Preteksty

Pretekst jest aktem przedstawiania się jako ktoś inny z zamiarem zmuszenia innych do podania poufnych informacji lub wykonania prośby. Chodzi o coś więcej niż mówienie kłamstw o tym, kim jesteś, ale o bycie osobą, za którą się podajesz. Preteksty dają inżynierom społecznym szereg bodźców, których w innym przypadku nie lubiliby, zachowując się jak oni. Inżynier społeczny zechce zmienić wszystko o sobie, by pasowało do pretekstu. Sposób mówienia, chodzenia, ubierania się, używania mimiki i gestów musi dokładnie odpowiadać ich pretekstowi. Dla wielu preteksty mogą wydawać się tak proste, jak zmiana wyglądu fizycznego. Jest jednak głębszy. Pretekst jest bardziej nauką. Osoba przyjmie zupełnie inną osobowość, która czasami jest w konflikcie z prawdziwą osobą głęboko w środku. Dlatego preteksty muszą być doskonale zaplanowane, aby uniknąć konfliktu między osobowością, aby zająć centralne miejsce podczas ataku, a tym samym zniweczyć jego szanse na odniesienie sukcesu. W tej części omówione zostaną aspekty pretekstu, jak to jest zaplanowane i jak najlepiej je wykonać, umożliwiając lepszą obronę przed nim. Należy tego dokonać w następujących tematach:

* Zasady pretekstu

* Udane preteksty

* Zagadnienia prawne związane z pretekstem

* Narzędzia do ulepszania pretekstów

Wprowadzenie

Pretexting polega na stworzeniu scenariusza mającego na celu przekonanie lub zmanipulowanie celu w celu uzyskania pewnych informacji lub spełnienia innych żądań. Inżynier społeczny przyjmie pretekst, który idealnie wpasowuje się w stworzoną sytuację i użyje tego pretekstu, aby doprowadzić cel do spełnienia żądań. Bez utworzonego scenariusza lub użycia pretekstu cel nie byłby zgodny. W inżynierii społecznej preteksty wykonuje się głównie w celu podszywania się pod osoby pełniące określone role w pracy, która daje im przywilej zamawiania lub prosić innych o zrobienie pewnych rzeczy. Na przykład pomoc techniczna w organizacji może poprosić użytkownika o podanie niektórych informacji związanych z komputerami. Dlatego nie może być zaskoczeniem, gdy użytkownik zostanie poproszony o podanie swojego hasła w celu jego zmiany. Chociaż prośba o hasło może wydawać się dziwna, fakt, że został złożony przez dział pomocy technicznej, zmienia wiele rzeczy i czyni użytkownika bardziej zgodnym. Nastąpił wzrost liczby inżynierów społecznych, w których pośredniczą ataki pod pretekstem, szczególnie po pojawieniu się bezpłatnych osobistych wiadomości e-mail. Jednym z przykładów, który zwrócił uwagę samej firmy, jest wiadomość e-mail z problemami z dostawą FedEx. Wiadomość e-mail ogólnie informuje użytkownika, że firma nie była w stanie dokonać dostawy paczki i użytkownik musi natychmiast skontaktować się z kierownikiem dostawy. Podawany jest złośliwy link, a czasami kontakty z fałszywymi menedżerami dostaw, którzy będą żądać od użytkowników poufnych informacji, wyłudzać pieniądze lub zainfekować komputer użytkownika złośliwym oprogramowaniem. Aby wyjaśnić fragment pretekstu tego ataku, użytkownik znajduje się w scenariuszu, w którym jest bardziej zgodny z instrukcjami podanymi przez atakujących. Jeśli użytkownik chce skontaktować się z osobą, która twierdzi, że pochodzi z FedEx, podane e-maile lub numery telefonów będą zawierały osoby atakujące, które będą pod pozorem prawdziwych pracowników FedEx. W ten sposób cel poczuje się bardziej komfortowo, ujawniając swoje poufne dane, takie jak SSN, a nawet posuwając się do tego, że przesyła pieniądze atakującym. Istnieje wiele innych wersji tego ataku, które atakujący zmienią tylko nazwy firmy, dla której twierdzą, że pracują. Czasami są tak dobrzy, że mogą oszukać kogoś, nie wzbudzając żadnych podejrzeń, że nie są tymi, za których się podają.

Dzięki technologii posiadają narzędzia, które mogą replikować wiadomości e-mail i strony internetowe należące do rzeczywistych firm, dzięki czemu preteksty wyglądają realnie. Preteksty są wybierane przez inżynierów społecznych w zależności od celu lub zadania. Niektóre zadania są proste; dlatego zostaną wybrane łatwe do osiągnięcia preteksty. Jednak niektóre zadania są złożone i inżynierowie społeczni będą musieli zadowolić się złożonym pretekstem, aby wykonać zadanie. Na przykład, jeśli celem jest użytkownik w organizacji, a celem jest uzyskanie hasła, pretekst jest dość prosty. Wszystko, co jest konieczne, to sfałszowany e-mail i przekonujące umiejętności pisania. Utworzony pretekst musiałby wskazywać, że wiadomość e-mail pochodzi z działu IT i że udostępnienie hasła jest pilne. Jeśli jednak misją jest kradzież dokumentów o wysokim stopniu tajności od dobrze zabezpieczonej organizacji, pretekst, który należy zastosować, będzie musiał być złożonym pretekstem, aby uzyskać te informacje.

Zasady i planowanie pretekstu

Pretekst, podobnie jak każda inna umiejętność, ma pewne zasady, które przy dobrych zastosowaniach osiągają dobre wyniki. Te zasady stosują inżynierowie społeczni za każdym razem, gdy muszą uciekać się do pretekstu, i zawsze się opłacają. Rzućmy okiem na niektóre z nich.

Robienie badań

Sukces pretekstu można bezpośrednio przypisać ilości czasu poświęconego na jego badanie. Im bardziej inżynier społeczny jest informowany o pretekście, tym większe są szanse, że zadziała. Odwrotna sytuacja jest również prawdą, ponieważ im mniej inżynier społeczny wie o pretekście, tym większe są szanse na błędy, a ostatecznie na niepowodzenie pretekstu. Duża część badań będzie polegać na określeniu zainteresowań i powiązań celu. Umożliwi to socjologowi stworzenie idealnego scenariusza dla pretekstu i także decydować o pretekście osobowości, który należy przyjąć. Ludzie mają kilka słabości i są ściśle związani ze swoją osobowością. Te słabości będą wyszukiwać i wykorzystywać inżynierowie społeczni. Czasami tylko niewielka część informacji o celu może mieć ogromne znaczenie. Przeszłe wydarzenia z życia celu, posiadane przedmioty, ulubione marki, preferencje zakupów i wysyłki oraz powiązania celu mogą skutecznie znaleźć słaby punkt, z którego można wykonać atak pod pretekstem. Na przykład cel, który przyczynia się do organizacji charytatywnej, może zostać zaatakowany przez inżynierów społecznych, którzy tworzą pretekst na tych samych podstawach. Pretekstem będzie musiała być duża organizacja charytatywna z obecnością w sieci i mediach społecznościowych, aby pomóc celowi zweryfikować jej istnienie. Na tej podstawie inżynier społeczny będzie musiał dotrzeć do celu, szukając pomocy finansowej. W ten sposób cel zostanie przekonany o istnieniu fundacji charytatywnej i przekaże pokaźną darowiznę na cele charytatywne, tak że pieniądze trafią do prywatnych kieszeni. Emocje są silnie wykorzystywane pod pretekstem. Dotarcie do celu jest łatwe, jeśli inżynier społeczny może bawić się swoimi emocjami. W dość smutnej manipulacji emocjami inżynierowie społeczni skorzystali z trzęsień ziemi na Haiti w 2010 r., które spotkały się z ogólnoświatowym zainteresowaniem, a artyści z całego świata starali się szerzyć świadomość i zbierać fundusze dla ofiar. Było też wiele innych organizacji charytatywnych, które robią to samo, próbując pozyskać fundusze od darczyńców, aby pomóc ofiarom trzęsienia ziemi. Jednak inżynierowie społeczni wykorzystali sytuację i stworzyli pretekst, który działał skutecznie. Byli tacy, którzy tworzyli fałszywe strony charytatywne i reklamowali je. W końcu wzbogacili się z dochodów z tego złego czynu, ponieważ było bardzo wielu chętnych dawców. Jednak istniała inna grupa inżynierów społecznych, którzy założyli witrynę, która, jak twierdzili, miała nazwiska osób zagubionych w tragedii. Jednak ich witryna była złośliwa i gromadziła tylko dane osobowe osób, które się na niej zapisały, a także rozprzestrzeniała niektóre złośliwe oprogramowanie na urządzenia, które odwiedzały witrynę. Szkodniki te były później wykorzystywane do hakowania i kradzieży większej ilości informacji od osób, które odwiedziły takie witryny. Jest wysoce prawdopodobne, że ten sam rodzaj pretekstu może się dziś powtórzyć, jeśli podobna tragedia na dużą skalę spotka ludzi. Istnieje zwiększona wiedza na temat algorytmu

indeksowania witryn Google, który umożliwia optymalizację witryn w celu uzyskania wyższej pozycji w wynikach wyszukiwania niektórych słów kluczowych. Inżynierowie społecznościowi mają już dostęp do technik optymalizacji swoich witryn pod kątem wyszukiwarek, takich jak Google. W związku z tym mogą szybko wymyślić witrynę i podnieść ją w rankingu wyników wyszukiwania związanych ze słowami kluczowymi, takimi jak katastrofy, akcje charytatywne lub darowizny. Niewinni ludzie mogliby z łatwością przekazać pieniądze na nieistniejące organizacje charytatywne w przypadku kolejnej katastrofy podobnej do Haiti. Z dyskusji na temat tej zasady zauważyłeś siłę dobrych badań. Przy wystarczającej ilości informacji można łatwo ustawić skuteczny pretekst. W przykładzie na Haiti, choć jest to bardzo smutne, widać, że doskonały pretekst zawsze działa, szczególnie gdy jest połączony z pewnymi emocjami. Weszli inżynierowie społeczni za stronami charytatywnymi na Haiti na wielkie głębiny, aby stworzyć nieistniejące podmioty w Internecie i skonfigurować ich obecność w sieci i mediach społecznościowych, aby przyciągać darczyńców. Wiedzieli, czego szukają dawcy, i dali im dokładnie to. Dzięki odpowiednim informacjom łatwo jest uzyskać udany pretekst.

Hakowanie Google

Hakowanie Google to technika, która wykorzystuje wyszukiwarkę Google, aby pomóc Ci znaleźć potrzebne informacje ukryte w Internecie. Polega na użyciu określonych ciągów tekstu w celu znalezienia wyników. Dla inżynierów społecznych ta technika to kopalnia złota. W oparciu o CSO online FBI wydało publiczne ostrzeżenie przed tym bardzo dobrze znanym problemem. Ostrzeżenia FBI informują agencje, że hakerzy / inżynierowie społecznościowi wykorzystają hakowanie Google do zlokalizowania informacji, których organizacje nie zamierzały być wykrywalne przez społeczeństwo lub aby znaleźć luki w zabezpieczeniach witryn internetowych do wykorzystania w kolejnych cyberatakach.

Moc hakowania Google

W 2013 roku, certyfikowany haker etyczny, znalazł kilka bardzo interesujących szczegółów zeskanowanych do Internetu, takich jak australijskie paszporty, prawa jazdy, akty urodzenia i wiele innych poufnych danych. Opublikował wyciek na swoim blogu po usunięciu treści z witryny będącej w połowie własnością rządu. Oczywiście wszystkie obrazy zostały zamazane, aby chronić ofiary, a ten post osiągnął ponad 20 000 kliknięć w ciągu tygodnia, miał wiele retweetów, a to zostało opublikowane w wielu e-mailach. Poniżej znajduje się dobry dowód na to, dlaczego powinniśmy być bardzo ostrożni, dzieląc się naszym identyfikatorem. Omówmy kilka przydatnych ciągów wyszukiwania Google, które mogą pomóc Ci znaleźć potrzebne informacje

Google hakowanie tajemnic

Napisano wiele książek na temat korzystania z tej potężnej umiejętności, ponieważ można się domyślić, że jest to bardzo duży temat, ale zróbmy podsumowanie hakowania Google, aby pomóc Google znaleźć to, czego dokładnie potrzebujesz.

Operatory

Jak większość z was wie, jestem pewien, że Google również wie, które to operatory:

* intitle: pokaże tylko te strony, które mają termin w tytule HTML. intitle: „strona logowania” zwróci wyszukiwane hasła, które w tytule zawierają termin strona logowania

* allintitle: wyszuka wszystkie określone terminy w tytule. Dla przykładu, indeks allintitle / admin

* inurl: spowoduje wyszukanie określonego terminu w adresie URL. Na przykład, inurl: „login.php”:

* filetype: Wyszukuje określone typy plików. filetype: pdf wyszuka pliki PDF na stronach internetowych. Załóżmy, że szukasz plików socjotechniki, a następnie wpisz to zapytanie - typ pliku: pdf „socjotechnika”:

* intext: Przeszukuje zawartość strony. Jeśli chcesz znaleźć indeks adresów, po prostu dodaj adres na końcu. Na przykład intext: „index of /”:

* site: ogranicza wyszukiwanie tylko do określonej witryny.

* link: użycie tego w zapytaniu pokaże wszystkie wyniki, które prowadzą do tego adresu URL.

* cache: Będąc jednym z najskuteczniejszych zapytań, pamięć podręczna zwróci wyniki prowadzące do stron w pamięci podręcznej przechowywanych przez Google.

Możesz łączyć wyszukiwane hasła i znajdować możliwie wszystko, co jest ukryte w Google. Oto przykład:

site:com filetype:xls "membership list"

To zapytanie będzie wyglądać w każdej witrynie internetowej .com, która ma pliki Excel o nazwie listy członkostwa i odzyska wynik. Jako inżynier społeczny może to być bardzo przydatne, aby dowiedzieć się więcej o swoim celu.

Jeśli chcesz, możesz nawet przeszukiwać wojskowe strony internetowe, a nawet pliki niejawne na własne ryzyko

Korzystanie z osobistych zainteresowań

Preteksty muszą być zakorzenione w osobie, która ich używa, a tym samym pomaga wykorzystać niektóre atrybuty, które osoba już ma. Aby zwiększyć wiarygodność pretekstu, inżynierowie społeczni często korzystają z ich osobistych zainteresowań. Interesy osobiste są silne i mogą sprawić, że ktoś będzie wyglądał bardziej autentycznie i autentycznie, nawet pod pretekstem. Na przykład inżynier społeczny, który jest entuzjastą technologii, może z łatwością przyjąć pretekst technika IT. Zainteresowanie i wiedza na tematy związane z technologią, takie jak cyberprzestępstwa, złośliwe oprogramowanie, wektory ataków i polityki bezpieczeństwa, odegrają pewną rolę w przekonaniu celu, że rzeczywiście współpracują z technikiem IT. Jeśli osoba, która prawie nic nie wie o IT, przyjmuje ten sam pretekst, atak może zakończyć się niepowodzeniem. Na przykład po wyświetleniu monitu o podanie hasła do aktualizacji cel może zadać kilka dalszych pytań. Jednym z nich może być powód, dla którego technik IT chce otrzymać stare hasło, aby je zmienić zamiast bezpośrednio zmieniać z aktywnej domeny. W przypadku osoby, która nie zna się na tym żargonie, atak może zakończyć się niepowodzeniem w tym momencie. Jednak specjalista w tej dziedzinie może wymyślić pretekst i może powiedzieć, że komputer docelowy wydaje się być odłączony od domeny organizacji. Osobiste zainteresowania dają inżynierom społecznym więcej rzeczy do powiedzenia i lepsze wymówki. To z kolei buduje relacje i zaufanie między inżynierem społecznym a celem. Różne preteksty będą jednak wymagać od inżyniera społecznego posiadania różnego rodzaju wiedzy. Najlepiej jest dopasować pretekst do rzeczy, które są już przedmiotem osobistego zainteresowania lub do rzeczy, o których inżynier społeczny już się mówi. Głównym celem jest upewnienie się, że inżynier społeczny ma coś, o czym swobodnie rozmawia, co bezpośrednio wiąże się z pretekstem. Jest to dobre dla pewności i ogólnego odwołania inżyniera społecznego do celu. Istnieją pewne wyzwania, kiedy inżynier społeczny wybiera pretekst, który bezpośrednio koliduje z jego osobistymi interesami. Jest to problem psychologiczny, który można wyjaśnić teorią dysonansu poznawczego autorstwa Leona Festingera. Teoria twierdzi, że ludzie zawsze dążą do konsekwencji w swoich przekonaniach, opiniach i poznaniu.

Kiedy pojawia się niespójność w ich postawach lub zachowaniach, musi nastąpić konsekwentna zmiana, aby usunąć niespójność. Festinger zauważył, że aby wyeliminować niekonsekwencję poznawczą, należałoby zmniejszyć znaczenie niespójnych przekonań, dodać bardziej spójne przekonania lub zmienić niespójne przekonania, aby były spójne. Aby zastosować tę teorię w praktyce, zbadajmy ją w świetle ataku inżynierii społecznej. Ilekroć inżynier społeczny przyjmuje pretekst sprzeczny z jego przekonaniami, zainteresowaniami i postawami, pojawia się niespójność lub dysonans. Ta niespójność stwarza problemy w mózgu inżyniera społecznego, które mogą prowadzić do niepowodzenia w budowaniu relacji i zdobywaniu zaufania do celu. Problemy te muszą zostać rozwiązane przy użyciu niektórych sposobów, które stwierdził Festinger. Jednym z nich jest zdobycie większej liczby przekonań, które są spójne. Inżynier społeczny może potrzebować więcej badań na temat przekonań dotyczących wybranego pretekstu, aby zdobyć więcej wiedzy, która jest zgodna z pretekstem, dzięki czemu wydaje się znajomy i nie dysonansowy. Istnieje również inna opcja zamiany niekonsekwentnego przekonania na konsekwentne. Jest to jednak trudne, ponieważ pretekst nie powinien odwoływać się do inżyniera społecznego, ale do celu. Dlatego inżynier społeczny nie może zdecydować się na działanie poza wytycznymi swojego pretekstu, aby nie czuł się niekomfortowo. W większości przypadków wybrany pretekst ściśle pasuje do przekonań, postaw, zachowań i działań celu. Dlatego inżynier społeczny może kształtować się tylko w celu spełnienia oczekiwań pod pretekstem.

.Ćwiczenie dialektów

Niektóre preteksty mogą obejmować użycie niektórych dialektów z kilku powodów. Ciekawą statystyką w branży marketingowej jest to, że prawie 75% Amerykanów uwielbia brytyjskie akcenty. Dlatego chętnie wysłuchają, co mają do powiedzenia ludzie z takimi akcentami. Niektóre preteksty mogą wymagać od inżyniera społecznego odwołania się do celu przy użyciu takiego akcentu. Problem polega na tym, że łatwo jest stwierdzić, kiedy ktoś udaje akcent. Jeśli zostanie to wykryte, cel może być zaniepokojony, a szanse powodzenia ataku mogą drastycznie spaść. Weźmy przykład inżyniera społecznego, który prosi o cenne prototypy określonego produktu, który zamierza wykorzystać w brytyjskiej organizacji. Może komunikować się z celami za pośrednictwem wiadomości e-mail, której punkty domeny należą do brytyjskiej firmy. Jeśli chodzi o połączenia głosowe, brytyjski akcent pomoże podkreślić, że inżynier społeczny jest w Wielkiej Brytanii. Wykrywanie, że inżynier społeczny próbuje za bardzo, będzie trudne i trudno mówić z brytyjskim akcentem. Może to doprowadzić do ponownego przemyślenia celu przez inżyniera społecznego. Na szczęście inżynierowie społeczni mają szczęście, że istnieje sposób na przyjęcie akcentu. Przemysł filmowy robi to cały czas. Aktorzy mają trenerów dialektu, którzy są wynagradzani, aby nauczyć ich mówić z pewnym akcentem. W 2012 roku ukazał się film o nazwie The Dictator, który w tym roku znalazł się na szczycie rankingów filmowych ze względu na ilość kreatywności i humoru. Ważny w tym temacie jest główny aktor, admirał generalny Alladin, lider wymyślonego kraju Bliskiego Wschodu o imieniu Wadiya. Aktorem tej roli był Sacha Baron Cohen. W tym filmie miał silny akcent na Bliskim Wschodzie, a niedoinformowany widz nigdy nie zgadłby, że Baron nie pochodzi z Bliskiego Wschodu. Jest Anglikiem, urodził się w Londynie i ma brytyjski akcent. Jednak w przypadku tego filmu musiał zostać przeszkolony do mówienia z innym akcentem i udało się. Oznacza to, że dialektu można się nauczyć, a jeden nie jest ograniczony do dialektu nabytego podczas dorastania. Inżynierowie społeczni nie zawsze będą jednak mieli do dyspozycji wystarczającą ilość pieniędzy, aby zatrudnić trenera dialektów. Dlatego muszą polegać na innych sposobach osiągnięcia tego samego celu, nie wydając tak dużo. Istnieje kilka kroków, które można podjąć, aby nauczyć się akcentu. Są to:

* Uczenie się od tubylców: Najlepszym sposobem na zdobycie akcentu jest język ojczysty. Słuchając native speakera i stale próbując dopasować jego wymowę, można uzyskać akcent mówiącego. Nie

trzeba mieć przyjaciela lub krewnego z pożądanym akcentem ani podróżować do miejsca, w którym są rodzimi użytkownicy. Do pobrania są audiobooki, których można użyć.

* Naśladowanie: Aby uzyskać akcent, najlepiej jest rozmawiać z native speakerem, aby ćwiczyć, jak brzmieć jak on lub ona. Dotyczy to również ćwiczeń z użyciem plików audio. To powoli działa na twoją artykulację i wymowę, a ostatecznie może się okazać, że brzmi dokładnie tak jak oni.

* Nagrywanie i korekta: Nie jest łatwo słuchać siebie podczas mówienia, ponieważ dźwięk, który słyszysz, nie jest dokładnym przedstawieniem tego, co usłyszą inni ludzie. Najlepszym sposobem monitorowania postępów jest nagranie siebie mówionego z pożądanym akcentem, a następnie słuchanie, aby wiedzieć, co poprawić.

* Ćwiczenie z inną osobą: Aby nie wyglądać na tak, jakbyś miał trudności z mówieniem akcentem, najlepiej jest ćwiczyć, jak mówić to naturalnie z inną osobą. Druga osoba nie musi znać akcentu, celem jest zastosowanie akcentu w warunkach rzeczywistych. Umożliwi to skorygowanie widocznych oznak próby mówienia z akcentem, takich jak nienaturalne zawirowania języka i inne oznaki walki podczas wymowy.

* Korzystanie z akcentu publicznie: Dzięki znacznemu postępowi i indywidualnej satysfakcji z rezultatów można wypróbować nowo nabrany akcent publicznie. To zachęci publiczną krytykę lub akceptację akcentu. Inżynier społeczny może skorzystać z tych wskazówek przez kilka miesięcy i uzyskać pożądany akcent. Ten akcent można następnie zastosować do prawdziwych ataków wykorzystujących pretekst.

Korzystanie z telefonów

Z powodu pojawienia się Internetu większość ataków socjotechnicznych przeprowadzana jest online za pośrednictwem wiadomości e-mail i stron internetowych. Moc telefonu została obniżona przez dzisiejszych inżynierów społecznych. Chociaż jednak wielu inżynierów społecznych zalewają Internet różnego rodzaju atakami inżynierii społecznej, ataki telefoniczne są puste. Dla inżyniera społecznościowego najlepszy czas na używanie telefonów do ataków to dziś. Ze względu na bezosobowy charakter Internetu, przekonywanie celu do zrobienia może wymagać więcej wysiłku. Jednak rozmowa telefoniczna nadaje osobisty charakter rozmowie i umożliwia inżynierowi społecznemu wywieranie nadmiernego nacisku na cel, aby przekazać wrażliwe informacje na miejscu. Największym problemem, z którym spotykają się inżynierowie społeczności podczas rozmowy telefonicznej, jest to, że nie ma miejsca na błędy. W przypadku wiadomości e-mail inżynier społeczny może ją edytować tysiąc razy, jeśli to konieczne, aby uzyskać odpowiednią treść. Dzwoniący ma tylko jedną próbę wywarcia pierwszego wrażenia i nie ma już miejsca na poprawianie każdego wydanego oświadczenia. Aby sobie z tym poradzić, inżynierowie społecznościowi muszą ćwiczyć sesje treningowe przed skontaktowaniem się z prawdziwym celem. Sesja ćwiczeniowa pomoże socjologowi dowiedzieć się, co może pójść nie tak podczas rzeczywistego połączenia, i naprawić to. Jeśli nie ma ludzi, do których mógłby zadzwonić, inżynier społeczny mógłby spróbować nagrać siebie nawiązywanego do wyimaginowanego celu, a następnie odsłuchać, aby ustalić, gdzie popełnił błąd. Połączenia telefoniczne mogą służyć do utrwalania pretekstu. W Internecie dostępne są różne dźwięki tła, których można użyć, aby zapewnić celowi, że inżynier społeczny znajduje się w określonym miejscu. Na przykład inżynier społeczny, który twierdzi, że pracuje w witrynie przemysłowej, może po prostu pobrać i odtworzyć dźwięki tła nagrane w witrynie przemysłowej, dzwoniąc do celu. Cel zostanie zapewniony, że dzwoniący rzeczywiście znajduje się na terenie przemysłowym. To samo można replikować dla wielu innych ustawień. Dźwięki w tle są dostępne do pobrania na stronach takich jak Audio Jungle, których można używać podczas połączeń. Słysząc oczekiwane dźwięki, cel łatwo wpada w pretekst. Tego nie da się osiągnąć za pomocą wiadomości e-mail, które pomogłyby odrzucić chmurę

podejrzeń, która niweczy szanse na sukces w ataku inżynierii społecznej. Kolejną zaletą dostępną tylko dla telefonów jest możliwość sfałszowania informacji o identyfikatorze dzwoniącego. Dostępne są łatwo dostępne usługi, takie jak karta fałszowania, która może być użyta do wskazania celom, że osoba dzwoniąca pochodzi z danej lokalizacji. Może to być główna siedziba ważnej firmy, komisariat policji, biuro ubezpieczeń lub bank, a także wiele innych miejsc. Te sfałszowane informacje pomogą celowi szybko zakochać się w pretekstie. Nie ma sensu kłócić się z kimś, kto twierdzi, że jest z banku, gdy prosi o jakieś dane osobowe, prawda? Właśnie to przejdzie przez cele, gdy otrzymają sfałszowane wywołania, które potwierdzą pretekst, który tworzy inżynier społeczny. Wreszcie, jak wspomniano wcześniej, telefon pozwala inżynierowi społecznemu wywierać większy nacisk na cel, aby natychmiast uzyskać poufne informacje. W przypadku wiadomości e-mail użytkownik ma czas na sprawdzenie, czy żądania osób z banku lub ubezpieczenia zdrowotnego są uzasadnione. Łatwo jest odkryć takie ataki. Jednak w rozmowie telefonicznej cel nie ma tego luksusu. Inżynier społeczny spróbuje wykorzystać pilność i konsekwencje, aby doprowadzić cel pod wystarczającą presją, aby przekazać poufne informacje lub spełnić inne żądania. Ponieważ nie ma czasu sprawdzić, czy żądania są uzasadnione, cele często ustępują inżynierom społecznym.

Wybór prostych pretekstów

Pod pretekstem im prościej, tym lepiej. Preteksty oparte są na fabułach, zmyślonych faktach i niektórych nieodłącznych szczegółach. Jest taki punkt, w którym pretekst może uzyskać, że jest po prostu zbyt wiele szczegółów, aby inżynier społeczny mógł je zapamiętać, tak więc pretekst kończy się niepowodzeniem. Jednym z powodów, dla których złapani są inżynierowie społeczni, jest to, że nie są w stanie przypomnieć sobie rzeczy, o których wspominali wcześniej lub gdy ich słowa nie łączą się z tym, co powiedzieli na początku. W ujęciu psychologa, który badał ludzkie oszustwo, dr Ekman napisał artykuł opisujący, w jaki sposób kłamstwa zawodzą w procesie ludzkiego oszustwa. Według niego kłamstwa zawodzą, gdy kłamca nie jest w stanie przewidzieć pytań, które mogą zostać zadane. Nawet jeśli kłamca jest sprytny, istnieją pewne nieoczekiwane zmiany okoliczności, które mogą go zdradzić. Ekman mówi również, że nawet gdy okoliczności się nie zmieniają, kłamca może mieć problemy z przywołaniem swoich kłamstw, a tym samym przyczyną niepowodzenia kłamstwa. Jak można zaobserwować na podstawie obserwacji dr. Paula Ekmana, lepiej jest stworzyć mniejsze kłamstwo lub pretekst, aby nie było wiele rzeczy, które można pomylić. Bardzo drobny błąd można odkryć bardzo skomplikowany pretekst. Dlatego nie warto poświęcać tyle czasu i zasobów, próbując stworzyć coś, co może zawieść w mgnieniu oka. Prostsze preteksty są bardziej optymalne dla inżynierów społecznościowych. Łatwo jest nie tylko stworzyć, ale także wszystko przypomnieć. Dzięki temu inżynier społeczny może wykonać oszustwo pewnie i wyglądać naturalnie. Na przykład, gdy pojawia się przed dyrektorem ds. Bezpieczeństwa jako osoba zajmująca się naprawą sieci w zakontraktowanej firmie, inżynier społeczny, który utrzymuje bardzo mały zakres swojego pretekstu, ma większą szansę na uzyskanie dostępu do serwerowni niż ten, który ma zaporę wymówek, które zostaną wpuszczone do serwerowni.

Chodzi o to, aby mieć i zachować proste fakty. Kiedy pretekst jest zbyt duży lub skomplikowany, jest po prostu zbyt wiele komponentów, z których jeden może się mylić. Cel będzie aktywnie nasłuchiwał podczas ataku, dzięki czemu będzie lepiej przygotowany do wychwytywania niekonsekwencji. Mały pretekst ma kilka zalet. Na początek inżynier społeczny może pominąć luki do wypełnienia przez cel. W ten sposób wyobraźnia celu będzie winna, jeśli później dojdzie do pewnych sprzeczności. Prosty pretekst pozwala także socjologowi go rozwinąć w razie potrzeby. Z drugiej strony trudniej jest zmniejszyć większy pretekst, ponieważ cel uświadamia sobie tak wiele rzeczy, że staje się podejrzliwy, gdy inni są upuszczani bez wyjaśnień. Prosty pretekst usuwa także inżyniera społecznego z pozycji opracowywania. Właśnie w trakcie opracowywania błędów można łatwo popełnić błąd, ponieważ

inżynier społeczny może osiągnąć własny cel, nie będąc w stanie dopasować wcześniej opisanej wersji opowiadania. Weźmy przykład prawdziwego wyjaśnienia tego. Powiedzmy, że jesteśmy inżynierem społecznym, który próbuje dostać się do serwerowni firmy. Możemy użyć umiejętności obserwacji, aby poznać prawdziwą firmę zajmującą się naprawami sieci lub komputerów. Z tego możemy uzyskać ich logo i wydrukować koszule z ich nazwami, logo i hasłami. Oprócz tego moglibyśmy stworzyć odznaki, które odważnie nosimy w dniu ataku. Będzie to bardzo pomocne, zwłaszcza w przypadku pracowników ochrony obsługujących wejście. Większość kontroli fizycznych przy wejściach to ochroniarze. Po wymachiwaniu naszymi odznakami i pełnym odzianiu w koszule opatrzone nazwą firmy, która naprawia, krótkie wyjaśnienie, które mamy ,że zostaliśmy wezwani przez dział IT, można go łatwo kupić i będziemy mieli bezpłatny wstęp do organizacji. W recepcji mogliśmy trzymać się tego samego pretekstu, że zostaliśmy wezwani przez dział IT, aby pilnie sprawdzić problem z jednym z serwerów. W tym momencie recepcjonistka może dać nam dostęp lub zadzwonić do jednego z pracowników działu IT, aby wpuścić nas do serwerowni. Jeśli coś się pojawi, możemy trzymać się prostego pretekstu, dopóki nie wejdziemy do serwerowni

Spontaniczność

Atak socjotechniki nie powinien wydawać się być skryptem; inżynier społeczny powinien mieć swobodę zmiany w zależności od okoliczności. Skryptowy atak będzie wyglądał nienaturalnie i ma większe szanse na porażkę niż na sukces. Skryptowy atak opiera się na idealnych warunkach, podczas gdy atak występuje w warunkach mniej niż idealnych. Cały inżynier społeczny powinien przejść do ataku z konturem lub ramą i pozwolić, aby rzeczy się zgadzały, ale w kontrolowany sposób. Istnieje kilka sposobów spontaniczności na dowolną interakcję z celem. Ponadto sposoby te można wykorzystać w normalnych scenariuszach życiowych, nie tylko w atakach. Są to:

* Nie myślenie o tym, jak się czujesz: jeśli inżynier społeczny myśli o tym, jak się czuje podczas interakcji, atak może się nie powieść. Mózg traci koncentrację na odbywającej się rozmowie i zaczyna zwracać większą uwagę na strach, nerwowość lub lęk, które odczuwa się. To jest przepis na porażkę. Czasami interakcja może przebiegać tak dobrze, że stajesz się nadmiernie podekscytowany. Myślenie o podekscytowaniu wykręca cię z zadania. Tę wskazówkę można wykorzystać podczas wywiadów lub po raz pierwszy interakcji ze specjalnymi ludźmi, szczególnie dla tych, którzy denerwują się w tych scenariuszach. Ignorowanie mieszanki uczuć, które mają miejsce na początkowych etapach interakcji, może uratować je przed zawstydzeniem lub całkowita porażka zamierzonego celu. Inżynier społeczny koncentruje się na celu i celu interakcji. Jeśli celem jest nakłonienie celu do powiedzenia czegoś, nie ma czasu na skoncentrowanie się na swoich uczuciach. Cały wysiłek powinien być poświęcony uważnemu słuchaniu tego, co mówi cel i planowaniu kursu, który powinna odbyć rozmowa.

* Nie traktuj siebie zbyt poważnie: spontaniczność ginie, gdy inżynier społeczny zaczyna zwiększać powagę tego, co robi. Ta nienaturalna powaga rodzi nerwowość i powoduje narastającą presję. Przy tym wszystkim konsekwencje awarii są również spotęgowane. To powoduje, że zaczynasz działać nienaturalnie, starając się doprowadzić wszystko do perfekcji. Przy całej presji, jaką się znajduje, szanse na pomyślne ukończenie misji są niewielkie, ponieważ trudniej jest myśleć prosto. Kiedy coś małego wypada z miejsca, trudno to również przywrócić.

* Identyfikacja odpowiedniego: Ostatnią sztuczką, którą inżynierowie społeczni zastosują, by być spontanicznym, jest zidentyfikowanie w jego otoczeniu rzeczy, które mają znaczenie dla tego, co robi. Podczas interakcji z celem inżynier społeczny powinien skoncentrować się na reakcji celu, mikroekspresji i mowie ciała, aby ocenić, jak dobrze przebiega interakcja. Zamiast próbować skupić się i wymyślić kolejne 10 kroków po interakcji, należy zwrócić większą uwagę na otoczenie wokół niego. Pomaga nam przekazywać komentarze i informacje zwrotne, gdy cel mówi, więc wierzy, że inżynier

społeczny jest na tej samej łodzi. Ludzie mogą łatwo stwierdzić, kiedy osoba, z którą rozmawia, nie słucha. To sprawia, że czują się nieważni i najprawdopodobniej mogą zakończyć rozmowę.

* Praktyka: W tych wskazówkach dla inżynierów społecznych nie można kłaść większego nacisku niż ćwiczenie. Nie jest powiedziane, że samo przeczytanie tych wskazówek sprawi, że opanujesz sztukę rozpoczynania i prowadzenia rozmów. To nie działa w ten sposób. Praktyka jest konieczna, jeśli wszystkie te wskazówki mają zostać wykorzystane w prawdziwym ataku. Istnieje wiele sposobów wypróbowania tych wskazówek, a najlepsze jest nawiązanie krótkich rozmów z całkowicie nieznajomymi. Tego rodzaju konwersacje nie muszą być celem, jedynym celem jest próba czucia się spontanicznie w rozmowach.

Powyższe wskazówki pomagają wyglądać i brzmieć naturalnie w interakcji. Ułatwia także rozpoczęcie rozmowy z inną osobą. Aby rozmowa trwała, potrzeba jednak więcej. Ważnym zadaniem jest uważne słuchanie. Zostało to omówione w poprzednim rozdziale. Jeśli chcesz, aby rozmowa trwała wystarczająco długo, aby budować relacje i zaufanie do celu, uważne słuchanie jest absolutną koniecznością.

Dostarczanie logicznych wniosków

System społeczny, w którym wychowuje się większość ludzi, sprawia, że chcą wiedzieć, co mają robić. W domu dzieci są instruowane przez rodziców; w pracy istnieje hierarchia przepływu poleceń; a w polityce liderzy polityczni wybierają ścieżkę dla większości. W większości konfiguracji zawsze będzie jedna osoba dowodząca, która ma rzekomy przywilej mówienia ludziom, co ma robić. Można to wykorzystać na korzyść inżyniera społecznego, ponieważ cele będą już przygotowane, aby powiedzieć im, co robić. W każdej interakcji z inżynierem społecznym cel musi zostać poinformowany, co dalej. Kiedy cel ataku zostanie w końcu osiągnięty, najlepiej wypełnić wszelkie dziury, które mogą pozostać. Inżynier społeczny powinien dać celowi logiczną konkluzję o tym, co się wydarzyło i że dobiegnie końca. Pozostawienie ich w zawieszeniu po ataku lub interakcji rodzi pytania, które mogą skłonić ich do poszukiwania własnych wyjaśnień. Czasami zamiast wyciągać wnioski, inżynier społeczny może wskazać celowi pewne dalsze działania. W naszym wcześniejszym ataku na uzyskanie dostępu do serwerowni; po wyjściu moglibyśmy powiedzieć organizacji, aby regularnie sprawdzała serwery pod kątem innych problemów i wezwała serwisantów, którzy pojawią się w przypadku wystąpienia błędów. Oczywiście w tym momencie logiczne jest podanie numeru rzeczywistej firmy naprawczej. Chodzi o to, że cel zostanie zamknięty i da inżynierom społecznemu wystarczająco dużo czasu, aby usunąć wszelkie powiązania z atakiem. Zaletą pretekstu dla inżyniera społecznego jest to, że jest on niezobowiązujący, zawsze można wybrać, kiedy go porzucić. Przeszliśmy przez zasady pretekstu; jednak wciąż nie wiemy nic o tym, jak inżynierowie społeczności budują pretekst i aktualizują go. Istnieje wiele aspektów pretekstowania, że inżynier społeczny musi się dobrze postarać, aby pretekst był udany. W poniższej sekcji omówiono je.

Udane preteksty

Ponieważ pretekstowanie polega na tworzeniu i przeżywaniu kłamstwa, najlepiej jest wziąć rzeczywiste przykłady niektórych scenariuszy, w których preteksty zostały pomyślnie wykonane. Jak stwierdzono wcześniej w tym rozdziale, preteksty są używane nie tylko w inżynierii społecznej i dlatego nie powinieneś być zaskoczony, jeśli przykład wykracza poza kontekst złośliwego ataku. Niektóre ze znanych przypadków pretekstowych są wyjaśnione dalej.

Wyciek informacji HP

W 2006 r. HP walczyło z problemem wycieku informacji niejawnych i poufnych z organizacji. Podejrzewano, że przecieki pochodzą od wysokich rangą urzędników organizacji, którzy zasiadali na posiedzeniach zarządu. W tym czasie przewodnicząca, pani Patricia Dunn, była tym zaniepokojona i starała się o uzyskanie rejestrów telefonicznych członków zarządu. Firma była w stanie złapać kreta, który okazał się reżyserem. Kret dostarczał CNET, internetowej agencji prasowej, poufne informacje wewnętrzne omawiane na spotkaniach zarządu. Ciekawym fragmentem tego przykładu są szczegóły tego, jak schwytali kret. Zastosowano wątpliwe taktyki w celu uzyskania rejestrów telefonicznych członków zarządu oraz w taki sposób, aby nie mogli stwierdzić, że są monitorowani. HP przyznał, że wykorzystał technikę zwaną pretekstem, aby dostać się na szlak kreta. Jednak zastosowanie tej techniki prześladowało ich, ponieważ kilku pracowników HP, w tym prezes, zostało oskarżonych o nieuczciwe uzyskiwanie danych osobowych innych osób. Sposób, w jaki przeprowadzono pretekst, był nieco podejrzany. My już dyskutowaliśmy, że preteksty obejmują tworzenie fałszywego scenariusza i / lub przyjęcie innej tożsamości, aby skłonić innych do ujawnienia poufnych informacji lub wykonania pewnych czynności. W przypadku HP udało się z powodzeniem zastosować kilka taktyk pretekstowych, aby podać dane telefoniczne członków zarządu i reporterów podejrzanych o wyciek informacji. Zatrudnieni konsultanci ds. Bezpieczeństwa prowadzący polowanie na czarownice dla mola zastosowali trzy taktyki. Przyjęli preteksty pracowników przewoźników komórkowych i wykorzystali te osobowości, aby uzyskać dostęp do niektórych zapisów telefonicznych od operatora. Zadzwoniliby do innych pracowników przewoźników i poprosili o przekazanie zapisów telefonicznych określonych numerów. Inną taktyką, którą stosowali, było fałszowanie tożsamości osób, które badali, a następnie poprosili o przekazanie ich rejestrów telefonicznych od przewoźników. Wreszcie, zarejestrowali się na kontach internetowych u przewoźników, wykorzystując informacje, takie jak numery ubezpieczenia społecznego podejrzanych, i wykorzystali te konta do uzyskania dostępu do rejestrów połączeń i innych informacji. Wszystkie te trzy techniki działały niesamowicie. Po poleceniu ujawnienia zebranych informacji przewodniczący powiedział, że ćwiczenie pretekstowe umożliwiło im uzyskanie rejestrów połączeń, raportów kredytowych, informacji bankowych, informacji o klientach, numerów ubezpieczenia społecznego i numerów telefonów związanych z właścicielami numerów, które badali. Oczywiście wykorzystanie pretekstów przez tę firmę w celu uzyskania pieprzyka mogło być kontynuowane za burtą, ale zadziałało. Obawy etyczne polegają na tym, że dochodzenie jednego mola kosztowało prywatność bardzo wielu innych. Zakontraktowani konsultanci ds. bezpieczeństwa wykonujący preteksty byli w stanie bezkrytycznie gromadzić prywatne informacje wielu niewinnych osób . Przekroczyli także swoje granice, używając pretekstu do operatorów komórkowych AT&T i Verizon w poszukiwaniu polis na telefony. Jednak incydent ten w istocie przyniósł pytania bezpieczeństwa innym firmom, ponieważ osoby z zewnątrz mogły uzyskać informacje o prywatnych użytkownikach. Ten jedyny atak potwierdza siłę pretekstu. Pokazuje, że przy wystarczającym zaangażowaniu można uzyskać poufne informacje przy użyciu fałszywych scenariuszy i fałszywych tożsamości. Ten atak pokazuje także prawne implikacje pretekstu. Oczywiście konsultanci ds. Bezpieczeństwa i prezes HP byli na dobrej drodze, by znaleźć kret, ale oni zastosowali bardzo potężną technikę i ostatecznie naruszył prywatność wielu niewinnych ludzi.

Stanley Rifkin

Pan Rifkin jest jednym z najbardziej znanych cyberprzestępców dlatego, że w latach 70. dokonał jednego z największych napadów na banki w Stanach Zjednoczonych Ameryki. Był konsultantem komputerowym, który prowadził własną działalność gospodarczą w tej dziedzinie. Został zatrudniony przez Narodowy Bank Bezpieczeństwa Pacific, z siedzibą w Los Angeles. Bank był dobrze zabezpieczony i poważnie podchodził do bezpieczeństwa w Internecie, dlatego zatrudnił Stanleya Rifkina, ponieważ miał wiarygodne umiejętności jako maniak komputerowy, aby dowiedzieć się, gdzie można go wykorzystać. Niestety dla banku Rifkin stał się kolejną opowieścią o przyjacielu, który został wrogiem

po tym, jak ukradł z niego 10 milionów dolarów. Uproszczony sposób, w jaki Rifkin obrabował bank, jest wciąż niewyobrażalny. W tym czasie przelewy bankowe były zwykle wykonywane przy użyciu przelewu bankowego. Aby zabezpieczyć te przelewy, bank wykorzystał kod numeryczny, który byłby zmieniany każdego dnia i udostępniany tylko kilku pracownikom banku. Numer będzie wysyłany każdego dnia w zabezpieczonym pokoju, z którego niewielu upoważnionych pracowników będzie go czytać. Ten kod był wymagany przez osoby dokonujące przelewów, aby je autoryzować. W dniu ataku Rifkin pojawił się na terenie banku, jak zwykle.

Ponieważ był znany innym pracownikom jako facet komputerowy, nikt tak naprawdę się nim nie przejmował. Wyglądał na przyjaznego młodego człowieka, który właśnie rutynowo sprawdzał komputer. Jednak tego dnia Rifkin postanowił pojechać windą w stronę bezpiecznego pokoju, w którym wysyłano wrażliwy kod numeryczny. Mimo że pokój był zabezpieczony przez strażników, był w stanie wymyślić idealne usprawiedliwienie jako pracownik IT, który miał uzyskać dostęp do pokoju. W środku Rifkin zapamiętał kod i wyszedł. Następnie zadzwonił do pokoju przelewów pod pretekstem pracownika oddziału międzynarodowego banku. Poinstruował pokój transferowy, aby dokonał przelewu w wysokości 10 milionów dolarów na inne konto. Poproszono go o podanie kodu numerycznego dnia, aby zezwolić na przeniesienie, coś co zrobił to bez wahania. Przekonani, że ta prośba rzeczywiście pochodzi od oddziału międzynarodowego, pokój transferowy przelał pieniądze na konto, o którym im mówiono. Wszystko wydawało się całkiem w porządku, dopóki nie odkryto, że prośba nie pochodziła z międzynarodowego oddziału banku. Jednak w tym momencie było już za późno, a pieniądze już się zmieniły. Z tego śmiałego ataku pod pretekstem należy zwrócić uwagę na kilka rzeczy. Po pierwsze, Rifkin był pewny siebie i dlatego był wiarygodny i naturalny w swoich interakcjach tego dnia. Dlatego nie wzbudził podejrzeń. Gdyby po raz drugi wątpił w siebie, nie byłby w stanie przejść obok strażników zabezpieczających pokój transferowy. Po drugie, Rifkin przeprowadził badania i uzyskał kod numeryczny dnia, który był wymagany, aby można było wykonać przelew. Bez tego kodu, nawet przy najsłodszych językach, Rifkin nie byłby w stanie przekonać pokoju transferowego do przelewania pieniędzy. Dołożył należytej staranności i uzyskał cenny kod. Po trzecie, Rifkin musiał być spontaniczny w swoich interakcjach ze strażnikami i personelem pokoju transferowego. Musiał mieć właściwe odpowiedzi na pytania, które mu zadano, ponieważ był to dość wrażliwy pokój, do którego miał dostęp. Wreszcie Rifkin musiał wykonać napad płynnie, bez pośpiechu, aby nie wzbudzić niepokoju. Skok okazał się dobry, ponieważ Rifkin był w stanie przelać pieniądze pod pretekstem pracownika w oddziale międzynarodowym. Na szczęście lub niestety został później aresztowany, ale trudno było uwierzyć, że niewinnie wyglądający konsultant komputerowy był złodziejem. Jego pretekst był dobrze zaplanowany i utrzymywał wodę przez cały atak. Został zatrzymany tylko dlatego, że wyddał go przyjaciel po połączeniu kropek między nagle zdobytym bogactwem Rifkina a napadem w słynnym banku, w którym pracował. Mówi się, że Rifkin próbował powtórzyć atak z innym bankiem, ale został złapany, ponieważ był to układ. Historia Rifkina kładzie nacisk na niektóre zasady, które omówiliśmy wcześniej w pretekstie. Być może ważnym dodatkiem do nich, którego możemy się nauczyć z jego napadów, jest to, że inżynier społeczny może zostać złapany, jeśli użyje pretekstu. Rifkin został złapany za kaucją za pierwszy skok, gdy próbował wykonać kolejny skok za pomocą tych samych sztuczek.

Hack DHS

Jest to poważny hack, który miał miejsce w 2016 r. i doprowadził do kradzieży danych osobowych 9000 pracowników Departamentu Bezpieczeństwa Wewnętrznego i 20000 funkcjonariuszy współpracujących z FBI. Skradzione dane osobowe obejmowały pełne nazwiska, stanowiska, adresy e-mail i aktualne numery telefonów. Jeszcze bardziej niepokojące jest to, że atak socjotechniczny został przeprowadzony bezpośrednio na oficerze wsparcia IT, osobie, której ranga pełni rolę ochrony innych

pracowników przed tym i podobnymi rodzajami ataków. Haker, który to zrobił, skontaktował się ze stroną internetową o nazwie Motherboard, aby wyjaśnić, w jaki sposób udało mu się zhakować departament sprawiedliwości. Haker próbował złamać dział przy użyciu innych technik ataku na formularz logowania, ale nie przyniosło to żadnych pozytywnych rezultatów. Właśnie tam przeszedł na socjotechnikę. Zadzwonił do biura wsparcia IT i powiedział, że jest nowy i nie może dostać się do portalu. Zapytali, czy ma token dostępu, na który odpowiedział, że nie. Biuro pomocy technicznej powiedziało mu, żeby się nie martwił, i pozwolą mu użyć go do logowania. Był to decydujący moment ataku, w którym pracownicy działu IT przekazali hakerowi token dostępu, aby móc dostać się do portalu. W następnych raportach z departamentu stwierdzono, że zasady bezpieczeństwa zabraniają personelowi IT wydawania tokenów niezweryfikowanym osobom. Weryfikacja miała się odbyć poprzez fizyczną wizytę w biurze IT lub uwierzytelnienie się przez telefon poprzez udzielenie odpowiedzi na niektóre tajne pytania. Oczywiście wszystkie te zostały zlekceważone przez personel IT, który pomógł hakerowi. Pretekst zastosowany w tym scenariuszu daje nam ważne informacje na temat inżynierii społecznej. Personel wsparcia IT będzie miał przede wszystkim sposoby na obejście rygorystycznych kontroli wprowadzonych w celu zapobiegania nieautoryzowanemu dostępowi do systemów. Mogą zmieniać hasła, dawać nowy dostęp

tokeny, twórz nowe konta użytkowników i zwiększaj uprawnienia użytkownika wśród wielu innych rzeczy. Są również pracownikami, którzy muszą być jak najbardziej pomocni dla innych pracowników w sprawach związanych z komputerami. Czasami muszą działać jako opiekunki lub rodzice, niestrudzenie kierując i poprawiając swoich użytkowników, którzy nie znają się lepiej. Są zatem idealnym celem dla hakera, który musi szybko uzyskać dostęp do zabezpieczonego systemu. Haker musi jedynie przekonać personel wsparcia, że jest on jednym z nich. Przed przejściem do inżynierii społecznej haker próbował bezpośrednio włamać się do portalu. To się nie udało. Większość systemów jest zbudowana tak, aby wytrzymać popularne typy włamań. Słabość leży po stronie użytkowników, co widać w tym scenariuszu. Rzućmy okiem na zasady zastosowane, aby ten pretekst się powiódł. Najpierw, haker wybrał bardzo prosty pretekst. Haker powiedział tylko, że jest nowy i próbuje uzyskać dostęp do portalu Departamentu Sprawiedliwości. Ten pretekst nie ma wiele. Jeśli zostaną mu zadane pytania, haker może uciec od zwykłego powiedzenia, że nie wie. Jest to prawdopodobnie powód, dla którego personel chętniej pomagał hakerowi. Dał mu również wątpliwości, nie rozpoczynając procesu weryfikacji. Wybór pretekstu był idealny do tego ataku. Sytuacja wyglądałaby inaczej, gdyby haker twierdził, że jest pracownikiem wyższego szczebla, ponieważ wszyscy pracownicy IT prawdopodobnie znają pracowników wyższego szczebla, co może prowadzić do problemów takich jak weryfikacja. Jak omówiono w zasadach pretekstu, im prostszy pretekst, tym lepiej. Inną zasadą zastosowaną w tym pretekstie jest spontaniczność. Gdyby haker brzmiał na napiętego lub nienaturalnego, dzwoniąc do biura wsparcia, istniałaby mniejsza szansa na przeprowadzenie tego ataku. Z pewnością haker właśnie zadzwonił i wyjaśnił swój przypadek bycia nowym, a także bezradnym zablokowaniem dostępu do portalu. To był odważny ruch, ale to może uratować ten atak. Personel IT mógł założyć, że żaden outsider nie będzie miał odwagi zadzwonić do biura i ich zhackować. Wreszcie pretekst wykorzystał skuteczną zasadę korzystania z telefonu. Większość osób atakujących będzie używać wiadomości e-mail, ponieważ nie będą one bezpośrednio kontaktować się z osobą po drugiej stronie, jest to wygodniejsze i mają więcej czasu na edycję tego, co chcą powiedzieć. Ten haker użył telefonu i uzyskał natychmiastowe wyniki. Rozmowa telefoniczna jest skuteczniejsza niż wiadomość e-mail, ponieważ można wykorzystać emocje lub wywrzeć presję na celu. Jeśli nagranie połączenia telefonicznego było dostępne, to co pokaże, że haker zastosował pewne taktyki, aby personel IT zastosował się tak szybko. Może haker wydawał się zrozpaczony lub beznadziejny. Prawdopodobnie haker powiedział, że otrzymał polecenie dostarczenia czegoś przez portal przed określonym terminem, a stało się to niemożliwe z powodu braku dostępu. Prawdopodobnie haker wykorzystał coś w tym celu, aby zmusić

personel IT do pomocy. Dlatego korzystnym jest używanie telefonu, gdy tylko jest to możliwe. Podsumowując ten atak, należy zauważyć, że to, co wydarzyło się w Departamencie Sprawiedliwości, może prawdopodobnie wydarzyć się w każdej innej organizacji. Nawet jeśli będą obowiązywać surowe zasady, przeważnie będą jakieś luźne cele, które można wykorzystać. W tym przypadku luźny koniec był zbyt pomocnym biurem wsparcia. Haker nie miał innych możliwości uzyskania dostępu do portalu, ponieważ inne techniki hakowania nie działały. Pretekstowanie działało jednak jak urok. Sukces tego pretekstu wynikał z trzech rzeczy, wyboru prostego pretekstu, spontaniczności i użycia połączenia telefonicznego. Ten atak pokazuje, że wielu pracowników, zwłaszcza w sektorze publicznym, nie jest odpowiednio przeszkolonych, aby zapobiec tego typu atakom. Ten atak pokazuje naruszenie podstawowych środków bezpieczeństwa przez cel, kogoś, kto powinien był wiedzieć lepiej, ale niestety nie wiedział.

Oszustwa związane z usługami skarbowymi

2017 rok mógł zostać zdefiniowany przez oszustwa IRS, ponieważ wielu obywateli USA zakochało się w tych dobrze zaplanowanych atakach. Według CNN przywódcą wszystkich tych oszustw IRS był 24-letni Indianin, Sagar Thakkar. Założył centra telefoniczne, za pomocą których wyłudzał miliony dolarów od Amerykanów. Zarzuty, przed którymi stoi Thakkar, to wymuszanie, oszukiwanie, podszywanie się i spisek. Jest to jeden z najbardziej udanych ataków inżynierii społecznej, jakiego kiedykolwiek doświadczyły Stany Zjednoczone. Stosował powszechny strach przed Amerykanami, ciężar składania deklaracji podatkowych. Przyjrzyjmy się uważnie, jak Thakkar i inni napastnicy byli nieświadomymi celami inżynierii społecznej, i zobaczmy, jakie zasady pretekstu zastosowali

Rozmowy telefoniczne

W tego typu ataku dzwoniący twierdzili, że pochodzą z IRS. Ich przesłanie było takie, że dali ostateczne powiadomienie o należnej płatności. Wydaliby groźby aresztowania, gdyby kwoty rzekomo należne od syndyka nie zostały zapłacone. Niektórzy dzwoniący nie brzmią natywnie; dlatego ich minusy nie były tak skuteczne, ponieważ wzbudziły podejrzenia. Byli też inni dzwoniący, którzy używali nagranych wiadomości, ale te również brzmiały nieoryginalnie i dlatego nie zawsze działały. Byli jednak inni, uzbrojeni po zęby, z pewnymi faktycznymi informacjami na temat swoich celów. Mówi się, że dzwoniący kupili tego rodzaju informacje od hakerów, którzy naruszyli bazy danych administracji i zdrowia. Ofiary byłyby bardziej niż pewne, że to IRS ponieważ prawie nikt inny nie miałby takich informacji. W końcu zapłaciliby ogromne sumy, tak jak kierowali nimi inżynierowie społeczni. Jednak dziwną rzeczą w sposobie, w jaki większość dzwoniących wymagała zapłaty pieniędzy, były karty upominkowe iTunes. Płatności te byłyby zatem niemożliwe do wyśledzenia. Jednak ofiary byłyby w tym momencie zbyt przestraszone, aby zadawać jakiekolwiek pytania. Patrząc uważnie na to oszustwo, użyty pretekst nie jest prosty, ale dotyczy IRS. Korzystanie z takiego pretekstu ma pewne zalety i wady. Wady, cel może zweryfikować czy to prawda, dzwoniąc do prawdziwego urzędu skarbowego. Ponadto, gdy sprawy idą na południe, a napastnik zostaje aresztowany, opłaty za to przyciągają więcej więzienia. Na plus, wielu generalnie obawia się IRS , więc ten pretekst będzie miał większe szanse powodzenia, ponieważ cele można łatwo postawić pod presją. To z powodu tej presji tysiące ofiar nie kwestionowały, dlaczego polecono im dokonywać depozytów za pomocą kart podarunkowych iTunes zamiast kart debetowych lub kredytowych. Zasadą stosowaną przez niektórych atakujących było dokładne badanie celu. Udane ataki miały miejsce, gdy atakujący miał wiele szczegółów na temat celu. Jednak uzyskanie szczegółów nie jest trudne. Serwisy społecznościowe to pewne miejsce, od którego ludzie chętnie umieszczają swoje dane osobowe. Strony takie jak LinkedIn zachęcają użytkowników do publikowania dokładnych informacji akademickich i dotyczących zatrudnienia. Dlatego uzyskanie tych informacji nie jest trudne.

E-maile

Inna wersja ataku IRS została przeprowadzona przy użyciu wiadomości e-mail, które zamiast grozić ludziom, zaoferowały im niewyobrażalnie dobre oferty. Ofiary powiedziały, że otrzymały wiadomości e-mail rzekomo od Taxpayer Advocate Service, działu IRS zajmującego się sporami podatkowymi spory komplikacjami. E-maile mają twierdzić, że wystąpił problem z podatkami celu i są ustawione na duży zwrot pieniędzy. Mówią, że zwrot zostanie zdeponowany bezpośrednio na koncie celu, a wszystko, czego potrzeba, to pewne informacje, aby to ułatwić. Informacje, o które proszą, dotyczą jednak. Proszą o podanie kodów PIN, haseł i innych informacji o koncie bankowym, aby umożliwić zdeponowanie tego zwrotu. Mówi się, że ofiary chętne do otrzymania zwrotu pieniędzy podały te poufne informacje. Stało się tak, że hakerzy opróżnili konta bankowe ofiary. uważając na ten atak, pretekstem był IRS, ale łagodniejszy ton. E-maile były zatem atrakcyjne dla celów, a nie dla nich groźne. Ponownie napastnicy przeprowadzili badania, aby uzyskać dodatkowe informacje o celach i zwiększyć wiarygodność ataku. Cele wykorzystały również logiczne wnioski. Wyjaśnili, że potrzebowali tylko danych osobowych celu, aby pomóc im w dokonaniu zwrotu pieniędzy. Wskaźnik skuteczności tego ataku był nadal wysoki, ponieważ ludzie byli podekscytowani otrzymaniem pieniędzy obiecanych przez IRS:

Naruszenia w e-mailach biznesowych

Było to bardzo popularne na początku 2017 roku i było bardzo udane. Firmowe adresy e-mail niektórych ważnych osób w organizacji były sfałszowane, a autorytet tej osoby uzyskiwał poufne informacje z celów. Atakujący sprawdzali szczegóły niektórych firm i uzyskiwali adresy e-mail pracowników niższego szczebla pracujących w tych firmach. Ważne było, aby byli oni pracownikami niskiego szczebla zarówno ze względu na atak, jak i dla sprawowania władzy do pracy. Atakujący fałszują adresy e-mail personelu działów zasobów ludzkich i wykorzystują je, aby prosić pracowników o przesłanie kopii formularzy W-2. Informacje w formularzach W-2 są dość poufne i można je wykorzystać do składania deklaracji podatkowych. Tym, co robili napastnicy, było składanie deklaracji podatkowych, ale w taki sposób, aby przyciągać zwroty i po prostu zbierać zwroty. W bardziej nikczemnych scenariuszach osoby atakujące wykorzystałyby te informacje, aby poprosić o pomoc finansową uczelni. Liczba ofiar, których informacje znalazły się w takich próbach, była tak wysoka, że Departament Edukacji Stanów Zjednoczonych zamknął tę usługę. Ci napastnicy bardzo go wykorzystali. Patrząc na atak, można zauważyć, że hakerzy stosowali zasadę prostoty. Pretekst składał się ze sfałszowanego adresu e-mail HR i prostej prośby o przesłanie formularza W-2. Skierowano go również do pracowników niskiego szczebla, którzy mieliby najmniej pytań do kierowania do personelu HR. Oczywiście przeważnie przestrzegali i wysyłali swoje formularze W-2 i dlatego ta wersja oszustwa IRS była tak skuteczna. Inną zastosowaną zasadą była zasada badań. Ten atak został poparty badaniami. Osoby atakujące musiały dowiedzieć się o pracownikach niskiego poziomu w pewnej organizacji, a także HR. Powszechne formaty służbowych wiadomości e-mail są takie, że składają się z imienia i nazwiska pracownika, a następnie domeny organizacji. Było to bardzo pomocne przy wyszukiwaniu e-maili roboczych celów. Sfałszowanie adresów e-mail nie jest bardzo trudne. Atakujący zwykle zamieniają niektóre słowa na cyfry lub dodają niektóre symbole, aby uzyskać adres prawie pasujący do prawdziwego. Oczywiście wiele osób nie sprawdza wewnętrznych szczegółów, takich jak domena nadawcy wiadomości e-mail. Kiedy widzą znane nazwisko i znajomy adres e-mail, wierzą, że to prawdziwa osoba. W ten sposób atak stał się tak skuteczny.

Litery

Wreszcie, oszuści wykorzystali fizyczne litery, aby oszukać obywateli USA. Jest to nadal uzasadniony sposób, w jaki IRS kontaktuje się z kimś, kiedy chce zainicjować korespondencję. Listy te były również

wykorzystywane do żądania od użytkowników podania danych osobowych, a czasem informacji bankowych. Było jednak mniej zgłoszeń o tego rodzaju oszustwach, ponieważ wymagały one zbyt wiele pracy. Ale niektóre z nich nadal odnosiły sukcesy. Wynika to z faktu, że obywatele USA bardzo poważnie podchodzą do urzędu skarbowego i zwykle nie odrzucają żadnej korespondencji to. Zasady zastosowane w tego typu pretekstach są dwa, badawcze i proste preteksty. Trzeba było przeprowadzić badania, aby znaleźć rzeczywiste skrzynki pocztowe celów. Ponownie jest to informacja, którą łatwo znaleźć w Internecie. Są takie strony jak Pipl, które je wymieniają. Inną zasadą jest to, że pretekstem były proste adresy pocztowe jednej czwartej populacji Ziemi. Dotyczyły tylko listów, żadnych telefonów ani e-maili. Jak powiedziano wcześniej, ludzie w Stanach Zjednoczonych nie zwalniają urzędu skarbowego, dlatego czytaliby i robili zgodnie z listem.

Sieci Ubiquiti

Ten atak jest częstym odniesieniem, ponieważ jest dziś używany w wielu opracowaniach oszustwa CEO. Sieci Ubiquiti znalazły się w niewygodnym miejscu w 2015 roku po tym, jak uświadomiły sobie, że stały się ofiarą inżynierii społecznej i straciły 36 milionów dolarów na hakerów. Kalifornijska firma zajmująca się produkcją urządzeń sieciowych potwierdziła, że stała się ofiarą inżynierii społecznej po tym, jak jej spółka zależna w Hongkongu została oszukana podczas ataku, najlepiej znanego jako oszustwo CEO. Sposób przeprowadzenia tego ataku jest bardzo interesujący dla tej części. Oszustwo pasuje do jednego z oszustw IRS opisanych jako oszustwo dotyczące firmowych wiadomości e-mail, w ramach którego pracownicy niskiego szczebla w organizacji otrzymywali wiadomości e-mail ze sfałszowanych adresów e-mail HR z prośbą o przesłanie formularzy W-2.

W ataku sieci Ubiquiti hakerzy sfałszowali wiadomość e-mail starszego pracownika i wykorzystali ją do komunikacji z pracownikami działu finansowego. W swoich wiadomościach e-mail hakerzy wyjaśnili, że niektórzy dostawcy zmienili szczegóły płatności, w związku z czym otrzymają zapłatę za pomocą zagranicznych kont bankowych. FBI twierdzi, że w ciągu 17 dni wyśledził 14 niezwykłych przelewów pieniężnych do krajów takich jak Chiny i Rosja z Ubiquiti. W tym momencie biuro podniosło alarm do Ubiquiti, że miały miejsce podejrzane transakcje z konta bankowego Ubiquiti w Hongkongu. Jest to punkt, w którym spółka matka interweniowała i powstrzymała dział finansowy od dalszych transferów. W tym momencie hakerzy mieli ponad 46 milionów dolarów. Uważa się, że gdyby FBI nie podniosło alarmu, transakcje te byłyby kontynuowane, a firma poniosłaby jeszcze większe straty. Firma śledziła sprawę i była w stanie odzyskać tylko około 8 milionów dolarów. Założyciel i dyrektor generalny firmy, Robert Pera, obwinił ten incydent za złą ocenę sytuacji i niekompetencję niektórych swoich księgowych. Przyjrzyjmy się uważnie temu niefortunnemu atakowi i zobaczmy elementy, dzięki którym ten atak był możliwy i skuteczny. Badania były ważną częścią tego ataku. Wynika to z faktu, że osoby atakujące musiały znać dostawców firmy, e-maile starszych pracowników i e-maile pracowników działu finansowego. Hakerzy musieli także wiedzieć, kiedy wypłacane są płatności dla dostawców, aby uderzyć we właściwym czasie. Kolejną wybraną zasadą pretekstu było wybranie prostego pretekstu. W tym ataku hakerzy używali tylko sfałszowanych wiadomości e-mail, podając się za członka personelu wyższego szczebla upoważniającego księgowych do przesyłania środków na zagraniczne konta. Wygląda na to, że pojawiła się seria e-maili, ponieważ przelewy odbywały się przez 17 dni. Ten pretekst był bardzo prosty do stworzenia i zarządzania. Wymagane było jedynie dowcipne użycie autorytatywnych słów. Hakerzy unikali używania telefonów, ponieważ pretekstem była osoba, którą znali księgowi. Hakerzy upewnili się również, że pretekst jest łatwy do zarządzania. Unikali również wchodzenia w szczegóły, dlaczego dostawcy przynajmniej raz zmieniali preferencje płatności. Zastosowane zasady były bardzo opłacalne, ponieważ firma nie odzyskała jeszcze 36 milionów dolarów.

Prawne obawy związane z pretekstem

Istnieją pytania, czy niektóre próby pretekstu są legalne, czy nie. W 2005 r. Federalna Komisja Handlu USA przedstawiła pewne znaczące informacje na temat nielegalności tej praktyki. W swoich oświadczeniach:

* Pretekstowanie polega na uzyskiwaniu poufnych informacji od klientów lub instytucji w sposób oszukańczy i wprowadzający w błąd i dlatego jest nielegalny

* Weryfikacja informacji uzyskanych o celu od innej instytucji jest nadal uważana za pretekst, a zatem nielegalna

* Pozyskiwanie zapisów telefonicznych dotyczących użytkownika z innej instytucji jest również pretekstem, a zatem nielegalne

W swoim prawnym rozumieniu FTC wyjaśniła, że:

* Nieuczciwe lub nieuczciwe jest uzyskiwanie informacji o celu bezpośrednio od klienta lub od instytucji posiadającej informacje o kliencie

* Pozyskiwanie informacji o kliencie od klienta lub instytucji używającej sfałszowanych, skradzionych lub utraconych dokumentów jest nielegalne

* Pozyskiwanie informacji o klientach od innej osoby jest niezgodne z prawem przy użyciu oszukańczych i nieuczciwych sposobów

Jak widać z tych oświadczeń, FTC bardziej martwiła się o klientów. Oświadczenia te dotyczą jednak prawie wszystkich innych, niekoniecznie klientów. Oznacza to, że praktykowanie pretekstów, nawet przy dobrych intencjach, może wpędzić kogoś w kłopoty. W podanych przykładach był jeden o HP. Szkoda, że ci zaangażowani zostali oskarżeni o poważne zarzuty, które przyciągają do więzienia. Dlatego należy zachować ostrożność, próbując udawać innych, albo w celu przeprowadzenia testów penetracyjnych, albo po prostu dla zabawy.

Narzędzia do ulepszania pretekstów

Wreszcie pretekst może być przekonujący za pomocą szeregu narzędzi. Najważniejsza jest wizytówka. Ludzie zwykle ufają wizytówkom i wierzą, że osoba jest wszystkim, co mówi wizytówka. Dlatego jeśli pretekst obejmuje twierdzenie, że pochodzi od pewnej firmy zajmującej się naprawą komputerów, zrobienie wizytówki z twoim nazwiskiem starannie napisanym obok nazwy firmy i logo pozwoli ci zaoszczędzić trochę kłopotów. Wizytówki można również rozdawać celom, które zaczynają wątpić w pretekst i chcą mieć czas na podjęcie decyzji. Innym narzędziem, które radykalnie zwiększa szanse powodzenia ataku pod pretekstem, jest mundur. Jeśli, na przykład, atakujący chce wysypać śmieci z organizacji, może po prostu udać się do strażników i wyjaśnić, że pochodzi z firmy zajmującej się zbieraniem śmieci, i chce usunąć worki na śmieci przed nadejściem ciężarówki. Przy odpowiednim mundurze strażnicy go wpuszczą. To część kadrowania, w której inżynier społeczny zabiera strażników do ich osobistych doświadczeń związanych z obserwowaniem ludzi wywożących śmieci w mundurach. Strażnicy nie będą mieli wątpliwości co do atakującego.

Możesz użyć narzędzia SET Kali Linux do inżynierii społecznej.

Porady

Wskazówki dotyczące postępowania z atakami pretekstowymi są następujące:

* Chroń swoje dane osobowe i nigdy nie udostępniaj ich przez telefon, e-mail ani wyskakujące okienka, jak pokazano na poniższym zrzucie ekranu lub na stronach internetowych:

* Zawsze miej oko na wyciągi bankowe, nawet niewielka ilość może prowadzić do znacznie większych

* Dodaj uwierzytelnianie dwuskładnikowe do wszystkiego, co jest możliwe (bankowość internetowa, konta w mediach społecznościowych, konta ISP itd.):

* Twórz hasła trudne do odgadnięcia lub złamania

* Filtruj wiadomości e-mail i nie klikaj żadnych podejrzanych łączy

* Nie polegaj tylko na technologii, pamiętaj o tym, co możesz zrobić, aby hakerzy utrudniali pracę, zawsze znajdą sposób (i prawdopodobnie poprzez socjotechnikę), aby się z Tobą skontaktować

* Używaj niszczarki do nurkowania w kontenerach na śmieci

* Zachowaj szczególną ostrożność w przypadku połączeń VOIP specjalnie od nieznajomych

* Pamiętaj, że nie ma nic za darmo

Podsumowanie

W tej części omówiono ważną część inżynierii społecznej, preteksty. Spojrzał na siedem zasad, które pomagają w udanej próbie pretekstu. Analizowano znaczenie zasady badania, aby uzyskać wystarczającą ilość informacji o celu. Analizowano także identyfikację osobistych zainteresowań, aby szybko uzyskać cel do spełnienia. Zbadano użycie akcentów, aby pretekst był bardziej przekonujący. Podano pewne kroki, które można zastosować, aby pomóc w uzyskaniu akcentu w tym celu. Wyjaśniono korzystanie z telefonów, które mają wysoki wskaźnik powodzenia, ponieważ większość hakerów korzysta obecnie z wiadomości e-mail i Internetu. Spontaniczność została również przeanalizowana i jak wpływa na szanse powodzenia ataku, szczególnie podczas ustnej interakcji z celem. Ostatnią analizowaną zasadą jest dostarczanie logicznych wniosków celom. Kapituła postanowiła przyjąć praktyczne podejście, omawiając, co stanowi udany pretekst; zrozumienie, w jaki sposób przeprowadzane są preteksty, pozwoli nam lepiej radzić sobie z atakami. Przeszedł przez kilka spraw pod pretekstem. W odniesieniu do każdego z nich omówiono zasady zastosowane w celu zapewnienia, że zastosowany pretekst będzie działał. Niektóre z omawianych ataków, szczególnie w ramach oszustw IRS, wciąż mają miejsce. Omówiono legalność pretekstów i stwierdzono, że jest to nielegalna praktyka. Wreszcie wspomniano o kilku dodatkowych narzędziach, które można wykorzystać do wzmocnienia ataku inżynierii społecznej. Podane przykłady z prawdziwego życia miały na celu dać czytelnikowi zrozumienie, co sprawia, że atak się powiódł. Z przykładów można zebrać sztuczki, dzięki którym atak się powiedzie. Z perspektywy prawnej część wyjaśniła, dlaczego preteksty są nielegalne i mogą sprawić kłopoty. Wyjaśniono kilka narzędzi, które mogą pomóc w udanym ataku pretekstowym.