato mentre si avvicinava al portone. A un paio di metri si è fermato. L’ho oltrepassato e mi sono voltato verso di lui; le spalle al portone.

“Bello il tempo”, ha detto, osservando il portone dietro le mie spalle.

“Eh già”, gli ho risposto.

“Una buona giornata per l’arrampicata”.

Mi sono messo a girare attorno all’edificio. Non avevo considerato la possibilità di arrampicarsi.

“No”, mi disse “Non andare in giro. Parliamo”.

“Parliamo?”, gli ho chiesto. “E di che cosa?”.

“Hai visto i Bears ieri sera?”, mi ha chiesto. Non avevo alcuna idea di cosa stesse dicendo o di cosa fossero i Bears, ma lui ha proseguito. “C’è qualcosa di speciale. Il modo in cui collaborano i giocatori di una squadra è quasi come se...”, Vince si è interrotto senza concludere la frase, mentre si apriva il portone; un impiegato l’ha aperto e poi si è diretto verso il parcheggio “... come se tutti formassero un’unica unità”, ha proseguito. Non capivo niente. Mi sono voltato. Il portone si era quasi chiuso.

“Accidenti!”, ho detto, “Avremmo potuto entrare!”.

“Sì, qui ci vuole un appendiabiti”.

Vince, a volte, diceva cose strane. Era parte di lui. Ma non era un folle; semplicemente diceva cose che la maggior parte delle persone comuni non era in grado di comprendere. Cominciavo a pensare di aver assistito al suo primo momento di follia vera. “Andiamo”, ha detto. “Ho bisogno di uno straccio. Dobbiamo tornare in hotel”. Non avevo alcuna idea del motivo per cui avesse bisogno di uno straccio, ma almeno non mi sentivo in pericolo. Avevo sentito parlare di persone fatte a pezzi con un’ascia, ma mai con uno straccio.

Siamo rientrati in hotel in perfetto silenzio; Vince sembrava assorto nei suoi pensieri. Arrivato davanti all’hotel, ha parcheggiato e mi ha chiesto di aspettarlo. È tornato qualche minuto dopo con un appendiabiti in filo di ferro e uno straccio per pavimenti umido. Li ha gettati sui sedili posteriori. “Dovrebbe funzionare”, disse, sedendosi e chiudendo la portiera. Avevo paura di porre domande. Mentre lasciavamo l’hotel, mormorava “Con questi dovrei farcela”.

Gli ho lanciato un’occhiata. Non so dire esattamente che tipo di occhiata fosse, ma immagino fosse una via di mezzo fra “Ho avuto uno sgradevole incontro olfattivo” e “C’è qualcosa che non va nella tua testa”. In ogni caso, ero abbastanza convinto che avesse perso il senno o che fosse stato rapito dagli alieni. Ho fatto finta di non averlo sentito, ma lui ha proseguito.

“Ogni edificio deve avere delle uscite. Le leggi federali impongono che in caso di emergenza, le porte debbano aprirsi dall’interno senza che l’utente conosca qualcosa del loro funzionamento”. Ho gettato uno sguardo al cielo dal parabrezza. Pensavo che gli alieni, la prossima volta, sarebbero venuti per me. “Inoltre, l’uscita non deve prevedere l’impiego di chiavi o altri oggetti particolari. Le porte di uscita devono essere molto facili da utilizzare”.

“Questo ha *qualcosa* a che fare con il portone che abbiamo osservato, giusto?”, gli ho chiesto. Le mie parole mi hanno preoccupato. Vince e io eravamo ormai sulla stessa frequenza operativa.

Mi ha guardato e a questo punto ho scoperto quale doveva essere il mio sguardo. Istantaneamente ho cercato di cacciar via dalla testa questi folli pensieri. “Questo ha *tutto* a che fare con quella porta”, ha detto, osservando fuori dal parabrezza e svoltando a sinistra. Eravamo arrivati a destinazione. “Il portone di questo edificio”, ha proseguito, “è formidabile. Usa un sistema a cilindri magnetici ad alta resistenza. Probabilmente è in grado di resistere all’impatto di un veicolo a 60 km/h. Le porte sono molto spesse, probabilmente corazzate e il sistema a prossimità è costoso”.

Non sono riuscito a resistere: “Ma noi abbiamo uno straccio per i pavimenti”.

“Esattamente. Hai notato il meccanismo di uscita?”.

No, non lo avevo notato e non potevo certo bluffare. “No”, ho ammesso.

“Devi sempre notare tutto”, mi rispose, fermandosi per fissarmi. Ho annuito e lui ha proseguito. “Il meccanismo di uscita è una barra di metallo più o meno all’altezza della cintola”.

Ho detto “Ah, sì, una barra a pressione”. Il termine sembrava sufficientemente tecnico. “No, non è una barra a pressione”. Ok, ho sbagliato. “La barra di quella porta è sensibile al tocco. Non funziona a pressione: si apre quando viene toccata. Molto comoda in caso di incendi”. Siamo entrati dal cancello e abbiamo parcheggiato. Vince è sceso e ha preso l’appendiabiti e lo straccio per i pavimenti dal sedile posteriore. Aveva allungato completamente l’appendiabiti, creando un lungo pezzo di filo di ferro, sottile ma resistente.

L'ha piegato a metà, ha disposto lo straccio dei pavimenti a un'estremità e gli ha girato il filo dell'appendiabiti; poi ha piegato il tutto per formare una curiosa bandiera piegata a 90 gradi. Ho pensato di non fare commenti sulla possibilità di arrendersi in questo modo alle guardie.

“Andiamo”, ha detto.

Ci siamo diretti al portone. Erano circa le sei del pomeriggio e in giro c'erano ormai pochi dipendenti. Si è diretto verso la porta, ha infilato l'estremità con lo straccio per i pavimenti fra le due porte all'altezza della cintola e ha iniziato ad agitarlo. Sentivo lo straccio che svolazzava dall'altro lato della porta. Pochi secondi dopo, ho sentito un clack, Vince ha aperto la porta ed è entrato. Ho fissato la porta mentre si richiudeva dietro di lui. La porta si riaprì e Vince mi domandò: “Non vieni?”.

L'incontro con il cliente è una cosa da raccontare. Dopo aver speso milioni di dollari per rendere sicuro l'edificio, avevano scoperto che l'intero sistema di sicurezza era stato sconfitto da uno straccio e da un appendiabiti, il tutto per una fessura fra le due porte. I dirigenti erano increduli e hanno richiesto una prova, che Vince ha accettato di fornire sotto forma di una visita in loco. Non so cosa sia accaduto dopo questa dimostrazione, ma non dimenticherò mai la lezione che ho appreso: le soluzioni più semplici sono spesso le più pratiche.

Certamente avremmo potuto lavorare sul sistema a prossimità, scoprire le tolleranze magnetiche della serratura o scalare le pareti e utilizzare la fiamma ossidrica, come nei film, per forare il soffitto, ma tutto ciò non è stato necessario. Questa è l'essenza dell'hacking non tecnologico. Sono necessarie conoscenze tecniche per ideare un attacco non tecnologico; tuttavia, queste conoscenze tecniche non sono necessarie per compierlo. Ancora peggio: nonostante la sua semplicità, un attacco non tecnologico è forse il più pericoloso e sottovalutato.

Nel corso degli anni, ho imparato a seguire i consigli di Vince. Ora noto tutto e tento di evitare i metodi troppo complessi. Non sono quasi mai fuori servizio. Sono costantemente impegnato a trovare nuovi vettori d'attacco, i più pericolosi dei quali possono essere svolti da chiunque.

La chiave dell'hacking non tecnologico

L'elemento chiave dell'hacking non tecnologico consiste nel pensare in modo semplice, essere vigili e viaggiare con gli occhi aperti e lo sguardo indagatore.

Per esempio, quando vado al supermercato o in qualche altra situazione socialmente ricca, osservo le persone. Per me gli estranei sono una sfida e cerco di scoprire di loro più che posso.

Quando incontro un uomo d'affari in aeroporto, la mia mente ingrana la quinta e cerca di scoprire il suo sedile e il suo status sociale; di dedurre i suoi problemi medici; di immaginare la sua situazione familiare (o di scoprire il suo orientamento sessuale); di valutare la sua situazione finanziaria, di stimare il suo reddito, di indovinare le sue abitudini alimentari e perfino il suo indirizzo.

Quando vado a un ristorante, ascolto le conversazioni che si svolgono attorno a me, traendo piccoli frammenti di informazioni. La mia attenzione vaga mentre analizzo i dintorni, tentando di scoprire quanto più possibile.