FOOTPRINTING I INŻYNIERIA SPOŁECZNA

W tym module nauczysz się, jak korzystać z narzędzi dostępnych w Internecie, aby dowiedzieć się, jak zaprojektowana jest sieć firmy. Poznasz również umiejętności potrzebne do prowadzenia wywiadu konkurencyjnego i jak wykorzystać te umiejętności do gromadzenia informacji. Zanim przeprowadzisz test bezpieczeństwa w sieci, musisz wykonać większość, jeśli nie wszystkie, zadania związane z FOOTPRINTINGiem, omówionych w tym module. Ten moduł wyjaśnia również taktykę atakujących, którzy wykorzystują inżynierię społeczną, aby uzyskać informacje od kluczowych pracowników firmy. Ponadto zbadasz niektóre mniej efektowne metody stosowane przez atakujących — takie jak przeszukiwanie koszy na śmieci, koszy na papier i śmietników w poszukiwaniu starych instrukcji komputerowych, wyrzuconych nośników i innych materiałów — w celu znalezienia informacji, które mogą umożliwić im włamanie się do sieci.

KORZYSTANIE Z NARZĘDZI SIECIOWYCH DO FOOTPRINTINGU

W filmach, zanim złodzieje obrabują bank lub ukradną biżuterię, „sprawdzają lokal", robiąc zdjęcia i zdobywając plany pięter. Złodzieje filmowi zazwyczaj mają wystarczająco dużo szczęścia, aby zdobyć schematy systemów alarmowych i systemów klimatyzacji/wentylacji. Przynajmniej tak przedstawia ich Hollywood. Każdy agent FBI powiedziałby ci, że większość prawdziwych złodziei nie ma tyle szczęścia. Jednak ci sprytni, którzy nie dają się złapać, są skrupulatni i ostrożni. Wielu napastników sprawdza miejsce, aby obejrzeć lokalizację, znaleźć słabe punkty w systemie bezpieczeństwa i ustalić, jakie rodzaje zamków i systemów alarmowych są używane. Próbują zebrać jak najwięcej informacji przed popełnieniem przestępstwa. Jako tester bezpieczeństwa ty również musisz dowiedzieć się jak najwięcej o organizacji, która zatrudniła cię do przetestowania bezpieczeństwa swojej sieci. W ten sposób możesz doradzić kierownictwu w kwestiach problematycznych. W żargonie komputerowym proces znajdowania informacji w sieci firmy nazywa się odciskiem stopy. Możesz również usłyszeć termin „rozpoznanie" i powinieneś znać oba te terminy. Ważną koncepcją jest to, że odcisk stopy jest pasywny lub nieinwazyjny; innymi słowy, nie uzyskujesz dostępu do informacji nielegalnie ani nie zbierasz nieautoryzowanych informacji z fałszywymi poświadczeniami. Dzięki pasywnemu rozpoznaniu nie angażujesz się nawet w zdalne systemy, ale raczej próbujesz uzyskać informacje o swoim celu z innych źródeł. Pasywne działania prawdopodobnie pozostaną niezauważone. Aktywne rozpoznanie z drugiej strony oznacza, że faktycznie prowokujesz sieć docelową w sposób, który może wydawać się podejrzany dla obrońców sieci. Obejmuje to działania takie jak skanowanie portów, transfery stref DNS i interakcja z serwerem internetowym celu. Dzięki aktywnym technikom odcisku prawdopodobnie zostaniesz zauważony, a Twoje działania zostaną zarejestrowane. Tester bezpieczeństwa (lub atakujący) stara się dowiedzieć jak najwięcej o organizacji i jej sieci, używając zarówno pasywnych, jak i aktywnych technik. Prawie wszystkie dostępne narzędzia do odcisku są bezpłatne i mają otwarte oprogramowanie. Narzędzia te są często określane jako narzędzia Open Source Intelligence (OSINT). Termin OSINT odnosi się do cech używanych narzędzi i do metodologii gromadzenia informacji z łatwo dostępnych źródeł publicznych (takich jak Internet).

UWAGA

Wiele narzędzi wiersza poleceń dołączonych do systemów Linux nie jest częścią środowiska Windows. Na przykład polecenia dig, netcat i wget nie działają z poziomu wiersza poleceń systemu Windows 10, ale zazwyczaj można pobrać wersje systemu Windows ze stron internetowych. Testerzy zabezpieczeń powinni poświęcić czas na naukę korzystania z tych narzędzi wiersza poleceń w systemie Linux. W tym module użyjesz narzędzi Domain Dossier i whois.domaintools.com, aby pobrać informacje o obecności firmy w sieci, i zobaczysz, jak transfery stref DNS mogą być używane do określania zakresów adresów IP i nazw hostów komputerów.

BAJTY BEZPIECZEŃSTWA

Co roku pracownicy Departamentu Obrony (DoD) muszą ukończyć szkolenie w zakresie świadomości bezpieczeństwa, które podkreśla niebezpieczeństwo związane z tym, że terroryści i szpiedzy mogą zbierać niejawne informacje. Informacje te można znaleźć w gazetach, witrynach internetowych oraz programach informacyjnych w telewizji i radiu, ale można je również zebrać z Facebooka, LinkedIn i Twittera. Łącząc małe fragmenty informacji, terroryści mogą stworzyć dość szczegółowy obraz działań DoD. DoD chce, aby jego pracownicy zdali sobie sprawę, że omawianie pozornie nieistotnych informacji może być bardziej niebezpieczne, niż się wydaje. Informacje te, w połączeniu z informacjami z innych źródeł, mogą być szkodliwe dla bezpieczeństwa narodowego. Na przykład marynarz w marynarce wojennej USA spotyka przyjaciela w restauracji i wspomina, że będzie nieobecny przez sześć miesięcy. W tej samej restauracji cywil pracujący dla DoD wspomina znajomej podczas lunchu, że musi zostać po godzinach, zamawiając zaopatrzenie. Jak widać, terroryści mogliby łatwo przechwycić obie informacje, podsłuchując rozmowy. Ten przykład może wydawać się naciągany, ale jest to główna metoda gromadzenia informacji wywiadowczych. Chodzi o to, że Ty również musisz zwracać uwagę na wszystkie dostępne informacje, czy to na stronie internetowej, w nagłówkach wiadomości e-mail, czy w oświadczeniu pracownika w wywiadzie. Niestety, atakujący sprawdzają strony internetowe i grupy dyskusyjne, badają adresy IP firm, czytają oferty pracy i szukają ogłoszeń od personelu IT zadających pytania o systemy operacyjne lub konfiguracje zapór sieciowych. Pamiętaj, że po zebraniu informacji powinieneś kontynuować kopanie, aby zobaczyć, co jeszcze potencjalni atakujący mogliby odkryć.

PROWADZENIE ANALIZY KONKURENCYJNEJ

Jeśli chcesz otworzyć studio fortepianowe, aby konkurować z innym studiem, które działa w Twojej okolicy od wielu lat, rozsądne jest zdobycie jak największej ilości informacji o swoim konkurencie. Skąd możesz wiedzieć, że studio odniosło sukces, nie mając dostępu do jego wyciągów bankowych? Po pierwsze, wiele firm upada po pierwszym roku, więc fakt, że studio istnieje przez lata, świadczy o tym, że właściciel robi coś dobrze. Po drugie, możesz po prostu zaparkować samochód po drugiej stronie ulicy od studia i policzyć wchodzących uczniów, aby uzyskać dobry pogląd na liczbę klientów. Możesz łatwo dowiedzieć się, ile kosztują lekcje, dzwoniąc do studia lub szukając reklam w mediach społecznościowych, ulotkach, witrynach internetowych, billboardach itp. Dostępnych jest wiele zasobów, które pomogą Ci dowiedzieć się jak najwięcej, co jest prawnie możliwe, o Twojej konkurencji. Ludzie biznesu robią to od lat. To gromadzenie informacji, zwane wywiadem konkurencyjnym, odbywa się również na jeszcze wyższym poziomie za pomocą technologii. Jako specjalista ds. bezpieczeństwa powinieneś być w stanie wyjaśnić swoim klientom metody, których używają konkurenci, aby zbierać informacje. Aby ograniczyć ilość informacji, które firma upublicznia, musisz dobrze zrozumieć, co konkurencja zrobiłaby, aby odkryć poufne informacje.

BAJTY BEZPIECZEŃSTWA

To, że możesz znaleźć informacje o firmie i jej pracownikach, nie oznacza, że powinieneś je ujawniać. Na przykład, załóżmy, że podczas testów bezpieczeństwa odkrywasz, że pracownik odwiedza stronę internetową serwisu randkowego lub podejrzane grupy dyskusyjne. Dopóki ta aktywność w żaden sposób nie zagraża firmie, nie masz obowiązku informowania firmy. W zależności od przepisów obowiązujących w Twoim kraju lub stanie, kwestie prywatności mogą wpłynąć na Twoją decyzję o sposobie postępowania w tej sytuacji. Specjaliści ds. bezpieczeństwa i urzędnicy firmy mogą zostać pozwani za ujawnienie poufnych informacji tego rodzaju.

Analiza strony internetowej firmy

Ataki często zaczynają się od zbierania informacji ze strony internetowej firmy, ponieważ strony internetowe są łatwym sposobem dla atakujących na odkrycie krytycznych informacji o organizacji. Strony internetowe są często określane jako aplikacje internetowe. Aplikacje internetowe to programy, które działają na serwerze internetowym, a strona internetowa jest jednym z takich programów. Do tego typu gromadzenia informacji dostępnych jest wiele narzędzi. Jednym z przykładów jest Zed Attack Proxy (ZAP), potężne narzędzie dla systemów Linux, macOS i Windows, które można pobrać bezpłatnie (www.zaproxy.org). ZAP to serwer proxy HTTP, który przetwarza żądania HTTP między przeglądarką a użytkownikiem. Rysunki w tej sekcji mają na celu pokazanie jednego narzędzia, którego można użyć do zbierania informacji o witrynie firmy i wykrywania wszelkich istniejących luk w zabezpieczeniach. Ważniejsze od konkretnego narzędzia jest zrozumienie procesu, którego używa tester bezpieczeństwa, rozpoczynając test bezpieczeństwa. Należy pamiętać, że skanowanie witryny za pomocą ZAP należy wykonywać tylko wtedy, gdy ma się do tego uprawnienia. Skanowanie witryny w poszukiwaniu luk w zabezpieczeniach jest atakiem, a wykonywanie tego skanowania bez autoryzacji może prowadzić do problemów. Można pobrać urządzenie wirtualnego pudełka o nazwie Metasploitable2 i użyć go jako celu skanowania (https://sourceforge.net/projects/metasploitable/ files/Metasploitable2). W rzeczywistości to właśnie zrobiono, aby uchwycić dane ZAP w tym module. ZAP wymaga zainstalowania Javy (pobranej ze strony www.java.com). Aby użyć ZAP do zbierania informacji ze strony internetowej lub aplikacji internetowej, musisz zmienić ustawienia w przeglądarce używanej do uzyskiwania dostępu do strony internetowej. ZAP ma funkcję o nazwie Launch Browser na karcie Szybki start, która edytuje konfigurację przeglądarki internetowej, aby kierować ruch przez serwer proxy ZAP. Umożliwia to narzędziu ZAP przechwytywanie i manipulowanie ruchem wysyłanym między przeglądarką internetową a docelowym serwerem internetowym. Aby użyć funkcji Launch Browser, wybierz kartę Szybki start, wybierz przeglądarkę, której chcesz użyć, z menu rozwijanego obok przycisku Launch Browser, a następnie kliknij przycisk Launch Browser. Rysunek 4-2 przedstawia funkcję Launch Browser z wybraną przeglądarką Firefox. Po skonfigurowaniu przeglądarki możesz (lub atakujący) użyć jej w ZAP, aby przejść do witryny docelowej. Rysunek 4-3 przedstawia witrynę docelową w przeglądarce Firefox. W tym przypadku do określenia witryny użyto adresu IP, a nie adresu URL. W ZAP docelowa witryna jest teraz wyświetlana na karcie Historia w dolnym panelu i na liście Witryny w lewym panelu. Możesz kliknąć prawym przyciskiem myszy witrynę w dowolnej lokalizacji, wskazać Attack w menu skrótów, a następnie kliknąć Spider. W oknie podręcznym, które otwiera się po wybraniu Spider, kliknij przycisk Start Scan, aby rozpocząć skanowanie. Przeszukiwanie (lub indeksowanie) to zautomatyzowany sposób odkrywania stron witryny poprzez podążanie za linkami. W ciągu kilku sekund ścieżki do stron internetowych w „przeszukiwanej” witrynie, w tym nazwy plików, są wyświetlane na karcie adresów URL. Przeszukiwanie nie jest atakiem, ale eksploracją witryny w poszukiwaniu treści. Jest to cichszy, przyjaźniejszy sposób analizowania witryny. Zobacz Rysunek 4. Po przeszukaniu witryny możesz ją aktywnie przeskanować, korzystając z funkcji ZAP Attack. Atak to aktywne skanowanie, które najpierw przeszukuje witrynę, a następnie wysyła do serwera WWW serię żądań mających na celu identyfikację luk w zabezpieczeniach. Po zakończeniu ZAP wyświetla luki w zabezpieczeniach na karcie Alerty. Możesz wyeksportować informacje o lukach w zabezpieczeniach do formatu raportu HTML. Rysunek 4-6 przedstawia przykładowy raport HTML z podsumowaniem ustaleń na górze i szczegółami dotyczącymi luk o średnim ryzyku na dole. Jak widać, skanowanie w poszukiwaniu ataków pozwala przetestować obszary witryny, które mogą mieć problemy. Wszelkie luki w zabezpieczeniach witryny są oznaczone w kolumnie Poziom ryzyka jako Wysoki, Średni, Niski lub Informacyjny. Na rysunku 4-6 poziomy ryzyka są oznaczone jako Niski i Średni. Gromadzenie informacji o konkurencji poprzez skanowanie tego typu jest czasochłonne, a im więcej się dowiesz, tym głębiej będziesz chciał kopać. Ustaw rozsądny czas trwania tej fazy swojego dochodzenia, aby nie spędzać zbyt dużo czasu na skanowaniu. Z drugiej strony nie chcesz spieszyć się ze zbieraniem informacji, ponieważ wiele z tego, czego się dowiesz, może być wykorzystane do dalszych testów i dochodzeń.

Korzystanie z innych narzędzi Footprinting

Narzędzie Whois jest powszechnym narzędziem internetowym do zbierania informacji o adresie IP i domenie. Mając tylko adres internetowy firmy, możesz odkryć ogromną ilość informacji. Niestety, atakujący mogą również wykorzystać te informacje. Często firmy nie zdają sobie sprawy, że publikują informacje w sieci, z których mogą korzystać przestępcy komputerowi. Narzędzie Whois dostarcza informacji o adresach IP firmy i wszelkich innych domenach, których firma może być częścią. W Ćwiczeniu 4-1 ćwiczysz korzystanie z funkcji Domain Dossier i whois.domaintools.com Whois.

Aktywność 4-1: Korzystanie z narzędzi do śledzenia

Czas trwania: 30 minut

Cel: Naucz się korzystać z narzędzi do śledzenia (znanych również jako pasywne narzędzia rozpoznawcze), w szczególności Domain Dossier i whois.domaintools.com funkcji Whois.

Opis: Testerzy bezpieczeństwa muszą wiedzieć, jak korzystać z narzędzi do zbierania informacji o sieciach. Dzięki funkcji Whois można odkryć, które czynniki konfiguracji sieci mogą być wykorzystywane do atakowania sieci.

1. Uruchom przeglądarkę internetową i przejdź do https://centralops.net/co/domaindossier.aspx.

2. Wpisz mit.edu w polu tekstowym domeny lub adresu IP, zaznacz pole wyboru rekordu whois domeny, a następnie kliknij przycisk Go. Przewiń w dół, aby wyświetlić wyświetlane informacje. Wiele domen zmniejsza ilość ujawnianych informacji, aby poprawić bezpieczeństwo. Zwróć uwagę na wiersz na rysunku, który brzmi „Przeczytaj o zmniejszonych danych Whois ze względu na GDPR". GDPR to ogólne rozporządzenie o ochronie danych, zbiór przepisów Unii Europejskiej (UE) regulujących ochronę danych osobowych. Każdy kraj, który chce prowadzić interesy z UE, musi przestrzegać tych przepisów dotyczących ochrony.

3. Zanotuj wymienione adresy IP i serwery nazw

4. Wpisz nazwy domen kilku innych organizacji w polu tekstowym domeny lub adresu IP i powtórz kroki 2 i 3. Niektóre organizacje są dyskretne w kwestii tego, co jest wymienione w ich rekordach domen. Na przykład opisując kontakt administracyjny, pokazanie tylko stanowiska jest bezpieczniejsze niż podanie rzeczywistego nazwiska, jak wkrótce odkryjesz.

5. Otwórz nową kartę w przeglądarce internetowej i przejdź do https:// whois.domaintools.com.

6. Wykonaj kroki od 2 do 4 ponownie, ale używając funkcji wyszukiwania w witrynie whois.domaintools.com. Jak wyniki mają się do Domain Dossier?

7. Pozostaw przeglądarkę internetową otwartą do następnej czynności

Korzystanie z adresów e-mail

Po zapoznaniu się z informacjami, które możesz zebrać za pomocą poleceń omówionych w tym module, możesz się zastanawiać, co jeszcze możesz zrobić. Znajomość adresu e-mail użytkownika może pomóc Ci kopać jeszcze głębiej. Na podstawie konta e-mail wymienionego w wynikach DNS możesz odkryć, że format adresu e-mail firmy to pierwsza litera imienia, po której następuje nazwisko i sekwencja @companyname.com. Możesz znaleźć inne konta e-mail pracowników, uzyskując firmową książkę telefoniczną lub przeszukując Internet w poszukiwaniu odniesień @companyname.com. Groups.google.com to idealne narzędzie do tego zadania. W Ćwiczeniu 4-2 używasz go do znajdowania firmowych adresów e-mail. Pamiętaj, że Twoim celem jest poznanie tego, co atakujący mogą odkryć

za pośrednictwem poczty e-mail. Jako etyczny tester bezpieczeństwa wykorzystałbyś te informacje tylko do zabezpieczania systemów.

Ćwiczenie 4-2: Identyfikowanie kont e-mail firmy

Czas trwania: 30 minut

Cel: Określenie adresów e-mail pracowników firmy.

Opis: Znajomość adresów e-mail pracowników może pomóc w odkrywaniu luk w zabezpieczeniach i gromadzeniu danych wywiadowczych dotyczących konkurencji. Na przykład możesz odkryć, że pracownik dołączył do grupy dyskusyjnej, używając swojego firmowego konta e-mail i udostępnił zastrzeżone informacje o firmie. Pracownicy IT, publikując pytania techniczne w grupie dyskusyjnej, mogą ujawnić szczegółowe informacje o zaporze sieciowej firmy lub systemie IDS, a dyrektor ds. marketingu może wspomnieć o nowej strategii kampanii reklamowej, którą firma rozważa.

1. W razie potrzeby uruchom przeglądarkę internetową i przejdź do https://groups.google.com.

2. Na pasku wyszukiwania wybierz Wszystkie grupy i wiadomości w pierwszym polu, wpisz @microsoft.com w drugim polu, a następnie naciśnij Enter. Ta metoda to szybki i łatwy sposób na znalezienie kont e-mail osób publikujących pytania w domenie Microsoft.

3. Przewiń listę elementów w dół i poszukaj postów od pracowników pracujących w różnych firmach. (Wskazówka: Wybierz wpisy zawierające „Re:" na liście. Zazwyczaj są to odpowiedzi na pytania wysłane przez pracowników.) Lista będzie się różnić, ale powinna dać ci pojęcie o niebezpieczeństwie związanym z używaniem adresu e-mail firmy podczas publikowania pytań na forach lub grupach dyskusyjnych.

4. W nowym zapytaniu wpisz @cisco.com i naciśnij Enter. Teraz możesz dowiedzieć się, kto publikuje pytania do firmy ochroniarskiej Cisco. Najprawdopodobniej posty pochodzą od użytkowników produktów Cisco. Czy widzisz, w jaki sposób atakujący mógłby wykorzystać te informacje?

5. Przewiń listę i poszukaj pytań od pracowników firmy ochroniarskiej i klientów, którzy chcą uzyskać poradę. Czy atakujący mogliby wykorzystać te informacje w złośliwych celach? Jeśli tak, w jaki sposób?

6. Czy znalazłeś jakieś informacje, które mogłyby być przydatne dla testera bezpieczeństwa? Jak stare są wiele zwróconych linków?

7. Aby wyświetlić nowsze posty, zmodyfikuj swoje zapytanie, aby uwzględnić „2020" i „2021". (Uwzględnij cudzysłowy wokół wyszukiwanych terminów

UWAGA

W Aktywności 4-2 nie wyszukiwałeś pełnych adresów e-mail. Jeśli jednak znasz adres e-mail użytkownika, możesz go wpisać na stronie wyszukiwania groups.google.com i przeprowadzić ukierunkowane wyszukiwanie wiadomości e-mail dotyczących tego użytkownika. W przypadku Projektu 4-1 masz szansę wyszukać konkretny adres e-mail. Jeśli przeprowadzałeś test bezpieczeństwa na żywo, wyszukałbyś konta e-mail pracowników IT i innych kluczowych pracowników.

Korzystanie z podstaw protokołu HTTP

Przypomnij sobie, że protokół HTTP działa na porcie 80, a protokół HTTPS (bezpieczna wersja protokołu HTTP) działa na porcie 443. Obie wersje wykorzystują polecenia HTTP (znane również jako metody) do interakcji z serwerami internetowymi. Tester bezpieczeństwa może pobierać informacje z serwera internetowego za pomocą poleceń HTTP. Prawdopodobnie widziałeś już wcześniej kody błędów klienta

HTTP, takie jak 404 Not Found. Podstawowa znajomość protokołu HTTP może być korzystna dla testerów bezpieczeństwa i nie musisz znać zbyt wielu kodów, aby wyodrębnić informacje z serwera internetowego. Jeśli znasz kody zwrotne generowane przez serwer internetowy, możesz określić, jaki system operacyjny jest używany na komputerze, na którym przeprowadzasz test bezpieczeństwa. Tabela 4-2 zawiera listę typowych błędów klienta HTTP, a Tabela 4-3 zawiera listę błędów serwera HTTP, które mogą wystąpić. Ponadto musisz zrozumieć niektóre z dostępnych metod HTTP, pokazanych w Tabeli 4-4. Nie musisz biegle posługiwać się metodami HTTP, ale musisz być wystarczająco biegły, aby używać najprostszej metody HTTP: GET / HTTP/1.1.

WSKAZÓWKA Bardziej szczegółową definicję metod HTTP można znaleźć w dokumencie RFC 2616.

Jeśli znasz metody HTTP, możesz wysłać żądanie do serwera WWW i na podstawie wygenerowanego wyniku określić, jakiego systemu operacyjnego używa serwer WWW. Możesz również znaleźć inne informacje, które mogłyby zostać wykorzystane w ataku, takie jak znane luki w zabezpieczeniach systemów operacyjnych i innego oprogramowania. Po ustaleniu, jakiej wersji systemu operacyjnego używa firma, możesz wyszukać wszelkie exploity, które mogłyby zostać wykorzystane przeciwko systemom tej sieci.

Aktywność 4-3: Korzystanie z metod HTTP

Czas trwania: 30 minut

Cel: Określenie informacji o serwerze WWW za pomocą metod HTTP.

Opis: Uzbrojony w informacje zebrane z firmowego serwera WWW za pomocą podstawowych metod HTTP, tester bezpieczeństwa może odkryć luki w zabezpieczeniach systemu i wykorzystać te informacje do dalszych testów. Na przykład zapytanie do serwera WWW może ujawnić, że serwer działa pod kontrolą systemu operacyjnego Linux i używa oprogramowania Apache. W tej aktywności używasz polecenia nc (netcat), aby połączyć się z portem 80, a następnie używasz metod HTTP. Większość serwerów WWW używa portu 443. Te, które używają portu 80, są podatne na ataki, więc znalezienie serwerów korzystających z portu 80 i użycie netcat do ich zbadania jest prawidłową aktywnością testowania penetracyjnego.

1. Uruchom komputer z systemem Kali Linux. Zaloguj się, a następnie otwórz powłokę poleceń, klikając ikonę terminala na pasku zadań panelu. W wierszu polecenia wpisz nc www.google.com 80 i naciśnij Enter. (Port 80 to port HTTP.)

WSKAZÓWKA Komputer z systemem Kali Linux może być fizycznym komputerem, na którym zainstalowano system Kali Linux, wirtualną maszyną z systemem Kali Linux, którą utworzyłeś, lub instalacją Kali Linux na żywo z możliwością rozruchu na pamięci USB. Jeśli potrzebujesz pomocy, wyszukaj w Internecie instrukcje dotyczące wykonywania tych opcji komputera z systemem Kali Linux.

2. W następnym wierszu wpisz oPtions / HttP/1.1 i naciśnij Enter. (Zwróć uwagę na spacje wokół znaku ukośnika między słowami OPTIONS i HTTP.)

3. W następnym wierszu wpisz HOST:127.0.0.1 i naciśnij Enter dwa razy. Chociaż metoda OPTIONS / HTTP/1.1 nie była dozwolona, odpowiedź informuje, jakie opcje są dozwolone. Nic dziwnego, że Google nie zezwala na polecenia, które mogą ujawnić hakerom luki w zabezpieczeniach.

4. Jakie informacje wygenerowane przez polecenie nc mogą być przydatne dla testera bezpieczeństwa? Jakie inne opcje są dostępne podczas uzyskiwania dostępu do tego serwera WWW?

5. Wpisz nc www.google.com 80 i naciśnij Enter ponownie.

6. W następnym wierszu wpisz Head / HttP/1.0 i naciśnij Enter dwa razy, aby pobrać informacje o nagłówku. Zwróć uwagę na dodatkowe informacje wygenerowane przez metodę HEAD, takie jak wskazanie, że połączenie zostało zamknięte i określenie długości zawartości (0 bajtów).

7. W wierszu poleceń terminala wpisz wget www.google.com i naciśnij Enter. To polecenie pobiera stronę indeksu (stronę startową) witryny www.google.com i przechowuje kod HTML tej strony lokalnie na Twoim komputerze. Możesz otworzyć wynikowy plik w edytorze, aby go zbadać.

8. Zamknij powłokę terminala i wyloguj się z systemu Linux, aby wykonać następną czynność.

WSKAZÓWKA Aby zobaczyć dodatkowe parametry polecenia nc, możesz wpisać nc -h w wierszu poleceń.

Korzystanie z innych metod zbierania informacji

Do tej pory poznałeś kilka metod zbierania informacji ze stron internetowych i adresów e-mail firmy. Mając tylko adres URL, możesz ustalić, z którego serwera WWW i systemu operacyjnego korzysta firma, a także poznać nazwiska pracowników IT. Musisz być świadomy innych metod, których atakujący używają do zbierania informacji o firmie. Niektóre z tych metod, takie jak używanie plików cookie i sygnałów nawigacyjnych, są nieuczciwe. Jednym z typów sygnałów nawigacyjnych jest błąd sieciowy.

Wykrywanie plików cookie i błędów sieciowych

Plik cookie to plik tekstowy generowany przez serwer sieciowy i przechowywany w przeglądarce użytkownika. Informacje w tym pliku są wysyłane do serwera sieciowego, gdy użytkownik powraca na stronę internetową. Na przykład powracającemu klientowi można wyświetlić spersonalizowaną stronę internetową, gdy ponownie odwiedzi stronę internetową sklepu internetowego. Niektóre pliki cookie mogą powodować problemy z bezpieczeństwem, ponieważ nieuczciwe osoby mogą przechowywać w plikach cookie dane osobowe, które mogą zostać wykorzystane do ataku na komputer lub serwer. Inne pliki cookie przechowują poufne informacje (takie jak dane uwierzytelniające użytkownika) w postaci niezaszyfrowanej. Web bug to plik obrazu o wymiarach 1 × 1 piksel, do którego odwołuje się znacznik <IMG>, zwykle działający z plikiem cookie. Jest to jeden z typów sygnalizatora internetowego, ukryta grafika lub fragment kodu osadzony na stronie internetowej w celu śledzenia aktywności użytkownika i zbierania informacji o użytkowniku. Cel sygnalizatora internetowego jest podobny do celu spyware i adware: zbieranie informacji o osobie odwiedzającej stronę internetową, takich jak adres IP, czas wyświetlenia sygnalizatora internetowego oraz typ przeglądarki użytej do wyświetlenia strony. Wszystkie te informacje mogą być przydatne dla hakerów. Web bugi nie pochodzą z tej samej strony internetowej, co twórca strony internetowej. Pochodzą od firm zewnętrznych specjalizujących się w zbieraniu danych. Ponieważ web bugi są rodzajem standardowego pliku graficznego, zwykle GIF, nie mogą zostać zablokowane przez przeglądarkę ani odrzucone przez użytkownika. Ponadto web bugi zwykle dopasowują się do koloru tła strony internetowej, co czyni je niewidocznymi. Inna forma sygnalizatora internetowego osadza kod JavaScript na stronach internetowych witryny. Ten kod JavaScript zwraca informacje o śledzeniu do organizacji zbierającej dane. Ten typ sygnalizatora internetowego jest również ukryty przed użytkownikiem, ponieważ jest częścią kodu tła strony internetowej i nie jest widoczny. Jeśli nie masz narzędzia do wykrywania błędów internetowych lub sygnalizatorów internetowych JavaScript, jednym ze sposobów ich znalezienia jest zbadanie kodu źródłowego strony internetowej w celu znalezienia pliku w tagu ładowanym z serwera internetowego, który różni się od innych plików graficznych na stronie. Użycie innego serwera może wskazywać, że plik graficzny jest błędem internetowym. Poszukaj również fragmentów JavaScript, które wydają się zbierać i wysyłać dane do znanych organizacji zbierających dane. Innym sposobem wykrywania sygnalizatorów internetowych jest sprawdzenie połączeń sieciowych na komputerze (być może za pomocą netstat) lub

przechwycenie ruchu sieciowego (być może za pomocą Wiresharka) i sprawdzenie, czy dane są wysyłane do znanych organizacji zbierających dane. W Ćwiczeniu 4-5 badasz temat sygnalizatorów internetowych. Podczas tego prawdopodobnie odkryjesz, kim są te „organizacje zbierające dane". Specjaliści ds. bezpieczeństwa muszą być świadomi istnienia plików cookie i sygnałów nawigacyjnych, aby chronić komputery firmowe przed tymi narzędziami służącymi do gromadzenia informacji.

Ćwiczenie 4-4: Odkrywanie plików cookie na stronach internetowych

Czas trwania: 30 minut

Cel: Określenie, czy pliki cookie są obecne na stronach internetowych.

Opis: Wiele firm umieszcza pliki cookie na swoich stronach internetowych, aby zbierać informacje o użytkownikach odwiedzających ich witryny. Informacje te mogą być wykorzystywane na przykład do analizy konkurencji lub określania nawyków zakupowych użytkowników. Testerzy bezpieczeństwa powinni wiedzieć, jak sprawdzić, czy strona internetowa zawiera pliki cookie.

1. Uruchom komputer w systemie Windows i uruchom przeglądarkę internetową Microsoft Edge. Jeśli korzystałeś z tej przeglądarki w systemie Windows, pliki cookie prawdopodobnie są już załadowane na Twoim komputerze, więc możesz je przeanalizować, a także nowe pliki cookie utworzone w tej aktywności, odwiedzając nową witrynę.

2. Kliknij przycisk Ustawienia i więcej (…) w prawym górnym rogu okna Edge, a następnie kliknij Ustawienia.

3. Na stronie Ustawienia kliknij łącze Pliki cookie i uprawnienia witryny w lewym panelu, a następnie kliknij Zarządzaj i usuwaj pliki cookie i dane witryny w prawym panelu.

4. Na stronie Pliki cookie i dane witryny kliknij łącze Zobacz wszystkie pliki cookie i dane witryny. Wyświetlana jest lista plików cookie, jak pokazano na rysunku 4-12. Wymienione pliki cookie zależą od witryn, które już odwiedziłeś w tej przeglądarce.

5. Kliknij ikonę rozwijania (strzałka w dół) po prawej stronie wymienionej witryny, aby otworzyć listę określonych grup plików cookie. Kliknij ikonę Wyświetl dane lokalne (strzałka w prawo) dla witryny, aby wyświetlić określone pliki cookie zapisane dla grupy. Na liście określonych plików cookie kliknij ikonę rozwijania, aby zobaczyć dane zapisane w pliku cookie. Kliknięcie ikony kosza umożliwia usunięcie pojedynczych plików cookie lub wszystkich plików cookie dla witryny. Sprawdź, czy masz pliki cookie z Amazon.com. Jeśli tak, możesz je wyczyścić lub wybrać witrynę, której wcześniej nie odwiedziłeś i użyć jej do ćwiczenia sprawdzania plików cookie w następnym kroku.

6. Otwórz nową kartę i przejdź do www.amazon.com (lub innej wybranej witryny). Wyszukaj buty.

7. Wróć do zakładki z informacjami o wszystkich plikach cookie i danych witryny (wróć, jeśli kliknąłeś głębiej), odśwież stronę, a następnie rozwiń wpis amazon.com. Czy pliki cookie są tworzone dla czegoś więcej niż tylko domeny amazon.com? Otwórz informacje o plikach cookie dla amazon.com, aż wyświetlisz dane zawarte w rzeczywistych plikach cookie. Czy którykolwiek z plików cookie zawiera dane osobowe?

8. Jeśli masz czas, odwiedź niektóre witryny, które wymagają zalogowania się za pomocą nazwy konta i hasła. Sprawdź, czy te witryny tworzą pliki cookie z danymi osobowymi.

Ćwiczenie 4-5: Badanie sygnałów nawigacyjnych i prywatności

Wymagany czas: 60 minut

Cel: Zdobycie wiedzy na temat gromadzenia danych za pomocą sygnałów nawigacyjnych.

Opis: Sygnały nawigacyjne są uważane za bardziej inwazyjne niż pliki cookie. Jako specjalista ds. bezpieczeństwa powinieneś zrozumieć, w jaki sposób firmy wykorzystują je do gromadzenia informacji o użytkownikach odwiedzających witryny.

1. Uruchom przeglądarkę internetową w systemie Windows, jeśli to konieczne, i przejdź do https://en.wikipedia.org/wiki/web_beacon.

2. Przeczytaj cały artykuł, zwracając uwagę na użyte metody oraz organizacje i aplikacje, które z nich korzystają.

3. Przeprowadź wyszukiwanie w sieci, używając terminu web beacons w połączeniu z nazwami różnych firm mediów społecznościowych i wyszukiwarek, takich jak web beacons google. Przeczytaj niektóre informacje zawarte w wynikach zapytania i zanotuj swoje odkrycia.

4. Napisz jednostronicowy raport na temat swoich odkryć. Twój raport powinien zawierać Twoją opinię na temat ukrytych metod śledzenia, które odkryłeś, a także opis swoich odkryć. Przedstaw ten raport członkom swojej klasy lub członkowi rodziny.

UŻYWANIE TRANSFERÓW STREF SYSTEMU NAZW DOMEN

Innym sposobem zbierania informacji podczas odciskania śladu sieci jest użycie systemu nazw domen (DNS). Jak wiesz z nauki podstawowych pojęć sieciowych, DNS jest składnikiem sieci odpowiedzialnym za rozwiązywanie nazw hostów na adresy IP i odwrotnie. Ludzie wolą zapamiętać adres URL niż adres IP. Niestety, używanie adresów URL wiąże się z wysoką ceną. DNS jest głównym obszarem potencjalnej podatności na ataki sieciowe. Nie wdając się w zbytnie szczegóły, DNS używa serwerów nazw do rozwiązywania nazw. Po ustaleniu, jakiego serwera nazw używa firma, możesz spróbować przenieść wszystkie rekordy, za które odpowiada serwer DNS. Ten proces, nazywany transferem strefy, można wykonać za pomocą polecenia dig. (Jeśli znasz polecenie nslookup, dig jest teraz zalecanym poleceniem). Aby określić główny serwer DNS firmy, możesz poszukać serwera DNS zawierającego rekord Start of Authority (SOA). Rekord SOA pokazuje, za które strefy lub adresy IP odpowiada serwer DNS. Po określeniu głównego serwera DNS możesz wykonać kolejny transfer strefy, aby zobaczyć wszystkie komputery hosta w sieci firmy. Innymi słowy, transfer strefy daje Ci diagram sieci organizacji. Możesz użyć tych informacji, aby zaatakować inne serwery lub komputery, które są częścią infrastruktury sieciowej. Narzędzia, o których się właśnie dowiedziałeś, nie są jedynym sposobem zbierania informacji. Czasami informacje o firmie są zbierane przy użyciu umiejętności nietechnicznych. W rzeczywistości najlepsi hakerzy niekoniecznie są najbardziej technicznie biegłymi ludźmi. Zamiast tego posiadają bardziej podstępną — i często niedocenianą — umiejętność zwaną inżynierią społeczną, omówioną w następnej sekcji.

Aktywność 4-6: Identyfikowanie adresów IP za pomocą transferów stref (opcjonalnie)

Czas trwania: 30 minut

Cel: Wykonaj transfer strefy na serwerze DNS.

Opis: Podczas wyznaczania śladu sieci musisz znaleźć adresy IP i nazwy hostów wszystkich serwerów, komputerów i innych węzłów podłączonych do sieci. Za pomocą poleceń takich jak dig możesz wykonać transfery stref rekordów DNS. Następnie możesz użyć tych informacji do tworzenia diagramów

sieciowych i uzyskania dobrego obrazu organizacji sieci. Na przykład możesz zobaczyć, ile hostów znajduje się w sieci i ile podsieci zostało utworzonych.

UWAGA

W tym przykładzie zonetransfer.me służy do zademonstrowania przeprowadzania transferu strefy, dzięki czemu możesz zobaczyć, jakie informacje można zebrać z transferu strefy. W momencie pisania tego tekstu transfer strefy za pomocą zonetransfer.me działał. Jednak wiele organizacji zaostrza zabezpieczenia i nie zezwala już na transfery stref, ale nadal powinieneś znać kroki, aby je wykonać.

1. Zaloguj się do Kali Linux i otwórz powłokę terminala. (Twoja instalacja Kali Linux może być fizycznym komputerem, maszyną wirtualną lub dyskiem USB z możliwością rozruchu Kali Linux na żywo). W wierszu poleceń wpisz dig NS zonetransfer.me i naciśnij Enter. Wyświetlane są dwa serwery nazw oznaczone jako „NS": nsztm1.digi.ninja i nsztm2.digi.ninja. (Informacje te mogą ulec zmianie do czasu wykonania tej czynności. Jeśli tak się stanie, poproś instruktora o wskazówki). Możesz zobaczyć informacje, które były dostępne dla hakera podczas transferów stref. Jeśli administrator DNS poprawnie skonfigurował DNS, poniższe polecenia nie powinny działać. Nieprawidłowe konfiguracje DNS sprawiają, że systemy są podatne na ataki.

2. Aby wykonać transfer strefy na serwerze DNS nsztm1.digi.ninja, wpisz dig axfr @nsztm1.digi.ninja zonetransfer. me i naciśnij Enter. Serwer nsztm1.digi.ninja to ten, dla którego próbujesz wykonać transfer strefy, a drugie polecenie zonetransfer.me to domena, w której znajduje się serwer. Po krótkim oczekiwaniu pojawia się kilka rekordów.

3. Wykonaj transfer ponownie, ale tym razem użyj parametru | less, wpisując dig axfr @nsztm1.digi.ninja zonetransfer.me | less i naciskając Enter.

4. Naciśnij Enter lub spację, aby wyświetlić dodatkowe rekordy, a następnie naciśnij q, aby zakończyć. Zamknij powłokę terminala i wyloguj się z systemu Linux.

UWAGA

Jako tester bezpieczeństwa zawsze powinieneś mieć świadomość, że atak może się udać jednego dnia, a nie udać innego dnia. Dlatego jeśli atak zadziała, skopiuj wszystkie pliki i dane uzyskane podczas włamania na dysk twardy lub dysk USB tak szybko, jak to możliwe. W przykładzie w Ćwiczeniu 4-6 tester bezpieczeństwa uzyskałby już niezbędne informacje i zapisał je na serwerze firmy. Nie miałoby znaczenia, gdyby DNS został prawidłowo skonfigurowany po przeprowadzeniu transferu strefy. Koniec gry!

Narzędzia, o których się właśnie dowiedziałeś, nie są jedynym sposobem zbierania informacji. Czasami informacje o firmie są zbierane przy użyciu umiejętności nietechnicznych. W rzeczywistości najlepsi hakerzy niekoniecznie są najbardziej biegłymi technicznie ludźmi. Zamiast tego posiadają bardziej podstępną — i często niedocenianą — umiejętność zwaną inżynierią społeczną, omówioną w następnej sekcji.

WPROWADZENIE DO INŻYNIERII SPOŁECZNEJ

Możesz zbierać informacje bez używania narzędzi hakerskich lub oprogramowania do zbierania informacji. Jedną z nietechnicznych metod zbierania informacji jest inżynieria społeczna. Inżynieria społeczna wykorzystuje sztukę oszustwa, aby wydobyć cenne informacje od dobrze nastawionych osób, które próbują być pomocne. Najlepszą obroną przed inżynierią społeczną jest szkolenie użytkowników, ponieważ obiektem, który jest hakowany w celu uzyskania informacji, jest osoba, a nie komputer. Szkolenie użytkowników, aby byli świadomi taktyk inżynierii społecznej, jest najlepszą

obroną. Sztuka inżynierii społecznej istnieje znacznie dłużej niż komputery. Inżynieria społeczna wykorzystuje wiedzę o naturze ludzkiej do zbierania informacji od ludzi. W atakach komputerowych informacjami są zazwyczaj hasła do sieci lub inne informacje, których atakujący może użyć do złamania zabezpieczeń sieci. Na przykład sprzedawca może zbierać dane osobowe klientów, takie jak dochód, hobby, życie towarzyskie i preferencje muzyczne, zadając klientowi odpowiednie pytania. Sprzedawca wykorzystuje umiejętności komunikacyjne, aby nawiązać kontakt z klientami i stworzyć wiadomość, która przekona klientów do zakupu produktu lub usługi. Inżynierowie społeczni mogą stosować podobne taktyki perswazji wraz z zastraszaniem, przymusem, wymuszeniami, a nawet szantażem, aby zebrać potrzebne im informacje. Inżynierowie społeczni są prawdopodobnie największym zagrożeniem dla bezpieczeństwa sieci i najtrudniejszymi do ochrony. Prawdopodobnie słyszałeś powiedzenie „Po co próbować złamać hasło, skoro można po prostu o nie poprosić?" Wielu atakujących robi właśnie to: proszą użytkowników o hasła i inne dane uwierzytelniające. Niestety, wielu użytkowników daje atakującym wszystko, czego potrzebują, aby włamać się do sieci. Większość osób, które pracowały w dziale pomocy technicznej lub przy obsłudze sieci, wie, że to prawda. Nawet jeśli polityka firmy stanowi, że haseł nie wolno nikomu podawać, użytkownicy często myślą, że ta polityka nie dotyczy personelu IT i głośno je recytują, gdy technik IT siedzi przed ich komputerami. Personel IT nie chce znać hasła użytkownika. Zwłaszcza nie chce, aby użytkownik wypowiadał je na głos lub wpisywał w wiadomościach e-mail. Jednak użytkownicy często nie uważają haseł firmowych za prywatne, więc nie chronią ich tak ostrożnie, jak osobistych haseł lub kodów PIN. Użytkownicy mogą nie sądzić, że dane przechowywane na komputerach firmowych mogą być interesujące dla atakującego. Inżynierowie społeczni wiedzą, jak uspokoić tego typu użytkowników. Poniżej znajduje się przykład typowej taktyki inżynierii społecznej. Najpierw inżynier społeczny podszywa się pod „Mike'a", imię, które znalazł po wykonaniu transferu strefy i sprawdzeniu serwera DNS firmy. Mike może nie być obecnym punktem kontaktowym IT (POC), ale to nie ma znaczenia. W zależności od wielkości firmy użytkownicy często nie znają wszystkich pracowników IT. Następnie inżynier społeczny dzwoni do Taishy, imienia pracownika, które znalazł w informacjach o transferze strefy i kilku stronach internetowych firmy, które pokazują format adresów e-mail. Aby uzyskać numer telefonu, dzwoni do głównej centrali firmy i pyta o Taishę. Następnie mówi, że chce zostawić wiadomość dla Taishy i prosi o przekierowanie do jej poczty głosowej. „Taisha jest teraz w biurze", odpowiada przyjazna recepcjonistka. „Czy chcesz, żebym cię z nią połączył?" Inżynier społeczny mówi: „Do diabła, dzwoni druga linia. Zapomniałem jej numeru wewnętrznego. Czy możesz mi go podać, a ja oddzwonię za kilka minut? Naprawdę muszę odebrać ten telefon". W tej rozmowie taktyka inżyniera społecznego polega na stworzeniu poczucia pilności, ale zachowaniu uprzejmości. Taktyka ta zwykle działa, ponieważ większość recepcjonistek nie widzi problemu w połączeniu rozmówcy z pracownikiem lub podaniu bezpośredniego numeru lub numeru wewnętrznego pracownika. W końcu dzwoniący zna imię Taishy i wydaje się, że ją zna. „Numer wewnętrzny 4100", mówi recepcjonistka. „Dzięki! Muszę iść", odpowiada inżynier społeczny. Po około 30 minutach inżynier społeczny ponownie dzwoni do firmy. „Dzień dobry. Numer wewnętrzny 4101, proszę", pyta. Recepcjonistka łączy go, a mężczyzna odbiera: „Dillon Bayard, księgowość". „Przepraszam, Dillon. Tu Mike. Dzwoniłem do Taishy, ale chyba przez pomyłkę dostałem twój numer wewnętrzny. Taisha miała problem z połączeniem z Internetem, więc sprawdzamy informacje o adresie IP. Właśnie naprawiliśmy jej system. Czy ty też masz problem?" Dillon mówi: „Wygląda na to, że tylko Dział Księgowości ma problem z konfiguracją VLAN". Mike pyta: „Nadal używasz Windows 7?" Dillon odpowiada, że nie, ale mówi Mike'owi, jakiego systemu operacyjnego używa. Dillon prawdopodobnie czuje, że zna Mike'a, chociaż tak nie jest. Innym sposobem, aby dowiedzieć się, jak działa personel IT, jest to, aby Mike podszywał się pod Dillona i zadzwonił z pytaniem lub problemem, który ma. Mike dowiedziałby się wtedy, jak pracownik pomocy technicznej obsługuje połączenie. Czy pomoc techniczna wystawia zgłoszenie pomocy technicznej? Czy Dillon musi podać dzwoniącemu jakiekolwiek informacje poza swoim imieniem i numerem telefonu? Wiele biur pomocy technicznej wymaga

przypisania unikalnego numeru do zgłoszenia pomocy, dopóki problem nie zostanie rozwiązany. Inżynier społeczny użył imienia Taishy, aby nadać swojemu zgłoszeniu większą wiarygodność. Ponadto, ponieważ zebrał informacje o systemie operacyjnym innymi sposobami, wykorzystał tę wiedzę, jak pokazuje jego pytanie o wersję systemu Windows. Mike może spróbować uzyskać to, czego chce od Dillona, lub może zdecydować się na ostateczny atak z Taishą. Jeśli do niej zadzwoni, może rozmawiać o Dillonie, jakby byli starymi przyjaciółmi. To, czego chce, to hasło Dillona lub Taishy. Może spróbować następującego fortelu: „Dillon, jest duża szansa, że będziemy musieli wyłączyć łączność sieciową Accounting na godzinę lub dwie. Mogę skrócić ten czas dla twojego systemu do pięciu minut, jeśli będę mógł zająć się tym problemem stąd. Jedynym problemem jest to, że potrzebuję twojego hasła. Mam już twoje konto logowania jako dbayard@gmailinfo.com. Czy to prawda?" Jest duże prawdopodobieństwo, że Dillon poda swoje hasło Mike'owi przez telefon. Nie wszystkie socjotechniki odbywają się przez telefon, ale jest to prawdopodobnie najpopularniejsza metoda, ponieważ jest anonimowa i pozwala socjotechnikowi przeprowadzać wiele ataków w tej samej organizacji. Ta metoda może być trudniejsza, jeśli jeden lub dwóch pracowników usłyszy różne historie od tej samej osoby. Jednak dobrze ubrana osoba z notatnikiem również może odnieść sukces w zbieraniu informacji od pracowników. To podejście wymaga większej odwagi, ponieważ socjotechnik musi stawić czoła osobom, od których próbuje zebrać informacje. Socjotechniki badają ludzkie zachowania. Uczą się rozpoznawać cechy osobowości, takie jak nieśmiałość lub niepewność, i jak czytać mowę ciała: pochylone ramiona, unikanie kontaktu wzrokowego, nerwowe wiercenie się itp. Jeśli sztuczka jest przeprowadzana przez telefon, ton głosu osoby może dać wskazówki socjotechnice, który wykorzystuje je do zidentyfikowania najbardziej narażonej osoby w organizacji. Następnie socjotechnik wykorzystuje cechy pracownika, aby wydobyć informacje.

BAJTY BEZPIECZEŃSTWA

Najtrudniejszym zadaniem specjalisty ds. bezpieczeństwa jest uniemożliwienie inżynierom społecznym zbierania kluczowych informacji od pracowników firmy. Bez względu na to, jak dokładna jest polityka bezpieczeństwa lub ile pieniędzy wydaje się na zapory sieciowe i systemy wykrywania włamań (IDS), pracownicy nadal są najsłabszym ogniwem w organizacji. Atakujący znają tę lukę i ją wykorzystują. Pracownicy muszą być okresowo szkoleni i testowani w zakresie praktyk bezpieczeństwa. Podobnie jak ćwiczenia przeciwpożarowe pomagają przygotować ludzi do ewakuacji podczas pożaru, losowe ćwiczenia bezpieczeństwa mogą poprawić praktyki bezpieczeństwa firmy. Na przykład losowe wybieranie i testowanie pracowników każdego miesiąca w celu sprawdzenia, czy podają swoje hasła komuś wewnątrz lub na zewnątrz organizacji, może pomóc w podniesieniu świadomości i zgodności z praktykami bezpieczeństwa. Inżynierowie społeczni stosują wiele technik w próbach uzyskania informacji od niczego niepodejrzewających osób, w tym następujące:

• Pilność — „Potrzebuję informacji natychmiast, albo świat się skończy!" Na przykład inżynier społeczny może powiedzieć użytkownikowi, że potrzebuje informacji szybko, albo sieć będzie niedostępna przez długi czas, tworząc w ten sposób fałszywe poczucie pilności.

• Quid pro quo — „Mogę poprawić twoje życie, jeśli podasz mi informacje, których potrzebuję". Inżynier społeczny może obiecać użytkownikom szybszy dostęp do Internetu, na przykład, jeśli pomogą, dostarczając informacje.

• Status quo — „Wszyscy inni to robią, więc ty też powinieneś". Wykorzystując nazwiska innych pracowników, inżynier społeczny może łatwo przekonać innych do ujawnienia swoich haseł.

• Życzliwość — Ta taktyka jest prawdopodobnie najniebezpieczniejszą bronią, jaką posługują się inżynierowie społeczni. Ludzie chcą pomagać tym, którzy są dla nich mili. Powiedzenie „Łatwiej łapać muchy miodem niż octem" odnosi się również do inżynierii społecznej. • Stanowisko — przekonanie

pracownika, że zajmujesz stanowisko kierownicze w firmie, może być skutecznym sposobem na zdobycie informacji. Jest to szczególnie ważne w wojsku, gdzie ranga ma swoje przywileje. Inżynierowie społeczni mogą twierdzić, że wysoki rangą oficer prosi o informacje, więc konieczne jest ich jak najszybsze podanie.

BAJTY BEZPIECZEŃSTWA

Jako tester bezpieczeństwa nigdy nie powinieneś stosować taktyk socjotechnicznych, chyba że osoba, która cię zatrudniła, udzieli ci pisemnego pozwolenia. Powinieneś również potwierdzić, u których pracowników masz prawo przeprowadzać testy socjotechniczne i udokumentować przeprowadzane testy. Twoja dokumentacja powinna zawierać otrzymane odpowiedzi, a wszystkie wyniki testów powinny być oczywiście poufne. Szkolenie użytkowników, aby nie podawali osobom trzecim żadnych informacji o systemach operacyjnych, musi być częścią szkolenia z zakresu bezpieczeństwa. Pracownicy powinni również zostać nauczeni potwierdzania tożsamości osoby zadającej pytania. Powinni rutynowo prosić osobę o numer telefonu służbowego, aby oddzwonić, zamiast ufać nieznajomemu po drugiej stronie linii telefonicznej. Uświadomienie pracownikom, że większość włamań odbywa się za pomocą inżynierii społecznej, a nie umiejętności programowania, może zwiększyć ich czujność wobec atakujących.

Sztuka surfowania przez ramię

Inną metodą wykorzystywaną przez inżynierów społecznych do uzyskiwania dostępu do informacji jest surfowanie przez ramię. Osoba surfująca przez ramię potrafi czytać to, co użytkownicy wpisują na swoich klawiaturach, zwłaszcza nazwy logowania i hasła. Osoby surfujące przez ramię wykorzystują tę umiejętność również do czytania kodów PIN wprowadzanych na klawiaturach bankomatów lub numerów kodów dostępu używanych do otwierania drzwi z blokadami klawiatury. Kradzież numeru klawiatury jest łatwiejsza niż surfowanie przez ramię komputera, ponieważ klawiatura ma mniej znaków do zapamiętania niż klawiatura komputera.

BAJTY BEZPIECZEŃSTWA

Powszechną taktyką surferów na ramieniu jest robienie zdjęć kart kredytowych nieświadomych klientów w supermarketach i sklepach za pomocą aparatów w smartfonach. Dzięki tej technice mogą oni uchwycić numer karty kredytowej i datę ważności. Połączenie tej techniki z obserwacją klienta wprowadzającego PIN zwiększa ryzyko kradzieży tożsamości. Wielu użytkowników klawiatury nie postępuje zgodnie z tradycyjną techniką palcowania nauczaną na lekcjach pisania. Zamiast tego polują i dziobią dwoma lub trzema palcami. Jednak surferzy na barkach trenują zapamiętywanie kluczowych pozycji na standardowej klawiaturze. Standardowa klawiatura może być klawiaturą fizyczną lub wirtualną na komputerze lub urządzeniu mobilnym. Uzbrojeni w tę wiedzę surferzy mogą określić, które klawisze zostały naciśnięte, zauważając położenie na klawiaturze, a nie palec, którego używa maszynistka. Osoby surfujące na barkach znają również popularne podstawienia liter, których większość ludzi używa podczas tworzenia haseł: $ dla s, @ dla a, 1 dla i, 0 dla o i tak dalej. Wielu użytkowników uważa, że p@$$w0rd jest trudne do odgadnięcia, ale nie jest to rozwiązanie dla wprawnego surfera. Ponadto wielu użytkowników musi używać haseł zawierających znaki specjalne i często wpisują je wolniej, aby mieć pewność, że wpisują prawidłowe znaki. Wolniejsze pisanie ułatwia pracę surfera.

BAJTY BEZPIECZEŃSTWA

Ponieważ tak wiele osób zabiera na lotniska swoje urządzenia mobilne, komercyjne linie lotnicze ostrzegają klientów, aby uważali na surferów na barkach. W ciasnym samolocie można łatwo

obserwować naciskane klawisze i czytać dane na ekranie. Podróżującym zaleca się produkty zapobiegające oglądaniu ekranów poza osią, takie jak nakładki na ekran lub soczewki zabezpieczające. Wielu pracowników prowadzi interesy w samolotach, a surferzy na barkach mogą wykorzystać zebrane informacje do włamania się do systemów komputerowych w firmie. Aby zapobiec atakom typu bark-surfing, należy poinstruować użytkowników, aby nie wpisywali nazw logowania i haseł, gdy ktoś stoi bezpośrednio za nimi lub nawet w pobliżu. Należy także przestrzec użytkowników przed wpisywaniem haseł, gdy ktoś w pobliżu rozmawia przez telefon komórkowy, ze względu na szeroką dostępność telefonów z aparatem. Aby jeszcze bardziej zmniejszyć ryzyko surfowania po ramionach, upewnij się, że wszystkie ekrany wyświetlaczy są skierowane w stronę przeciwną do drzwi lub wejścia do kabiny. Ostrzeż użytkowników, aby natychmiast zmienili hasła, jeśli podejrzewają, że ktoś mógł zauważyć, jak wprowadzali hasła.

Sztuka nurkowania w śmietniku

Inną metodą wykorzystywaną przez inżynierów społecznych w celu uzyskania dostępu do informacji jest nurkowanie w śmietnikach. Chociaż nie jest to efektowna forma gromadzenia informacji, sprawdzanie śmieci może dostarczyć informacji, które mogą zostać wykorzystane przez atakujących. Na przykład wyrzucona dokumentacja komputera może wskazywać używany system operacyjny. Jeśli instrukcje dotyczą systemu Windows Server 2016, istnieje duże prawdopodobieństwo, że nowy system to nowszy system operacyjny Windows, taki jak Windows Server 2019. Czasami administratorzy sieci piszą notatki w dokumentacji lub nawet zapisują hasła, a inżynierowie socjologiczni mogą wykorzystać te informacje. Innym źródłem informacji są firmowe książki telefoniczne. Nurek w śmietniku, który znajdzie katalog zawierający listę pracowników firmy, może wykorzystać te informacje, aby udawać pracownika w celu gromadzenia informacji. Kalendarze firmowe z harmonogramami spotkań, harmonogramami urlopów pracowników itp. można wykorzystać do uzyskania dostępu do biur, które nie będą zajęte przez określony czas. Śmieci mogą być na wagę złota dla nurka w śmietniku, który wie, co z nimi zrobić. Oto kilka innych przedmiotów, które mogą być przydatne dla nurków w śmietnikach:

• Raporty finansowe

• Notatki międzybiurowe

• Wyrzucone nośniki cyfrowe

• Schematy organizacyjne firmy przedstawiające nazwiska menedżerów

• Życiorysy pracowników

• Zasady firmy lub podręczniki systemów i procedur

• Profesjonalne czasopisma lub czasopisma

• Rachunki za media

• Powiadomienia o zaproszeniach od dostawców zewnętrznych

• Raporty kierowników regionalnych

• Raporty dotyczące zapewnienia jakości

• Raporty dotyczące zarządzania ryzykiem

• Protokoły spotkań

• Raporty federalne, stanowe lub miejskie

• Wpływy z kart pracowniczych

Nurkowanie w śmietnikach może dostarczyć ogromnej ilości informacji, dlatego użytkownicy muszą zostać przeszkoleni w zakresie prawidłowego usuwania śmieci. Dyski zawierające informacje firmowe należy sformatować za pomocą oprogramowania do „czyszczenia dysku", które zapisuje binarne zera na wszystkich fragmentach dysków. To formatowanie należy wykonać co najmniej siedem razy, aby mieć pewność, że wszystkie poprzednie dane będą nieczytelne. Stare instrukcje obsługi komputera należy wyrzucić poza teren zakładu, aby nurkowie w śmietnikach nie mogli skojarzyć ich z firmą. Przed utylizacją wszystkie te przedmioty należy umieścić w zamkniętym pomieszczeniu z odpowiednimi zabezpieczeniami fizycznymi, administracyjnymi i technicznymi. Wszystkie dokumenty należy zniszczyć, nawet jeśli informacje wydają się niewinne. Inżynierowie społeczni wiedzą, jak gromadzić informacje z różnych źródeł. Ułożenie puzzli z wielu małych elementów umożliwia atakującym włamanie się do sieci.

Sztuka chodzenia na barana

Czasami testerzy bezpieczeństwa muszą wejść do części budynku, do której dostęp ma wyłącznie upoważniony personel. W tym przypadku tester lub atakujący stosuje technikę zwaną piggybackingiem. Podążanie na baranach oznacza podążanie tuż za pracownikiem mającym dostęp do danego obszaru, przy czym pracownik nie zdaje sobie sprawy, że nie użyłeś kodu PIN ani identyfikatora bezpieczeństwa, aby wejść do tego obszaru. Osoby wykwalifikowane w przewożeniu na baranach obserwują, jak upoważniony personel wchodzi do bezpiecznych obszarów i czekają na dogodny moment, aby szybko do nich dołączyć przy wejściu chronionym. Liczą na ludzką naturę i chęć innych, aby zachować się grzecznie i trzymać otwarte zabezpieczone drzwi. Ta sztuczka zwykle działa, zwłaszcza jeśli baran ma obie ręce zajęte i wydaje się, że stara się wyjąć kartę dostępu z torebki lub kieszeni spodni. Niektórzy baranie noszą na szyi fałszywą plakietkę lub udają, że skanują kartę bezpieczeństwa za pomocą czytnika kart. Jeśli zostaną wykryci, mogą powiedzieć, że karta sprawia im problemy, i wykorzystać swoje umiejętności socjotechniczne, aby przekonać ochroniarza, aby ich przepuścił. Dobrym środkiem zapobiegawczym przeciwko przechodzeniu na barana jest używanie kołowrotów w miejscach, w których może wystąpić przechodzenie na baranach. Jednakże najlepszym środkiem zapobiegawczym jest przeszkolenie personelu w zakresie powiadamiania ochrony, gdy zauważy nieznajomego w obszarze o ograniczonym dostępie. Pracownicy muszą czuć żywotny interes w bezpieczeństwie obszaru i nie powinni polegać na pracownikach ochrony. Należy uczyć pracowników, aby nie otwierali zabezpieczonych drzwi nikomu, nawet osobom, które znają. Edukuj swoich użytkowników, aby wyrobili w sobie nawyk upewniania się, że wszyscy pracownicy korzystają ze swoich kart dostępu w celu wejścia do zastrzeżonego obszaru i zgłaszania wszelkich podejrzanych lub nieznanych osób ochronie.

BAJTY BEZPIECZEŃSTWA

Dobrze ubrany tester bezpieczeństwa wszedł do szpitala z laptopem i usiadł w poczekalni obok stanowiska pielęgniarek. Miał dostęp do haseł i danych logowania na swoim laptopie i gromadził dane przez ponad tydzień bez przesłuchań ze strony ochrony lub personelu szpitala. Tak naprawdę tester bezpieczeństwa miał wrażenie, że jest niewidzialny. Lekarze, pielęgniarki, administratorzy i inny personel szpitala nigdy nie kwestionowali obecności nieznajomego wśród nich, mimo że większość stołu w poczekalni zakrył notesami i laptopem. Po zakończeniu testu bezpieczeństwa ustalono, że wszyscy myśleli, że nieznajomy pracuje dla kogoś innego w okolicy. Nikt nie czuł się odpowiedzialny za odkrycie, kim był nieznajomy i dlaczego się tam znalazł.

Wyłudzanie informacji

Prawie każdy, kto posiada adres e-mail, otrzymał kiedyś wiadomość e-mail typu phishing. Typowym tematem jest „Aktualizuj dane swojego konta”. Wiadomość jest zwykle sformułowana jako pilna prośba o odwiedzenie strony internetowej, aby upewnić się, że nie utracisz dostępu do konta, na przykład do usługi bankowości internetowej. Ta strona jest fałszywa, ale jeśli zostaniesz oszukany i podasz dane swojego konta osobistego, pieniądze, które stracisz, będą prawdziwe. Rysunek 4-15 przedstawia rzeczywistą wiadomość e-mail phishingową rzekomo pochodzącą z serwisu PayPal. Jedną ze wskazówek, że wiadomość e-mail jest nieprawdziwa, jest to, że do odbiorcy zwraca się ogólne „Witam, kliencie”, a nie jego imię i nazwisko. Błędy ortograficzne, gramatyczne i formatowanie są również charakterystycznymi oznakami wiadomości e-mail typu phishing. Praktyką potencjalnie bardziej niebezpieczną dla firm jest spear phishing – kolejny atak przeprowadzany za pośrednictwem poczty elektronicznej, który łączy socjotechnikę z wykorzystaniem luk w zabezpieczeniach. Napastnicy wykorzystali phishing typu spear do kradzieży milionów dolarów. W przeciwieństwie do phishingu, ten atak jest skierowany na konkretne osoby w organizacji i wykorzystuje inżynierię społeczną opartą na wcześniejszych danych rekonesansowych, aby złapać ofiary. Może się wydawać, że wiadomość e-mail typu spear phishing pochodzi od nadawcy, którego odbiorca zna i zawiera tematy będące przedmiotem wspólnego zainteresowania. Celem jest nakłonienie ofiary do otwarcia załącznika lub kliknięcia łącza; działanie to instaluje złośliwe oprogramowanie typu „spear phishing”, które może mieć niszczycielski wpływ na sieć organizacji. Niektóre firmy konsultingowe ds. bezpieczeństwa uwzględniają w swoich testach ataki typu spear phishing, korzystając z narzędzi, które mogą wstrzykiwać kod powłoki do plików Adobe PDF. Jednym z przykładów takich narzędzi jest Metasploit, który jest zawarty w Kali Linux. Technologie uwierzytelniania poczty e-mail — takie jak Sender Policy Framework, DomainKeys Identified Mail, S/MIME i PGP — a także szkolenia w zakresie świadomości bezpieczeństwa dla użytkowników i stała czujność pomagają zmniejszyć zagrożenie phishingiem i spear phishingiem.

PODSUMOWANIE MODUŁU

• Footprinting to proces gromadzenia informacji o sieci za pomocą narzędzi internetowych. Narzędzia internetowe do gromadzenia informacji o infrastrukturze sieciowej obejmują Whois, OSINT Framework i Google.

• Informacje korporacyjne można gromadzić, korzystając z informacji o konkurencji uzyskanych poprzez obserwację i narzędzia internetowe.

• Adresy IP i nazwy domen można znaleźć za pomocą narzędzi takich jak Domain Dossier i polecenie dig.

• Testerzy bezpieczeństwa muszą mieć świadomość, w jaki sposób pliki cookie i błędy internetowe mogą być wykorzystywane do pobierania informacji i uzyskiwania dostępu do danych bez wiedzy użytkownika.

• Transfery stref mogą służyć do pobierania informacji o topologii sieci i przeglądania wszystkich komputerów-hostów i domen w sieci.

• Inżynieria społeczna to umiejętność wykorzystania zrozumienia natury ludzkiej w celu wydobycia informacji od niczego niepodejrzewających ludzi.

• Inżynierowie społeczni stosują wiele metod, aby przekonać użytkowników do przekazania im informacji, np. stwarzają fałszywe poczucie pilności, udają, że mają władzę, są uprzejmi i przyjacielscy, oferują coś w zamian za spełnienie prośby lub sprawiają wrażenie, że że wszyscy inni spełnili żądanie.

• Edukowanie personelu firmy na temat ataków socjotechnicznych jest ważne, ale można również przeprowadzić losowe testy, aby upewnić się, że pracownicy przestrzegają zasad firmy.

• Atakujący wykorzystują techniki takie jak surfowanie po ramieniu, nurkowanie w śmietnikach, przesiadywanie na baranach i phishing w celu zdobycia poufnych informacji.

Projekty przypadków

Projekt przypadku 4-1: Zbieranie informacji o bezpieczeństwie od niechętnego administratora

Wymagany czas: 30 minut

Cel: Zbierz informacje i utwórz notatkę dotyczącą bezpieczeństwa.

Opis: W wielu biurach firmy Alexander Rocco Corporation działa wiele systemów operacyjnych. Przed przeprowadzeniem testu bezpieczeństwa w celu ustalenia luk, które należy naprawić, warto ustalić, czy działają jakieś systemy operacyjne, o których nie wiesz. Administrator sieci nie chce przekazywać Ci informacji, gdy dowiaduje się, że pracujesz nad wykryciem luk w zabezpieczeniach sieci. Administrator postrzega Cię jako zagrożenie. Po kilkugodzinnych rozmowach dowiadujesz się jedynie, że osobisty adres e-mail administratora sieci to vader2601@gmail.com, a na jednym z systemów firmy działa stary serwer Red Hat Enterprise Linux (RHEL). Na podstawie tych informacji odpowiedz na następujące pytania:

1. Z jakich narzędzi możesz skorzystać, gdy poznasz adres e-mail administratora sieci?

2. Co możesz ustalić wpisując adres e-mail administratora sieci w Google? A co z wpisaniem tylko klamki vader2601?

3. Czy informacje, które uzyskałeś od Google, mogą zostać wykorzystane do przeprowadzenia testów podatności?

Napisałem notatkę do menedżera IT, Jawada Safari, na temat potencjalnych problemów związanych z działaniem starego serwera RHEL 5.8 i wspomniałem o znaczeniu higieny poprawek. Upewnij się, że twoja notatka wyjaśnia, w jaki sposób zebrałeś te informacje i zawiera konstruktywną informację zwrotną. Twoja notatka nie powinna wskazywać palcem na żadnego pracownika firmy; powinien omawiać problemy na poziomie ogólnym.

Projekt przypadku 4-2: Testowanie bezpieczeństwa DNS

Wymagany czas: 30 minut

Cel: utwórz raport przedstawiający plan ustalenia, czy jakiekolwiek serwery DNS są podatne na ataki związane z transferem strefy.

Opis: Właśnie dołączyłeś do działu IT w firmie Alexander Rocco Corporation. Próbujesz poznać konfigurację sieci firmowej, w tym jakie serwery DNS są zainstalowane i jak są skonfigurowane. Inni pracownicy IT są zbyt zajęci, aby Cię szkolić, więc decydujesz się samodzielnie rozwiązać problem. Wiesz, że lepiej nie zaczynać skanowania sieci i sprawdzania luk bez pisemnego upoważnienia, dlatego utworzysz dokument, który określi, co chcesz zrobić i zatwierdzi go przełożony. Utwórz dwustronicowy raport, który możesz przesłać do zatwierdzenia przełożonemu. W tym raporcie opisz, jakich narzędzi możesz użyć i jak byś ich użył, aby odkryć, jakie serwery DNS masz w swojej sieci i czy któreś z wykrytych serwerów DNS są podatne na ataki polegające na transferze strefy.