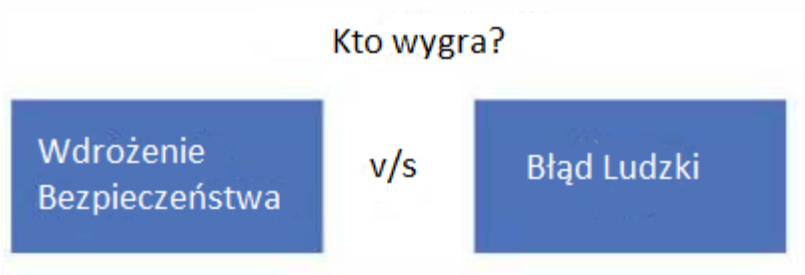
Wprowadzenie do inżynierii społecznej

W każdej bitwie nie ma lepszej wiedzy niż znajomość taktyki wroga. Ta część zapozna Cię ze światem inżynierii społecznej i przyjrzy się temu, na czym polega inżynieria społeczna. Inżynieria społeczna to zestaw technik, które są szeroko stosowane w cyberatakach do organizowania najbardziej udanych ataków. Inżynieria społeczna jednoznacznie atakuje słaby element łańcucha bezpieczeństwa cybernetycznego - użytkownika. W przeciwieństwie do systemów i sieci użytkownicy nie mogą być chronieni przed socjotechniką za pomocą drogich narzędzi, takich jak zapory ogniowe i programy antywirusowe. Zawsze są otwarci i zawsze przekazują informacje, które mogą zostać wykorzystane przez atakujących, aby trafić ich w najmniej oczekiwanym momencie. Ludzie mają również wyższy zwrot z inwestycji w porównaniu do systemów. W ciągu godziny ekspert inżynierii społecznej może zebrać tyle informacji, ile zajęłoby mu 100 godzin, próbując zaatakować bezpośrednio chroniony system. Atakujący zdają sobie sprawę z obecnego zaawansowania elementów bezpieczeństwa, które chronią systemy. Większość organizacji stosuje wiele warstw zabezpieczeń. Nawet jeśli jeden jest zagrożony, haker nie może łatwo ominąć innych. Dlatego trudniej jest próbować atakować same systemy. Jednocześnie hakerzy odkrywają, że łatwo jest zhackować dzisiejszych użytkowników, co zostało potwierdzone przez rosnącą liczbę mediowanych ataków socjotechnicznych. Ta część zawiera przegląd inżynierii społecznej.

Przegląd inżynierii społecznej

Jeden z największych cyberataków stulecia miał miejsce na Yahoo!, gdzie uważa się, że osoby atakujące mogły złamać jego systemy w 2014 roku i usunąć dane kont ponad 500 milionów użytkowników. FBI potwierdziło, że w ataku wykorzystano socjotechnikę, aby sprawić, by napastnicy przeszli kontrolę warstw po warstwie narzędzi bezpieczeństwa i systemów używanych do ochrony takich danych. Ten atak na Yahoo!, gigantyczną firmę technologiczną, potwierdza zatem, że inżynieria społeczna jest bardziej niebezpieczna niż się jej przypisuje. Nikt nie jest bezpieczny, jeśli jeden z najstarszych dostawców usług e-mail, który dużo inwestuje w narzędzia bezpieczeństwa cybernetycznego, może zostać łatwo złamany przy użyciu tej techniki. Rosyjscy hakerzy prawdopodobnie wykorzystali prosty e-mail phishingowy dla pracownika Yahoo, aby zhakować 500 milionów kont użytkowników. Inżynierowie społeczni byli również w stanie zarabiać ogromne sumy pieniędzy za pomocą prostych ataków socjotechnicznych. W 2015 roku firma o nazwie Ubiquiti Networks, która produkuje sprzęt sieciowy, została dotknięta techniką inżynierii społecznej. Atakujący byli w stanie zebrać informacje o CEO i skutecznie przejąć jego osobowość. Wykorzystali tę personifikację, aby skierować dział finansowy do kierowania ogromnych kwot pieniędzy do zagranicznej firmy, która poinformowała go o zmianie preferencji dotyczących płatności. Pracownik działu finansowego bez wątpienia przekazał pieniądze, aby później odkryć, że zamówienia nie pochodziły od prawdziwego dyrektora generalnego i że napastnicy zdążyli już zarobić miliony ciężko zarobionych pieniędzy organizacji. Dalsze dochodzenia ujawniły, że systemy bezpieczeństwa były nadal stosowane i nie były narażone na szwank, a kradzież nastąpiła jedynie w wyniku oszustwa z zakresu inżynierii społecznej. Oszuści oszukali tę firmę, aby przekazała 40 milionów dolarów Robertowi Hackettowi. Oba te incydenty podkreślają fakt, że ludzkiej słabości nie można lekceważyć w łańcuchu bezpieczeństwa cybernetycznego. Szybko staje się powszechnie stosowaną metodą atakowania organizacji:



Dzisiejsi cyberprzestępcy mają szczęście, ponieważ użytkownicy narażają się na ataki socjotechniki. Wzrost wykorzystania platform mediów społecznościowych był kluczowym czynnikiem przyczyniającym się do wzrostu liczby ataków z zakresu inżynierii społecznej. Wynika to z faktu, że dzisiejsi użytkownicy żyją w mediach społecznościowych i podają szczegółowe informacje na temat swojego codziennego życia, rodziny, miejsca pracy, osobistych preferencji itp., które mogą być wykorzystane do ataku inżynierii społecznej. Osoba atakująca musi tylko przejrzeć konta użytkownika w mediach społecznościowych, aby uzyskać wystarczającą ilość informacji, aby przeprowadzić udany atak inżynierii społecznej. Na Facebooku, Twitterze, Instagramie i Snapchacie jest więcej niż wystarczająca ilość informacji, aby inżynier społeczny mógł przyjąć osobowość większości użytkowników. Zaskakująco łatwo jest stworzyć fałszywe konto społecznościowe wyższego kierownictwa. Konto to zapewnia natychmiastowy szacunek i zgodność z wszelkimi zamówieniami wydawanymi do celu, a zatem może być wykorzystywane do robienia pieniędzy na młodszych pracownikach w organizacji. Inną metodą stosowaną w mediach społecznościowych jest tworzenie kont honeypot nieistniejących ludzi, które służą do atakowania prawdziwych ludzi. W lipcu 2017 r. Starszy pracownik działu IT w firmie METCO uniknął ataku o włos wkrótce po zatwierdzeniu zaproszenia znajomego z konta honeypot. Wydaje się, że atak był wysoce ukierunkowany na fotografa-amatora-mężczyznę. Wynika to z faktu, że napastnicy stworzyli atrakcyjny profil młodej dziewczyny o imieniu Mia, która powiedziała, że jest fotografem w Londynie, i dzielił z nią wiele zainteresowań. Cel najwyraźniej szybko zaakceptował prośbę przyjaciela, wierząc, że mieli silny związek. Po kilku tygodniach rozmów Mia wysłała mężczyźnie ankietę fotograficzną. Ankieta, nieznana pracownikom IT, była plikiem zawierającym złośliwe oprogramowanie o nazwie Pupy RAT, które służy do kradzieży danych logowania po otwarciu. Na szczęście komputer firmy został zabezpieczony skutecznymi programami antywirusowymi hostów końcowych, które szybko wykrywały i dezynfekowały złośliwe oprogramowanie przed wyrządzeniem jakichkolwiek szkód. Dalsze dochodzenia ujawniły grupę hakerską stojącą za próbą ataku socjotechniki. Potwierdzono, że grupa próbowała wcześniej zaatakować firmę przy użyciu wiadomości e-mail typu phishing, ale żadna z nich się nie powiodła. Pracownicy zostali poinformowani o fałszywych wiadomościach e-mail i klikaniu podejrzanych łączy lub otwieraniu załączników wiadomości e-mail. Wygląda na to, że grupa hakerska była w stanie wymyślić atak inżynierii społecznej i zaatakować jednego pracownika za pośrednictwem Facebooka.

Ten incydent potwierdza, że użytkownicy, niezależnie od działów, w których pracują, są podatni na ataki socjotechniki. Tutejszy cel był specjalistą w dziedzinie informatyki, a jednak postawa młodej, atrakcyjnej kobiety, która podzielała jego zainteresowania, był w stanie zachować czujność. Otworzył plik w sieci organizacji, który mógł ukraść dane logowania, a nawet rozprzestrzenić się w sieci i zainfekować inne komputery. Gdyby zastosowano silniejsze szkodliwe oprogramowanie, atak prawdopodobnie zostałby przeprowadzony. Wszyscy użytkownicy mają do czynienia z tymi samymi słabościami w zakresie inżynierii społecznej. Wystarczy, aby atakujący znalazł słabe punkty w jednej osobowości. Może to być ślepe posłuszeństwo wobec wszelkich autorytetów, samotności, potrzeb finansowych lub potrzeb inwestycyjnych między innymi. Okenyi i Thomas przeprowadzili badanie dotyczące anatomii hakowania ludzi, które można przełożyć na inżynierię społeczną. Powiedzieli, że ludzie są zawsze otwarci na manipulacje ze strony inżynierów społecznych; wystarczy odpowiednie

pokrętła, które należy obrócić. Odkryli, że ludzie byli posłuszni władzy nad nimi i dlatego byli gotowi wykonywać polecenia przekazane przez ich przełożonych. Jest to słabość, z której często korzystają inżynierowie społeczności, próbując przekazywać złośliwe polecenia przy użyciu fałszywych profili wyższej kadry zarządzającej w organizacji. Obaj autorzy doszli również do wniosku, że ludzie są sympatyczni wobec obcych i ufają im. Ludzie są troskliwi i chętnie pomagają nieznajomym, co stawia ich w niefortunnym miejscu, gdy mogą być manipulowani przez zwykłych oszustów. Wykorzystano uprzejmość, zaufanie i współczucie, aby skłonić ludzi do ujawnienia szczegółów hakerom na ich urządzeniach osobistych zawierających bardzo wrażliwe dane. Ci hakerzy mogą następnie zainstalować złośliwe oprogramowanie lub skopiować poufne dane, zanim cel zda sobie z tego sprawę.

Kobiety, zwłaszcza kobiety w ciąży lub niepełnosprawne, były wykorzystywane do pozyskiwania celów w celu ujawnienia szczegółów urządzenia tylko w celu posadzenia złośliwego oprogramowania lub skopiowania lub usunięcia danych. Autorzy odkryli, że ludzie są zawsze zainteresowani pewnymi nagrodami i są gotowi podjąć działania, które rzekomo przyniosą im nagrody. Powszechnie stosowaną taktyką phishingową jest informowanie użytkowników, że mają szansę wygrać ogromne nagrody, jeśli klikną określone linki. Wiele osób chce nagród i dlatego kliknie linki rzekomo prowadzące ich do stron z nagrodami, aby stwierdzić, że linki prowadzą do złośliwych stron internetowych. Ludzie mają także poczucie winy, pragnienie zadowolenia i poczucie moralnego obowiązku. Są to kwestie psychologiczne, które zostaną omówione w kolejnych częściach. Dobrze jest zrozumieć, że inżynieria społeczna nie jest ogólnie złą praktyką; ma zarówno dobre, jak i złośliwe aplikacje. Jest skuteczna w obie strony, ponieważ cele mają te same cechy, które zostały wcześniej szczegółowo opisane, a zatem są zawsze otwarte na atak. Inżynieria społeczna odgrywa kluczową rolę w społeczeństwie; umożliwia ludziom uzyskanie przysług. Bez względu na to, czy są dobre czy złe, ludzie podejmują decyzje korzystne dla osoby, która o nie prosi. Tylko złoczyńcy wykorzystują teraz socjotechnikę do popełniania wielkich przestępstw. Ramy taktyki wykorzystywanej do manipulowania ludźmi podczas przestępstw są takie same, jak stosowane dla pozytywnych rezultatów. Wykorzystywane słabości są względnie takie same i wszyscy ludzie je dzielą. Jednym z najstarszych oszustw socjotechnicznych jest oszustwo w Nigerii. Być może był to pierwszy szeroko zakrojony atak socjotechniczny za pośrednictwem technologii e-mail. Odkąd pojawił się w pierwszych dniach e-maili, wiele osób zakochało się w nim. Atakujący udawali zamożnego nigeryjskiego księcia, który miał lukratywny interes, który wymagał jedynie celu, by zaoferować pomoc i uzyskać duże cięcia. Oszustwa zostały wykonane, gdy cele zostały poproszone o rozwiązanie pewnych problemów poprzez zapłacenie pewnej ilości gotówki w celu uwolnienia dużej wypłaty. Problemy pojawiały się, dopóki cel w końcu nie zorientował się, że nie ma pieniędzy na uwolnienie. W tym ataku wykorzystano kilka cech ludzkich omówione w następujący sposób:

* Pierwszym jest chciwość, w której celom uwierzono, że rzeczywiście dostaną duże cięcie z ogromnej fortuny. Każdy chce pieniędzy, a jeśli przychodzi tak łatwo, wiele osób będzie gotowych zrobić to, o co proszą. Nie jest to dziwna cecha, która występowała tylko u ofiary; jest to charakterystyczny dla wszystkich.

* Kolejną wykorzystaną cechą było zaangażowanie. Ludzie naturalnie chcą widzieć rzeczy do końca. To jest powód, dla którego atakujący odkryli, że mogą oszukiwać ludzi z pieniędzy, zapewniając ich, że im wcześniej dokonają płatności, tym szybciej wypłata zostanie zwolniona. Znów jest to charakterystyczny prezent dla każdego.

* Ostatnią cechą jest zaufanie i była to podstawowa część ataku. Nieznajomi byli manipulowani, aby zaufać innemu nieznajomemu na innym kontynencie i wierzyć, że wszystko, co im powiedziano, było prawdą. Zaufanie jest potężne, a nieznajomi szybko dali rzekomemu nigeryjskiemu księciu korzyść z wątpliwości, kiedy wystąpił błąd w przetwarzaniu wypłaty. Wykorzystując jednocześnie trzy ludzkie słabości, atak był bardzo silny i niektórzy ludzie skończyli tracąc nawet 50 000 $.

Poprzednia instancja opisuje dobrze zorganizowany atak inżynierii społecznej, który wykorzystuje cechy ludzkie do szkodliwych celów. Należy zauważyć, że te same cechy są wykorzystywane do pozytywnych wyników. Zaufanie jest wykorzystywane codziennie w umowach lub podczas zawierania transakcji i tylko w niefortunnych scenariuszach jest wykorzystywane w sposób złośliwy. Zobowiązanie jest stosowane w prawie wszystkich przedsiębiorstwach, aby zapewnić ich pomyślną realizację. Ludzie otrzymują pewną nagrodę wewnętrzną za wykonywanie zadań i dlatego są zobowiązani do przeglądania wszystkiego, co zaczynają. Chciwość niekoniecznie jest też złą cechą. Subtelnie chciwy jest tylko człowiek. Pieniądze są poszukiwane i to subtelna chciwość pozwala ludziom szukać ich na wszystkie możliwe sposoby. Dlatego tylko w niefortunnych scenariuszach te cechy są wykorzystywane do szkodliwych celów.

Zastosowania inżynierii społecznej

Inżynieria społeczna jest wykorzystywana w wielu konfiguracjach i zawodach przez ludzi i instytucje, omówione tutaj w następujący sposób:

* Prawnicy i psychologowie: te grupy ludzi muszą wprowadzać ludzi w określony stan umysłu, aby manipulować ich umysłami. Używają tej samej taktyki, jakiej używałby każdy inny inżynier społeczny. Po prostu używają ich w nie-złośliwych zamiarach. Dzięki tej taktyce są w stanie przeprowadzić udane przesłuchania i wywiady oraz skłonić ludzi do ujawnienia informacji, których w innym przypadku odmówiliby.

* Rządy: Rządy muszą korzystać z inżynierii społecznej, aby mieć kontrolę nad ludźmi, którymi rządzą. Jednym z kluczowych sposobów inżynierii społecznej jest wykorzystanie autorytetu. Rządy kontrolują większość autorytetów w kraju, a mózgi ludzkie są uwarunkowane przynależnością do autorytetu. Innym sposobem jest użycie niedoboru. Jeśli tego nie będzie, rządy stworzą niedobór, aby mogli zachować w świadomości ludzi, że to oni (rządy) są tymi wciąż odpowiedzialnymi. Niedobór może dotyczyć wielu rzeczy, takich jak informacje, pieniądze, a nawet jedzenie. W krajach takich jak Korea Północna niedobór żywności i informacji jest nadużywany przez reżim władzy, aby ludzie byli posłuszni.

* Sprzedawcy: opanowali sztukę przekonywania ludzi do kupowania rzeczy, w tym tych, których nie potrzebują. Sprzedawcy są dobrymi inżynierami społecznymi, ponieważ potrafią wykorzystywać umiejętności wielu osób w celu wywołania popytu na ich produkty od potencjalnych klientów. Dzisiaj sprzedawcy wykorzystują technologię, aby pomóc im w gromadzeniu informacji i wpływać na ludzi, aby kupowali określone produkty. Inżynieria społeczna odgrywa w tym wszystkim kluczową rolę.

* Rekruterzy: działy zasobów ludzkich (HR) w większości organizacji zajmują się doświadczonymi inżynierami społecznymi. Rekruterzy opanowali sztukę czytania w myślach ludzi, aby dowiedzieć się, co ich tak naprawdę napędza, i ich przydatność na reklamowanych stanowiskach. Inżynieria społeczna jest wykorzystywana, aby zachęcić kandydatów do otwarcia i ujawnienia informacji, które mogłyby pomóc HR w ustaleniu, czy ich zatrudnić.

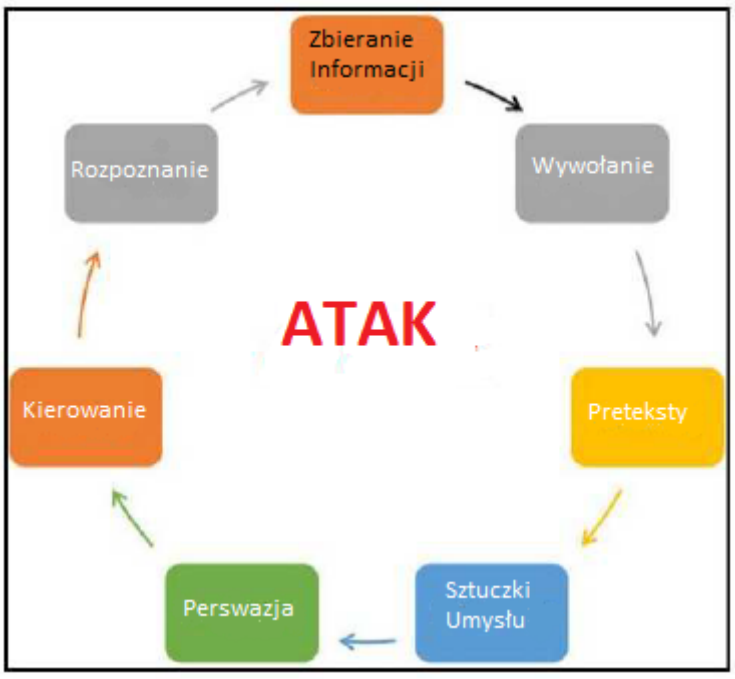
* Szpiedzy: Szpiedzy są intensywnie uczeni specjalnych technik inżynierii społecznej, których używają, aby oszukiwać ludzi, aby wierzyli, że są ludźmi, którymi zostali wysłani. Uczą się także, jak stosować taktykę inżynierii społecznej do zbierania danych wywiadowczych od niczego niepodejrzewających ludzi. Szpiedzy mogą łatwo uzyskać zeznania od hardcorowych przestępców dzięki inżynierii społecznej. Nawet w przypadku naruszenia bezpieczeństwa mogą odzyskać swoją tajną tożsamość za pomocą inżynierii społecznej. Inżynieria społeczna oznacza dla nich przetrwanie i dlatego są w tym wyjątkowo dobrzy.

* Oszuści: Oszustwa są w większości możliwe dzięki inżynierii społecznej. Oszuści muszą wiedzieć, jak przyciągnąć ludzi do kupowania oszustów bez pytania. Oszuści identyfikują swoje znaki z daleka i badają je z czasem. Zbierają krytyczne wskazówki na temat swoich znaków, dopóki nie mają wystarczającej ilości informacji, aby je trafić. Oszuści udoskonalili sztukę tworzenia scenariuszy, którym nie można się oprzeć. Wszystko to jest możliwe dzięki inżynierii społecznej.

* Złodzieje tożsamości: Kradzież tożsamości jest przestępstwem większym niż kradzież czyjegoś nazwiska, konta bankowego, adresu i danych finansowych. Złodziej tożsamości czasami musi stać się osobą, z której ukradł tożsamość, aby popełnić większe przestępstwo, które przynosi większe zyski. W tym miejscu wkracza inżynieria społeczna. Złodziej tożsamości użyje różnych taktyk, aby dogadać się z ludźmi w życiu ofiary. Złodziej tożsamości wykorzysta status profilu ofiary, aby zrobić mu przysługę. Jeśli skradziona tożsamość dotyczy wyższego członka personelu w organizacji, złodziej tożsamości może wykorzystać uprawnienia do zmuszenia pracowników finansowych do dokonania niektórych niezweryfikowanych płatności. Kradzież tożsamości jest wysoce wspierana przez socjotechnikę. Wszyscy ci ludzie używają inżynierii społecznej zarówno pozytywnie, jak i negatywnie. My koncentrujemy się jednak na inżynierii społecznej do szkodliwych celów. Jest to poważny problem dla wielu ludzi, organizacji i rządów. Sprawiło, że wielu straciło wiarę w ochrona ich systemów.

Ramy inżynierii społecznej

Cykl inżynierii społecznej pokazano na poniższym rysunku:



W każdym udanym ataku inżynierii społecznej przestrzegane są określone ramy. Struktura składa się z siedmiu dyskretnych kroków, które prowadzą inżyniera społecznego na drodze do uzyskania większej wiedzy na temat celu, wyboru strategii ataku, a następnie skrupulatnego jej wykonania. Ramy są następujące:

Zbieranie informacji

Jest to uważane za najbardziej krępujący krok w całym ćwiczeniu inżynierii społecznej i może trwać od kilku godzin do kilku lat. Jest nie tylko długi, ale wymagający i wymaga od atakującego ciągłej obserwacji celu. Dzisiejszy inżynier społeczny musi być dobrze poinformowany o poszukiwanych

danych i narzędziach programowych, które mogą w tym pomóc. Szybkie przyjęcie platform mediów społecznościowych przez duży procent ludzi sprawiło, że proces ten jest nieco prostszy. Jednak dane te są czasami niewystarczające lub zbyt sfabrykowane, aby mogły być pomocne, dlatego może być wymagane więcej źródeł danych. Atakujący może zatem zostać zmuszony do gromadzenia danych przy użyciu specjalistycznych narzędzi programowych lub umiejętności miękkich, aby uzyskać te dane bezpośrednio od celu bez wywoływania alarmu. Informacje rzadko są zbierane jednocześnie. Jest to trudne i dlatego inżynier społeczny często zbiera małe dane i łączy je, aby ukończyć zagadkę o celu. Na przykład, zbierając informacje o CEO, osoba atakująca może rozpocząć od rozmowy z ludźmi, z którymi CEO się spotyka lub z którymi rozmawia. Strażnicy, sekretarki, podwładni, a nawet goście mogą zostać przesłuchani, aby znaleźć małe informacje, które mogą nie być tak dyskretnie przydatne, ale bardzo potężne, gdy zostaną zebrane razem. Nawet najbardziej nieistotna z osób, z którymi współdziała cel, może mieć klucz do odblokowania znacznie większej układanki. Dlatego każde źródło informacji jest traktowane jako wartościowe. Istnieją dwie główne metody gromadzenia danych, które mogą zostać wykorzystane przez atakującego - metody nietechniczne i techniczne.

Nietechniczne

Metody te nie uwzględniają użycia jakichkolwiek środków technologicznych do gromadzenia danych. Mogą być bardziej męczące, ale najprawdopodobniej znajdą bardziej dokładne dane na temat celu. Metody nietechniczne omówiono w następujący sposób:

* Nurkowanie w kontenerach: polega na przejściu papierowych odpadów celu, aby znaleźć cenne informacje, które mogły zostać usunięte. Nawet przy niszczarkach papieru ludzie są na tyle leniwi, że beztrosko wyrzucają cenne dane, które atakujący mogą znaleźć podczas nurkowania na śmietniku.

* Fizyczne dostosowywanie celu: daje atakującemu informacje na temat procedur celu, harmonogramów, polubień, nielubień i tak dalej. Gra końcowa polega na zbliżeniu się do celu z kilkoma pytaniami, a następnie przedstawieniu ofert, których nie mogą odmówić. Dzięki temu inżynier społeczny może potencjalnie uzyskać mnóstwo informacji i dostęp do ograniczonych miejsc. Po ustaleniu racjonalizacji celu można nadużyć, aby uzyskać znacznie więcej. Metody nietechniczne są jednak stopniowo wycofywane i obecnie większość gromadzenia informacji odbywa się metodami technicznymi:

Techniczny

Metody te obejmują wykorzystanie produktów technologicznych do uzyskiwania informacji o kliencie. Jedną z tych metod jest śledzenie celu na ich kontach w mediach społecznościowych. Większość celów będzie mieć aktywne profile na LinkedIn, Facebooku, Twitterze, Instagramie lub Snapchacie. Użytkownicy tych platform są tak nieostrożni ze swoimi danymi, że inżynierowie społecznościowi w wielu przypadkach nie muszą szukać daleko. Nawet po powtarzających się ostrzeżeniach dla osób o zmianie ustawień prywatności bardziej prawdopodobne jest, że konto celu będzie widoczne publicznie,

a tym samym dla każdego. Użytkownicy poświęcali całe swoje życie nieznajomym i wszystko, co może polubić, prawdopodobnie zostanie opublikowane. Informacje, które niegdyś były prywatne, są teraz umieszczane bez ograniczeń w domenach publicznych. To sprawia, że inżynier socjalny jeszcze łatwiej gromadzi dostępne dane na temat celu. Jednak w niektórych przypadkach atakujący może nie mieć tyle szczęścia, ponieważ podane dane są zbyt małe lub konto jest ustawione jako prywatne. Wymaga to zatem od inżyniera społecznościowego utworzenia fałszywego konta, które pasuje do preferencji i upodobań celu. Dzięki temu klient może poprosić cel, aby został przyjaciółmi lub podążał za nimi. Innym powszechnym podejściem było użycie fałszywego konta utworzonego na nazwisko osoby znanej celowi. Bliscy przyjaciele, krewni i szefowie w pracy byli wykorzystywani w wielu atakach socjotechnicznych z dużym powodzeniem. Drugą powszechnie stosowaną techniczną metodą inżynierii społecznej jest wyszukiwanie w wyszukiwarkach. Wyszukiwarki indeksują wiele witryn, a niektóre z nich przechowują informacje o użytkownikach zebrane z wielu źródeł i zebrane razem w centralnym miejscu. Istnieją specjalne zapytania Google, które można wykorzystać do wyszukiwania informacji o osobach znajdujących się na stronach internetowych. Zostaną one szczegółowo omówione w następnej części na temat gromadzenia danych. Przykładem może być następujące zapytanie: „David Wilson" intitle: „curriculum vitae" „telefon" „adres" „e-mail" „Jest to bardzo potężne zapytanie, którego można użyć do znalezienia jakichkolwiek informacji o osobie dzwoniącej. Google szuka Davida Wilsona w poszukiwaniu stron internetowych o nazwie David Wilson i takich tytułów, jak życiorys, telefon i adres. Wiele tablic ofert pracy przechowujących dane osób poszukujących pracy przechowuje informacje o osobach poszukujących pracy w domenie publicznej, łatwo będzie znaleźć osobę o imieniu David Wilson, z której można odzyskać dane osobowe. To zapytanie może nawet przywołać CV Davida Wilsona, jeśli istnieje strona, która przechowuje informacje na jego temat. Strona znana jako Pipl (https ://pipl. com) jest jednym z największych archiwów informacji o dużej liczbie osób. Dla każdej osoby, którą ma w swojej bazie danych, strona zachowuje adres e-mail tej osoby, konta w mediach społecznościowych, numer telefonu i adres fizyczny. Witryna twierdzi, że zawiera szczegółowe informacje na temat ponad trzech miliardów ludzi. Szybko zbliża się do połowy ludzkiej populacji na ziemi. Ta strona jest kopalnią złota dla inżynierów społecznych, ponieważ mogą oni bez trudu znaleźć dość osobiste informacje o swoich celach. Istnieje wiele innych witryn, takich jak ujawnianie prywatnych informacji o osobach wszystkim, którzy proszą o takie informacje. Witryny te mają szerokie źródło tych rejestrów, które obejmują platformy społecznościowe, dane sprzedawane przez strony trzecie, dane uwalniane przez hakerów, dane skradzione z innych stron internetowych oraz dane na stronach agencji rządowych. Aktualizują swoje dane tak często, jak to możliwe. Niestety takie witryny nie są nielegalne, dlatego trudno jest zmusić je do usunięcia Twoich danych. Innym technicznym źródłem informacji, z którego nadal korzystają inżynierowie społeczności, jest korzystanie z telefonów. Jest to zwykle skierowane do osób starszych, ponieważ łatwo jest ich oszukać. Dzwoniący zawsze twierdzą, że pochodzą od renomowanych firm lub agencji rządowych. Używają kuszących ofert lub poważnych zagrożeń, aby zdobyć cele i wysłać im gotówkę. Istnieją doniesienia o niektórych dzwoniących, którzy podają się za policję i grożą aresztowaniem celów, jeśli nie wyślą pewnej kwoty w określonym terminie. Inne osoby również są atakowane, a najcenniejszym zasobem, jaki mają inżynierowie społeczności, jest informacja o celu. Sama znajomość konta bankowego celu może być wystarczającą zachętą, aby przekonać klienta, że to bank dzwoni. Mogą użyć numeru konta bankowego, aby cel ujawnił jeszcze więcej danych, w tym numery ubezpieczenia społecznego. Kiedy cele uświadamiają sobie, że może to nie telefon z banku, zwykle jest już za późno. Inżynierowie społeczności będą mieli wystarczającą ilość informacji, aby zaplanować atak. Gromadzenie danych jest w rzeczywistości żmudne, długotrwałe i wymagające. Jest to jednak warte. Ilość informacji zebranych od celów jest niezbędna w planowaniu ataku. Najlepsza metoda gromadzenia danych to taka, która nie wyklucza motywacji inżyniera społecznego. Dlatego gromadzenie danych odbywa się dyskretnie.

Małe fragmenty informacji są wyciągane krok po kroku i łączone razem. Z czasem inżynier społeczny będzie miał więcej niż wystarczającą ilość informacji, aby profilować cel. Inżynier społeczny dowie się więcej o życiu celu niż jego rodzina lub małżonek. To są informacje, które określą powodzenie ataku. Istnieje wiele innych metod gromadzenia danych i narzędzi, które są wykorzystywane w tym procesie. Te, które zostały omówione, również nie zostały szczegółowo omówione. Zostaną one jednak omówione w następującym temacie dotyczącym gromadzenia danych. Zidentyfikujemy wszystkie metody i narzędzia, opiszemy je i podamy przykłady zastosowania każdego z nich. Pod koniec rozdziału będziesz biegły w zbieraniu danych o celach dokładnie tak, jak robi to inżynier społeczny.

Wywołanie

Nawet ze swoimi słabościami ludzie na ogół zostaną na początku wycofani z powodu zwierzenia się komukolwiek. Potrzeba umiejętności, aby oderwać ludzi od ich stref bezpieczeństwa, aby mogli zacząć wyrzucać prywatne informacje. Wywoływanie to coś więcej niż budowanie relacji z nieznajomymi; jest to technika stosowana w pokojach przesłuchań, stosowana przez terapeutów i lekarzy w celu uzyskiwania informacji od osób, które w przeciwnym razie odmawiałyby takich informacji. Wywołanie jest zatem drugim krokiem w ramach socjotechniki, który następuje podczas ataków inżynierii społecznej. Atakujący używają technik wywoływania po zebraniu wystarczającej ilości informacji o celu, aby zainicjować rozmowę. Wywołanie można zdefiniować jako czynność wyciągnięcia czegoś za pomocą logiki. Odbywa się to poprzez stymulację, aby skłonić kogoś do działania w pewnej klasie zachowań. Definicja oznacza zatem, że wzbudzanie to zdolność wyciągania ludzi ze stref bezpieczeństwa, pobudzając ich do działania w określony sposób. Inżynier społeczny opanuje sztukę wzbudzania do tego stopnia, że może doprowadzić cel do tego stopnia, że chce po prostu odpowiedzieć zgodnie z prawdą na każde postawione pytanie. Szpiedzy i przesłuchujący są szkoleni, jak korzystać z tej umiejętności, aby wyciągać informacje podczas normalnych rozmów. To pokazuje, że jest to już umiejętność ceniona przez rządy. Celowi trudno jest wykryć próbę wywołania. Wydaje się tak niewinny i występuje w normalnych warunkach. Oto niektóre z czynników, które sprawiają, że pozyskiwanie jest tak skuteczne:

* Większość ludzi będzie starać się być grzecznym podczas rozmowy z nieznajomym

* Specjaliści, gdy zostaną przesłuchani, będą chcieli wyglądać na kompetentnych

* Większość ludzi nie okłamuje kogoś, kto wygląda na naprawdę zaniepokojonego

* Bardziej prawdopodobne jest, że ktoś odpowie na dobrze postawione pytania na swój temat.

W odpowiedzi inżynier społeczny będzie próbował związać cel z określoną ścieżką, aby otwarcie udostępniać poufne informacje bez zastanowienia. Przedstawiono go jako prostą interakcję pytanie-odpowiedź, podczas gdy w prawdziwym sensie cel jest doprowadzony do ujawnienia tajnych informacji. Inżynier społeczny postara się zachować zgodność celu z odpowiedzią na niektóre pytania, które mogą być przede wszystkim niewygodne. Cel będzie na nie odpowiadał, dopóki inżynier społeczny poprawnie zagra swoje karty. Jeśli chodzi o prawidłowe zagrywanie kartami, inżynier społeczny jest bardzo surowy. Są to:

* Bycie naturalnym: Jednym z najlepszych sposobów na kontynuowanie rozmowy bez podnoszenia brwi jest zapewnienie komfortu celu, brzmiąc autentycznie i naturalnie. Łatwo jest wystraszyć cel, jeśli rozmowa wydaje się nienaturalna lub skryptowana. Dlatego inżynier społeczny zaangażuje cel w rozmowę, z którą on / ona (inżynier społeczny) jest zaznajomiony. Inżynier społeczny będzie również pracował nad swoją postawą, mową ciała i zapewnieniem wiedzy. Wszystko musi wyglądać zupełnie normalnie, aby inżynier społeczny wyglądał na pewnego siebie i naturalnego. Inżynierowie społeczni

często odgrywają role ze swoimi przyjaciółmi, aby zebrać się w sobie przed podjęciem rzeczywistej próby podniecenia.

* Wiedza: wiedza jest idealną tarczą dla inżyniera społecznego podczas interakcji z celem. Dlatego bez względu na to, jakie pytania będą zadawane celowi, musi on wiedzieć o ich oczekiwanej odpowiedzi. Pozwoli to inżynierowi społecznemu na potwierdzenie lub różnicę w stosunku do celu przy użyciu pewnej wiedzy, co pozwoli kontynuować rozmowę. Oczywiście od inżyniera społecznego nie oczekuje się dużej wiedzy na temat udzielanych odpowiedzi; może to podnieść czerwoną flagę. Potrzebna jest jedynie podstawowa wiedza, aby móc zadawać pytania uzupełniające i odpowiadać na odpowiedzi podane przez cel.

* Unikanie chciwości: Inżynierowie społeczni muszą upewnić się, że nie wydają się być chciwi wobec swoich celów. Jeśli dla celu stanie się oczywiste, że inżynier społeczny szuka określonej informacji, cel najprawdopodobniej wyłączy inżyniera społecznościowego. Dlatego powszechną praktyką jest, aby inżynier społeczny ćwiczył dawanie i branie. Inżynier społeczny wymyśla fałszywe informacje i oferuje je celowi. Widząc tę otwartość, cel odwzajemnia się, udzielając pewnych informacji, ale w tym przypadku okazuje się, że są to informacje faktyczne.

Te trzy są podstawowymi kartami, które każdy inżynier społeczny musi mieć w rękawach podczas interakcji z celem. Poza tym bardzo ważne jest, aby inżynier społeczny używał właściwych mimik we właściwym czasie. Istnieje kilka wyrażeń, które są trudne do sfałszowania i dlatego wymagają od inżyniera socjalnego przeprowadzenia rozległych prób, aby je poprawnie. Wyraz twarzy wpływa na sposób, w jaki ludzie odpowiadają na pytania. Dlatego inżynier społeczny musi stosować wyrażenia, które wykazują zainteresowanie i poprawiają nastrój celu, jeśli to konieczne. Wyraz twarzy wiele mówi i może potencjalnie wpłynąć na wynik próby wywołania. W każdym razie inżynier społeczny musi być w stanie naprawdę pojawić się w rozmowie. Wywoływanie jest kluczowym krokiem w inżynierii społecznej. Istnieje kilka sprawdzonych umiejętności wywoływania.

Preteksty

Jest to zwykle trzeci krok w ataku inżynierii społecznej. W tym momencie atakujący staje się kimkolwiek, kto może wpłynąć na cel przy podejmowaniu pewnych decyzji. Atakujący wybiera pewną osobowość, która pasuje do postaci, którą chce zostać podczas próby inżynierii społecznej. Wraz z pojawieniem się Internetu łatwo jest stać się kimkolwiek. Jest tak wiele zasobów informacyjnych, że inżynier społeczny może użyć do dostosowania charakteru każdego. to umiejętność niezbędna do pretekstowania dla każdego inżyniera społecznego w celu przeprowadzenia ataku. Pretekst jest czymś więcej niż tylko odgrywaniem roli osoby; można to uznać za osobę. Cel nie powinien mieć wątpliwości, że inżynier społeczny nie jest tym, za kogo się podaje. Charakter inżyniera społecznego, jego sposób mówienia, mowa ciała i każda inna zauważalna cecha musi pasować do charakteru osoby, którą udaje. Jest to niezbędna umiejętność, która pozwoli inżynierowi społecznemu przeprowadzić atak bez podejrzeń. Jest bardzo wiele dynamiki, jeśli chodzi o preteksty. Zapewniają, że inżynier społeczny jest w stanie wymyślić scenariusz i skłonić cel do podjęcia pewnych działań lub ujawnienia poufnych informacji. W ostatnich atakach coraz częściej zauważono, że inżynierowie społeczni wykorzystują ludzi na niektórych szanowanych stanowiskach lub profilach starszych pracowników w niektórych organizacjach. Inżynierowie społeczni są gotowi poświęcić odpowiednią ilość czasu na zbadanie ról, które będą pełnić z ich nowymi osobowościami. Trenują, aż dojdą do punktu, w którym będą idealnymi klonami ludzi, których chcą podszyć się. Mogą następnie wykorzystać te personifikacje, aby przekonać swoich celów do robienia tego, co chcą, aby mogli z łatwością. Preteksty są bardzo skuteczne i są powszechnie stosowane w innych dziedzinach. Lekarze, prawnicy, a nawet terapeuci stosują jakieś techniki pretekstowe, ilekroć wchodzą w interakcje z ludźmi w życiu zawodowym. Są w stanie

wprowadzić ludzi w strefę komfortu, gdzie ujawniają informacje, które powstrzymywali. Inżynierowie społeczni starają się osiągnąć taką samą ilość perswazji i zaufania w swoich próbach pretekstu. W poprzedniej dyskusji na temat zbierania informacji zauważono, że zbieranie informacji jest kluczową determinantą sukcesu całego ataku socjotechniki. Jest to jeden z etapów, na którym liczy się zebrana informacja. Inżynierowie społeczni muszą ostrożnie używać pretekstów, które są absolutnie pewne, że cel padnie. Jeśli w niefortunnym przypadku inżynier społeczny użyje pretekstu, z którym cel nie może się odnieść, cały atak zostanie sabotowany. Na przykład, jeśli cel korzysta z banku B, a inżynier społeczny dzwoni, mówiąc, że jest urzędnikiem z banku A, cel będzie wiedział, że jest to ustawione i atak się nie powiedzie. Co więcej, cel będzie tak przerażony, że nawet kolejna próba nie spowoduje, że podda się oszustwu. Inżynier społeczny niewiele może zrobić, gdy cel zda sobie sprawę, że atakuje go on lub ona. Jedyną wskazaną rzeczą jest ratowanie się i porzucenie całego ataku. Dlatego niezwykle ważne jest, aby próba pretekstu zakończyła się powodzeniem. Istnieje kilka ogólnych zasad, które są przestrzegane podczas pretekstu, w tym:

* Więcej badań: Istnieją większe szanse na próbę pretekstu, jeśli inżynier społeczny przeprowadził odpowiednie badania. Cel może zacząć zadawać pytania i niezwykle ważne jest, aby inżynier społeczny dysponował pewnymi informacjami, które można wykorzystać, aby odpowiedzieć na nie zgodnie z wiedzą oczekiwaną od jego osobowości.

* Używaj osobistych zainteresowań: preteksty umieszczają osobę w skórze innej osoby, co jest bardzo trudnym zadaniem. Są rzeczy, których nie można łatwo podrobić. Dlatego inżynierowie społeczni mogą nieco odwrócić uwagę od osobowości ludzi, którymi udają, i wykorzystać swoje rzeczywiste interesy. Nic nie może być tak katastrofalne, jak wstydliwe odkrycie, że inżynier społeczny nie ma wiedzy na temat zainteresowań, które przekazuje celowi. Lepiej jest skorygować założenie dotyczące pewnych osobistych zainteresowań, niż grać tylko po to, aby osiągnąć cel, w którym cel zaczyna mieć wątpliwości. To jest dobre dla pewności siebie i dla budowania zaufania, że inżynier społeczny wykorzystuje interesy, z którymi jest zaznajomiony podczas budowania relacji z celem.

* Ćwicz wyrażenia lub dialekty: łatwo jest ustalić, że dana osoba nie jest tym, za kogo się podaje, po prostu słuchając dialektu lub wyrażenia. Istnieje kilka żargonów obecnych w niektórych branżach zawodowych, które pomagają przyjąć założenie, że inżynier społeczny jest rzeczywiście osobą, za którą się podaje. Zwykła rozmowa może nie być tak pewna dla celu na temat osobowości przyjętej przez inżyniera społecznego. Jeśli na przykład inżynier społeczny przyjmuje osobowość prawnika, powinien istnieć pewien poziom żargonu prawnego, na przykład wzmianka o niektórych ustawach, rachunkach lub karach za niektóre przestępstwa. To szybko zbuduje przekonanie klienta, że inżynier społeczny jest prawdziwym prawnikiem. Dlatego dialekty są bardzo ważne w pretekstach, a inżynierowie społeczni zwykle zwracają na nie dużą uwagę.

* Używaj prostszych pretekstów: im bardziej skomplikowany staje się pretekst, tym mniejsza szansa na sukces. Jest tak, ponieważ potrzeba więcej badań i wysiłków, aby go utrzymać i może się to nie powieść. Z drugiej strony prostszy pretekst będzie szybszy i łatwiejszy do perfekcji, a to oznacza, że będą większe szanse na trafienie celu. Dlatego tylko legendarni inżynierowie społeczni mają możliwość wyboru złożonych pretekstów, ponieważ mają większą wiedzę i doświadczenie w obsłudze takich pretekstów. Oznacza to również, że istnieje wiele ataków socjotechniki niskiego poziomu, które można łatwo przeprowadzić. Ze strony ofiary bardziej prawdopodobne jest, że ktoś podejdzie do niej pod pretekstem starego przyjaciela, krewnego lub starego kolegi z klasy. Są łatwe do sfałszowania.

* Logiczne wnioski: ataki socjotechniki są dobrze skoordynowane. Od momentu wzbudzenia do etapu pretekstu należy przestrzegać ogólnego wzorca. Kroki muszą być logiczne. Na etapie pretekstu informacje podawane na początku muszą być zgodne z tym, czego chce inżynier społeczny. Pretekstu

adwokata nie można na przykład użyć, aby uzyskać cel ujawnienia poświadczeń logowania do pracy. Pretekst powinien logicznie doprowadzić cel do pewnego wniosku. Pretekstu do wsparcia IT można łatwo użyć do przekonania celu do podania danych logowania. Można by powiedzieć celowi, że niektóre systemy napotkały pewne problemy, a firma przechodzi na systemy tworzenia kopii zapasowych, dlatego w celu ułatwienia migracji wymagane są stare poświadczenia. Ten scenariusz ma logiczny wniosek. Bardziej prawdopodobne jest, że zadziała, niż jeśli pretekst prawnika zostanie wykorzystany do uzyskania tych samych informacji. Nie będzie połączenia i celowi będzie trudno połączyć kropki i podać wymagane informacje.

Istnieje wiele innych zasad, z których korzystają inżynierowie społecznościowi. Zostaną one szczegółowo omówione w kolejnych częściach. Preteksty są bardzo trudne i na tym etapie wiele prób socjotechniki może się nie powieść. Z punktu widzenia obrony należy nauczyć użytkowników, jak przesłuchiwać podejrzanych inżynierów społecznych, aby w tym momencie zapobiec atakom. Pretekst jest czymś więcej niż zakładaniem sfałszowanej tożsamości; bardziej żyje się tą tożsamością. Jest to trudne, ale jeśli się powiedzie, atak socjotechniki zostanie nakreślony we właściwym kierunku. W tym kroku użyto kilku narzędzi, które zostaną omówione w tej części.

Sztuczki umysłowe

Cały atak socjotechniki opiera się na sztuczkach umysłowych, więc jest to krok, który jest wykorzystywany w wielu innych częściach struktury ataku socjotechniki. Ta część ataku socjotechniki polega na użyciu specjalnie spreparowanych sztuczek w celu zmiany wzorców myślowych ofiar. Sztuczki umysłowe są do pewnego stopnia wykorzystywane w wielu innych obszarach życia, takich jak sprzedaż, aby ceny produktów wydawały się mniej kosztowne, a także w pokojach przesłuchań, aby podejrzani przyjmowali zarzut. Sztuczki umysłowe są raczej sprawą psychologiczną i służą do odblokowywania umysłów celów, wystawiając je na kontrolę inżyniera społecznego. Doskonały inżynier społeczny jest dobrym czytelnikiem umysłu, a osiąga się to poprzez opanowanie wielu sztuczek umysłu. Sztuczki umysłowe zaczynają się od relacji. Jest to pierwotny wysiłek wykorzystywany do zdobycia zaufania celów. Stąd inżynier społeczny stosuje kilka sztuczek mających na celu zmianę normalnego myślenia mózgu celu. Można to przyrównać tylko do techniki hakowania zwanej przepełnieniem bufora. To tutaj program jest dostarczany z większą ilością danych, niż może zawierać w swoich buforach. W związku z tym program zaczyna zachowywać się nieregularnie z powodu przepełnienia informacji. Ludzki mózg może być podobnie przytłoczony, otwierając go na manipulację ze strony inżynierów społecznych. Istnieją trzy tryby myślenia, które można wykorzystać u człowieka. Są to:

* Myślenie wizualne: Myśliciele wizualni to ludzie, którzy przetwarzają informacje wizualnie. Są dobrzy w wyobrażaniu sobie rzeczy, a ich decyzje zwykle opierają się na ogólnym obrazie, który tworzą w ich mózgach. Myśliciele wizualni są zatem ukierunkowani na rzeczy, które są atrakcyjne wizualnie, a nie na te, które są dla nich korzystne. Mężczyźni są głównie myślicielami wizualnymi i dlatego ich produkty są atrakcyjne wizualnie w reklamach. Aby dotrzeć do umysłów myślicieli wizualnych, inżynierowie społeczni również skupiają się na przekazywaniu im informacji wizualnych.

* Myślenie słuchowe: Myśliciele słuchowi są bardzo dobrzy w rozumowaniu na podstawie dźwięku rzeczy. Łatwo ich przekonują głosy, ponieważ są stronnicze w tym, jak przetwarzają informacje z różnych dźwięków. Łatwo ich dotykają dźwięki i łatwo tworzą z nich wspomnienia. Warto zauważyć, że nie musi się z nimi rozmawiać fizycznie. Można wprowadzić ich w stan myślenia, w którym mogą odczytać określony głos podczas czytania dowolnego tekstu. Stąd więcej zajmuje się starannym doborem słów i bardzo mało uwagi poświęci doborowi słów o niskim wysiłku.

* Myślenie kinestetyczne: Myśliciele kinestetyczne są myślicielami emocjonalnymi i łączą się z emocjami pochodzącymi z rozmowy. Robią się ciepli, jeśli rozmowa jest ciepła, sympatyczna, jeśli rozmowa dotyczy smutnych doświadczeń i wielu innych emocji. Ich emocje są do zdobycia za każdym razem, gdy prowadzą rozmowę, co stawia ich w bardzo niekorzystnej sytuacji, ponieważ ruchy są zwykle bardzo silne. Emocje mogą być wykorzystane do gwałtownej zmiany decyzji bez żadnych pytań. Kobiety w dużej mierze należą do tej kategorii, w której ich emocje można łatwo kołysać.

Są to trzy podstawowe tryby myślenia obecne u ludzi. Należy zauważyć, że ludzie zasadniczo nie są przywiązani do określonego sposobu myślenia. Mogą mieć wszystkie trzy sposoby myślenia, ale jeden będzie bardziej dominujący nad innymi. Jest to sposób myślenia, którego będzie szukał inżynier społeczny. Po jego odkryciu reszta będzie dziecinnie prosta. Bardzo łatwo będzie wymyślić scenariusze, które spowodują, że cel straci normalne rozumowanie i będzie działał zgodnie z życzeniem inżyniera społecznego. Największą przeszkodą jest zawsze dostrzeganie dominującej metody myślenia. Wymaga to rozmowy, w której inżynier społeczny może wypróbować różne konteksty opowieści i sprawdzić, czy wywołują dominujący sens w celu.

Wizualnego myśliciela można określić za pomocą wizualnych pytań i komentarzy. Jeśli cel wydaje się odpowiadać w naturze, powołując się na więcej aspektów wizualnych, można stwierdzić, że jest on myślicielem wizualnym. Z drugiej strony myśliciela kinestetycznego można określić za pomocą poruszających opowieści. On lub ona może być również zdeterminowana chęcią dotykania i odczuwania rzeczy. Dlatego jeśli cel chce dotknąć i poczuć materiał lub zegarek, najprawdopodobniej jest myślicielem kinestetycznym. Podobnie, jeśli małe historie pełne emocji wydają się poruszać cel, można powiedzieć, że cel jest myślicielem kinestetycznym. Myśliciela z dominacją słuchu można ustalić, obserwując jego reakcje podczas słuchania lub czytania czegoś. Ci, którzy ledwo się wzdrygają, są myślicielami niesłyszącymi. Z drugiej strony ci, którzy wydają się łączyć ze słowami mówionymi lub pisanymi, są myślicielami słuchowymi. Temat sztuczek umysłowych jest bardzo długi i zostanie dogłębniej omówiony wkrótce. Należy pamiętać, że sztuczki umysłu nie są nauką. Polegają na aktywnych dostosowaniach inżyniera społecznego. Omawiane na przykład sposoby myślenia nie są łatwe do ustalenia. Jedyne, co może zrobić inżynier społeczny, to obserwować jak najwięcej. Zastosowanie pytań do odkrycia sposobu myślenia może być irytujące i odrażające. Dlatego najlepszą bronią jest obserwacja. Jest wiele innych rzeczy związanych z myśleniem, które zostaną omówione. Jak wspomniano, sztuczki umysłu mają tendencję do przekrojowego wykonywania wszystkich kroków w ramach socjotechniki. Nie są zarezerwowane na określone wydarzenie; są wprowadzani do gry w momencie rozpoczęcia ataku inżynierii społecznej. Zbieranie informacji, pozyskiwanie i preteksty są wykorzystywane do budowania bardziej otwartego etapu, w którym można je zastosować. Są one niezbędne w ataku inżynierii społecznej, ponieważ mogą sprawić, że będzie on krótszy i bardziej skuteczny. Po podbiciu umysłu celu atak jest równie dobry, jak gotowy.

Perswazja

Podobnie jak sztuczki umysłu, perswazja jest tematem przekrojowym w całym procesie inżynierii społecznej i dlatego nie można go ograniczyć do określonego kroku. Aby przekonać cel, inżynier społeczny musi najpierw odwołać się do jego zainteresowań. Perswazja pozwala celom reagować, myśleć i robić dokładnie tak, jak chce inżynier społeczny. Perswazja prowadzi do niekwestionowanego wpływu w umysłach celów. Aby atak się powiódł, inżynierowie społeczni doskonalą swoje umiejętności perswazyjne. Zapewniają, że wpływ, jaki mają na cele, jest niewykrywalny, ale dalekosiężny. Perswazję najlepiej zrozumieć dzięki pięciu podstawom zastosowanym przez inżynierów społecznych do zaszczepienia jej w umyśle celu. Zawierają:

* Jasne cele: Jest to zdefiniowane tak, aby cel mógł bezradnie znaleźć się pod kontrolą inżyniera społecznego; on lub ona musi wyglądać, jakby miał jasne cele podczas starć. Wszystko sprowadza się do powiedzenia, że jeśli skoncentrujesz się na czymś, prawdopodobnie staniesz się tym. Inżynier społeczny ma już ustalone jasne cele i wszystkie mają logiczną strukturę. Cele powinny ułatwić osiągnięcie celu następujące po nich. Dlatego przy każdym zaangażowaniu inżyniera społecznego w cel, na przykład wpadając na niego w kawiarni, będzie już określony cel, a osiągnięcie tego celu ułatwi osiągnięcie innego celu. Żaden cel nie jest samotny; jeśli tak, można go zignorować, ponieważ nie wpłynie to na powodzenie ataku.

* Relacje : Relacja została zbudowana, aby zapewnić, że cel ufa inżynierowi społecznemu. Aby zbudować relację, która pozwoli socjologowi przekonać cel, inżynier społeczny musi rozumieć umysł celu. Istnieją różne tryby myślenia, które zostały omówione w poprzedniej sekcji. Są bardzo ważne w budowaniu tej relacji.

* Dostrajanie się: inżynierowie społeczni są zawsze świadomi siebie i swojego otoczenia. Dzięki temu inżynier społeczny może mieć widok zewnętrzny i odnotowywać, kiedy atak porusza się lub nie porusza się zgodnie z oczekiwaniami. Jest to niezbędne dla każdego inżyniera społecznego, który chce być bardzo przekonujący, aby być mistrzem zarówno oglądania, jak i słuchania. Inżynier społeczny jest również człowiekiem i naturalnie będzie przekazywał cel lub komunikację. Jednak inżynier społeczny powinien być w stanie zamaskować prawdziwe mimikę twarzy, gesty, mikroekspresje, a nawet ich tempo oddychania i zastąpić je fałszywymi zgodnie z postępem ataku. Dlatego inżynier społeczny powinien nauczyć się obserwować te sygnały jako podmiot zewnętrzny i oceniać swój apel do celu. Powinien on być świadomy niewerbalnych wskazówek podawanych przez ciało i dostosowywać je do warunków ataku. Ta świadomość umożliwi mu nieustanne apelowanie do celu.

* Elastyczność: Perswazja nie jest gwarantowaną metodą dotarcia do celu. Nie jest to reakcja chemiczna, w której pewne reagenty prowadzą do określonego wyniku lub roztworu. Czasami, nawet przy najlepszych trikach, cel może nie wydawać się przekonany . Może to wezwać inżyniera społecznego do wycofania się ze skryptu ataku i wymyślenia innych sztuczek, które mogą ostatecznie pozyskać cel. Dlatego też planowanie z wyprzedzeniem nie zawsze gwarantuje, że atak zadziała, a w wielu przypadkach inżynier społeczny będzie musiał dostosować swoje metody.

* Wzajemność: jest to jedna z powszechnie stosowanych taktyk przekonywania celów. Wzajemność w tym kontekście odnosi się do cechy celu, który chce spłacić przysługę inżyniera społecznego. Ludzie są przyzwyczajeni do tego, że wzajemność odbywa się prawie nieświadomie. Jest to sztuczka używana do nieświadomego kontrolowania umysłów ludzi, aby robić rzeczy na czyjąś korzyść. Na przykład firma farmaceutyczna, która przychodzi i daje pracownikom szpitala bezpłatne rzeczy, takie jak ubrania, długopisy, książki i czapki, nie robi tego na próżno. Wie, że jeśli chodzi o wybór leku dla pacjentów, pracownicy będą chcieli odwzajemnić przysługi i ostatecznie wybrać leki firmy w stosunku do innych. Wzajemne działanie działa tak samo jak inżynieria społeczna. Wynika z czterostopniowego cyklu, który omówiono w następujący sposób:

* Na początku inżynier społeczny rozdaje coś cennego

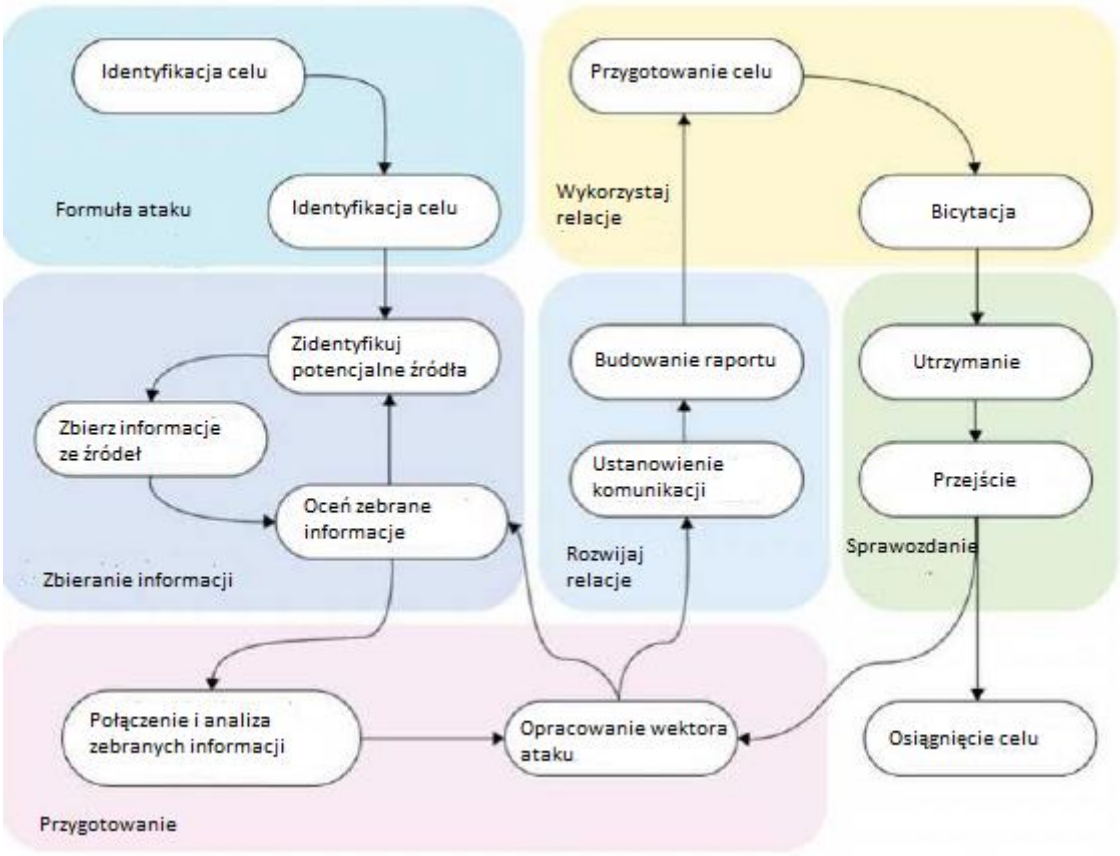
* Cel, który go otrzymuje, ma poczucie długu

* Po pewnym czasie inżynier społeczny złoży proste zapytanie

* Cel będzie bardziej niż chętny do spełnienia tego żądania

Dzięki temu inżynier społeczny zyskuje kontrolę nad mózgiem celu. Jest to bardzo cenna taktyka dla każdego inżyniera społecznego. Utrzymuje atak w ruchu i zapewnia, że cel jest ustawiony w pozycji, w

której on lub ona może jedynie wspierać postęp ataku. Jak wspomniano, nie zawsze może się to powieść zgodnie z oczekiwaniami, dlatego we wszystkich próbach perswazji powinny istnieć plany tworzenia kopii zapasowych. Mapa drogowa inżynierii społecznej jest pokazana na poniższym rysunku:



Narzędzia stosowane w inżynierii społecznej

Inżynierię społecznąa najlepiej jest przeprowadzać za pomocą narzędzi, aby zbliżyć inżyniera społecznego do sukcesu. Należy zauważyć, że samo posiadanie lub dostęp do narzędzi nie wystarczy; należy zrozumieć wewnętrzne szczegóły tego, jak skutecznie z nich korzystać. Że wiedza to różnica między sukcesem a porażką. Istnieją dwie główne kategorie narzędzi stosowanych w inżynierii społecznej - fizyczne i oparte na oprogramowaniu. Narzędzia socjotechniczne stanowią zwykle mile widziane uzupełnienie, ponieważ uzupełniają ręczne działania inżyniera społecznego.

Narzędzia fizyczne

Narzędzia fizyczne odnoszą się do wszystkich narzędzi wykorzystywanych do ułatwienia ataku socjotechnicznego, który nie wymaga użycia komputerów. Organizacje i osoby inwestują w środki bezpieczeństwa fizycznego, aby ograniczyć fizyczny dostęp do kilku upoważnionych osób. To jest powód, dla którego domy mają drzwi, a nawet lepiej, są otoczone płotem i bramą. W razie potrzeby inżynierowie społeczni będą musieli przebić się przez wszystkie fizyczne systemy bezpieczeństwa, które wprowadziły ich cele. Istnieje wiele fizycznych narzędzi, które są następujące:

* Narzędzie do otwierania zamków: służy do uzyskiwania dostępu do miejsc, których dostęp jest blokowany przez zamki. Otwieranie zamków działa na bardzo wielu zamkach i dlatego wciąż jest dużym zagrożeniem. Organizacje reagują na otwieranie zamków za pomocą bardziej skomputeryzowanych fizycznych kontroli dostępu, takich jak magnetyczne karty identyfikacyjne. Zaskakujące jest, w jaki sposób organizacje będą chronić sprzęt za tysiąc dolarów za pomocą zamka o wartości 30 USD.

* Pchnięcie nożem: To narzędzie służy do uzyskiwania dostępu do drzwi z zamkami. Wiele domów i serwerowni będzie miało tego rodzaju drzwi, a najlepszym narzędziem do włamania się do nich jest pchnięcie nożem. Wsuwa się na miejsce i zwalnia zatrzask. Robi to bez uszkadzania drzwi.

* Klucz uderzeniowy: Blisko spokrewnionym narzędziem jest klucz uderzeniowy, który jest specjalnym kluczem, który ma zęby zaprojektowane tak, aby uderzały w kołki zamka, powodując ich przesunięcie do prawidłowego ustawienia i umożliwienie obrotu wtyczki. Podobnie nie uszkadza zamka.

Wszystkie narzędzia używane do uzyskania fizycznego dostępu są zwykle używane, aby umożliwić inżynierowi społecznemu dostęp do niektórych przedmiotów lub informacji, które albo finalizują atak, albo pomagają w jego przeprowadzeniu. Na przykład inżynier społeczny, który doprowadził cel do momentu ujawnienia tajnego pokoju w domu, który zawiera skrzynię pełną klejnotów, użyje tych narzędzi do sfinalizowania ataku i kradzieży klejnotów.

Narzędzia programowe

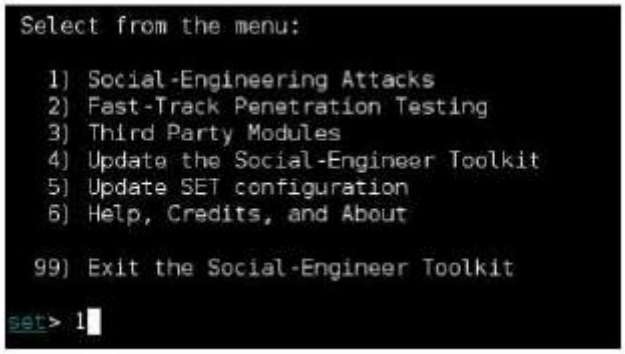
Narzędzia inżynierii społecznej oparte na oprogramowaniu to takie, które wymagają użycia komputerów. Należy zauważyć, że są to narzędzia, które można wykorzystać do wielu innych celów, nie tylko inżynierii społecznej. W rzeczywistości inżynierowie społeczni pożyczają niektóre z tych narzędzi, które są omawiane w następujący sposób, przez ludzi takich jak szpiedzy:

GPS tracker: Jednym z nich jest GPS tracker. Czy istnieje lepszy sposób na przypadkowe zderzenie z celami niż śledzenie wszystkich ich ruchów i wiedza, gdzie dokładnie je znaleźć? Dobrym przykładem jest SpyHawk o wartości 200 USD, który magnetycznie utknął w samochodzie celu i wykorzystuje GPS do odesłania dokładnych współrzędnych pojazdu. Obecnie większość narzędzi inżynierii społecznej opartych na oprogramowaniu jest dostępna online. Mogą zbierać informacje o celu ze źródeł internetowych.

Maltego: Jest to strona internetowa, która kataloguje między innymi informacje o domenach, adresach IP, organizacjach i ludziach. To spełnienie marzeń każdego inżyniera społecznego. Maltego jest w stanie zebrać najdrobniejsze informacje dotyczące osoby, w tym recenzje napisane w mniej znanych sklepach e-commerce. Może znaleźć informacje o osobie, członkach rodziny, krewnych, bliskich przyjaciołach i tak wielu innych szczegółach, że łatwo będzie znaleźć słabość do trafienia w cel. Z perspektywy inżyniera socjalnego głównym celem jest zaoferowanie celowi oferty, której nie może odrzucić. Naturalna chciwość zajmie się resztą i wkrótce cel będzie błagał o ofertę:

* Social Engineer Toolkit (SET): Jak sama nazwa wskazuje, SET zawiera zestaw narzędzi, z których socjotechnik może korzystać w wielu atakach. Zasadniczo zestaw służy do tworzenia złośliwych plików, które można przesyłać pocztą e-mail do celów docelowych. Głównym celem jest zainfekowanie urządzenia docelowego złośliwym oprogramowaniem, którego można użyć do zebrania większej ilości informacji lub do wyrządzenia szkodliwego uszkodzenia na urządzeniu. SET jest podstawowym narzędziem wykorzystywanym w atakach łowiectwa podwodnego. Gdy wiadomość e-mail celu jest znana, SET pozostaje do wyczarowania zaklęcia: pliku, który zaatakuje cel po pobraniu i otwarciu. Zestaw służy również do klonowania stron internetowych i hostowania ich. Może sklonować Facebooka i wysłać celowi link umożliwiający uwierzytelnienie Facebooka, a gdy cel wprowadzi poświadczenia, błąd zostanie wyrzucony z powrotem. Ta technika jest używana do masowego gromadzenia informacji, szczególnie w przypadku poświadczeń używanych w systemach e-mail i bankowości internetowej.

Inne narzędzia oparte na oprogramowaniu to między innymi spoofery i narzędzia do profilowania haseł. Zrzut ekranu SET z Kali Linux wygląda następująco:



Przykłady inżynierii społecznej z Hollywood

Naprawdę trudno nie zakochać się w podstępach inżyniera społecznego; może być krępujące, o ile dzieje się to z kimś innym. Filmy to świetne zasoby, które pomogą Ci lepiej zrozumieć inżynierię społeczną. Oto moje trzy najlepsze filmy z Hollywood, które mogą pomóc ci zobrazować i dowiedzieć się, jak działa inżynieria społeczna:

Naciągacze (2003)

Naciągacz Roy i Frank zaczynają oszustwo, dzwoniąc do ofiar i próbując sprzedać swoim klientom systemy filtracji wody za setki dolarów, które były dostępne za jedyne 50 USD w rzeczywistych sklepach. Dwaj nacigacze używają wielu klasycznych ruchów inżynierii społecznej, takich jak przekazanie telefonu Frankowi Royowi, który udaje szefa Franka, nadanie operacji większej wiarygodności i zabawa umysłem ofiary, aby wszystko było bardziej realistyczne i zyskało zaufanie ofiary. W historii jest wiele innych technik inżynierii społecznej. Jest to dobry sposób na wizualizację niektórych technik, o których przeczytasz w tej książce.

Złap mnie, jeśli potrafisz (2002)

Opiera się to na historii życia Franka Abagnale, który jest jednym z najbardziej niesławnych inżynierów społecznych. Swoją podróż rozpoczął jako nastolatek. Abagnale uciekł z domu i udał, że jest pilotem Pan Am i oszukuje tysiące kilometrów darmowych lotów po świecie, dzięki czemu ludzie wierzą, że był prawdziwym pilotem. To nie wszystko. Abagnale udawał również, że jest lekarzem i nauczycielem, zanim został złapany przez FBI (lata później). Film jest dobrym przykładem tego, jak inżynieria społeczna jest sztuką hakowania ludzi i jak podatni jesteśmy na niebezpieczeństwo.

Ocean's Eleven (2001)

Danny Ocean (George Clooney) i jego 11 wspólników planowali jednocześnie obrabować trzy kasyna w Las Vegas. Pan Ocean i jego wspólnicy korzystali z inżynierii społecznej, sprytów technicznych i strategicznie rozmieszczonych pracowników, aby przeniknąć do kompleksowego, najnowocześniejszego systemu bezpieczeństwa Bellagio i uciekać za 160 milionów dolarów. Pod tym względem nawet najlepsza ochrona nie mogła uodpornić organizacji na penetrację przez skoordynowanych przeciwników.

Porady

Rozważ następujące wskazówki:

* Nie ma łaty na ludzką głupotę lub, innymi słowy, zawsze istnieje sposób na manipulowanie ludźmi. W rezultacie Ty lub Twoi pracownicy jesteś najtrudniejszym i największym zasobem, który musisz chronić.

* Często przeprowadzaj sesję uświadamiającą użytkownika. W szkoleniach z zakresu inżynierii społecznej zawsze jest miejsce na poprawę.

* Nie udostępniaj nikomu niczego poufnego. Pamiętaj, że gdy tajemnica zostanie poznana przez dwie osoby, nie jest już tajemnicą.

* Jeśli nie masz pewności, postępuj ostrożnie.

* Zapewnij bezpieczeństwo fizyczne.

* Klasyfikuj informacje przed atakami zrzucania śmieci. Nawet duże korporacje stosowały tego rodzaju ataki w przeszłości.

* Należy pamiętać, że w oparciu o ISACA w 2016 r. inżynieria społeczna była, w 52%, największym zagrożeniem dla organizacji cybernetycznych.

Podsumowanie

Przegląd inżynierii społecznej przedstawiony tutaj wykazał, że istnieje wiele aspektów tego rodzaju ataku. Obejmują one od sztuczek umysłu i taktyk perswazji po internetowe narzędzia inżynierii społecznej oparte na oprogramowaniu. Przegląd ujawnił ważną świadomość, że ludzkie słabości można wykorzystać. Ludzki mózg może zostać zhackowany tak samo jak komputery. Umożliwia to inżynierom społecznym manipulowanie ludźmi w celu podjęcia działań, których normalnie by nie podjęli. Wprowadzenie wprowadziło pewien poziom świadomości na temat możliwości inżynierów społecznych, od czytania w myślach po śledzenie ruchu za pomocą lokalizatorów GPS. W przyszłych częściach omówimy je bardziej szczegółowo. Pod koniec ostatniej części zapalony czytelnik nabywa umiejętności inżynierii społecznej, które najprawdopodobniej zostaną wykorzystane w nauce myślenia inżynierów społecznych, abyś mógł się przed nimi chronić.