Pierwszym krokiem w procesie hakerskim jest zbieranie informacji o celu. Gromadzenie informacji, zwane również footprintingiem, to proces gromadzenia wszystkich dostępnych informacji o organizacji. W dobie Internetu informacje są dostępne w bitach i utworach z wielu różnych źródeł. Pozornie nieistotne fragmenty informacji mogą być oświecone, gdy zostaną połączone - co jest celem gromadzenia informacji. Footprinting może być skuteczny w rozpoznawaniu wysokiej wartości celów, które hakerzy będą poszukiwać, aby skoncentrować swoje wysiłki. Haker wykorzystuje techniki zbierania informacji w celu określenia wysokowartościowych celów organizacji, w których znajdują się najcenniejsze informacje. Gromadzenie informacji pomaga nie tylko określić, gdzie zlokalizowane są informacje, ale także pomaga określić najlepszy sposób uzyskania dostępu do celów. Informacje te można następnie wykorzystać do identyfikacji i ewentualnego włamania systemów docelowych. Wiele osób wskakuje w narzędzia do hakowania, ale gromadzenie informacji ma kluczowe znaczenie dla zminimalizowania prawdopodobieństwa wykrycia i oceny, gdzie spędzić najwięcej czasu i wysiłku. Inżynieria społeczna może być również wykorzystana do uzyskania większej ilości informacji o organizacji, co może ostatecznie doprowadzić do ataku. Inżynieria społeczna jako narzędzie do gromadzenia informacji jest wysoce efektywna w wykorzystywaniu najbardziej zagrożonych zasobów w organizacji: ludzi. Interakcja między ludźmi i chęć przekazywania informacji sprawiają, że ludzie są doskonałym źródłem informacji. Dobre techniki socjotechniczne mogą przyspieszyć proces hakowania iw większości przypadków znacznie ułatwią uzyskiwanie informacji. W tej części przyjrzymy się gromadzeniu informacji jako pierwszy krok w hakowaniu systemów docelowych.

Rozpoznanie

Termin "rozpoznanie" pochodzi z wojska i oznacza aktywne poszukiwanie intencji wroga poprzez zbieranie informacji o składzie i zdolnościach wroga poprzez bezpośrednią obserwację, zwykle przez zwiadowców lub personel wywiadu wojskowego przeszkolony w szpiegowaniu. W świecie hackingu etycznego rozpoznanie dotyczy procesu zbierania informacji. Rozpoznanie to termin, w którym można obserwować cel hakerski i zbierać informacje o tym, jak, kiedy i gdzie się robi. Identyfikując wzorce zachowań, ludzi lub systemów, wróg może znaleźć i wykorzystać lukę.

Użycie umiejętności Rozpoznania w celu uzyskania dostępu fizycznego

Każdy dzień powszedni o 3 po południu Kierowca Federal Express zatrzymuje się przy rampie ładunkowej budynku, w którym znajdują się biura firmy Medical Associates, Inc. Kiedy kierowca cofa ciężarówkę do tylnych drzwi budynku, naciska brzęczyk i informuje strażnika, że jest przy drzwiach. Ponieważ personel ochrony budynku rozpoznaje kierowcę - kiedy przychodzi do drzwi każdego dnia w tym samym czasie, aby odebrać i wysłać - zdalnie otwiera drzwi i pozwala kierowcy wejść. Haker obserwuje ten proces z samochodu na parkingu i odnotowuje procedurę uzyskania fizycznego wejścia do budynku. Następnego dnia haker przenosi duże tekturowe pudło w stronę drzwi, tak jak kierowca Federal Express który otrzymał wstęp do budynku. Kierowca naturalnie trzyma drzwi dla hakera, ponieważ nosi to, co wydaje się ciężkie, duże pudło. Wymieniają uprzejmości i haker kieruje się do windy do biur Medical Associates. Haker opuszcza pudło w korytarzu budynku, kierując się do swojego docelowego biura. Po dotarciu do recepcji biura Medical Associates prosi o rozmowę z kierownikiem biura, którego nazwisko wcześniej przeglądał na stronie firmy. Recepcjonistka wychodzi z biurka, aby wezwać kierownika biura, a haker sięga pod biurko i podłącza dysk USB z narzędziami hakerskimi z tyłu komputera. Ponieważ komputer nie jest zablokowany hasłem, dwukrotnie klika ikonę napędu USB i cicho instaluje oprogramowanie hakerskie na komputerze recepcjonisty. Usuwa dysk USB i szybko wychodzi z pakietu biurowego, i nic nie jest wykryty. Jest to przykład tego, jak rozpoznanie i zrozumienie zachowania ludzi może umożliwić hakerom uzyskanie fizycznego dostępu do celu - w tym przypadku sieci Medical Associates za pośrednictwem trojana - i obejść punkty kontrolne bezpieczeństwa

Zrozumienie analizy konkurencyjności

Inteligencja konkurencyjna oznacza gromadzenie informacji na temat produktów konkurencji, marketingu i technologii. Większość wywiadów konkurencyjnych nie pozostawia żadnych zastrzeżeń do badanej firmy i ma charakter łagodny - służy do porównywania produktów lub jako taktyka sprzedaży i marketingu, aby lepiej zrozumieć, jak konkurenci pozycjonują swoje produkty lub usługi. Istnieje kilka narzędzi do gromadzenia informacji konkurencyjnych, które mogą być wykorzystywane przez hakerów do zbierania informacji o potencjalnym celu. W ćwiczeniach od 2.1 do 2.3 pokażę ci, jak używać narzędzi online SpyFu i KeywordSpy do zbierania informacji o docelowej stronie. SpyFu i KeywordSpy będą podawać słowa kluczowe dla stron internetowych. Pozwala to na zbieranie informacji dotyczących strony internetowej. Używam tych dwóch narzędzi, ponieważ są łatwe w użyciu i całkowicie pasywne, co oznacza, że potencjalny cel nie może wykryć gromadzenia informacji.

Ćwiczenie 2 .1

Użycie SpyFu

Aby użyć narzędzia online SpyFu do zbierania informacji o konkurencji:

1. Przejdź do strony internetowej www.spyfu.com i wprowadź adres strony docelowej w pole wyszukiwania

2. Przejrzyj raport i określ wartościowe słowa kluczowe, linki lub inne informacje

Ćwiczenie 2.2

Użycie KeywordSpy

Aby użyć narzędzia online KeywordSpy do zbierania informacji o konkurencji:

1. Przejdź do strony www.keywordspy.com i wprowadź adres strony docelowej w polu wyszukiwania

2. Przejrzyj raport i określ wartościowe słowa kluczowe, linki lub inne informacje.

Innym przydatnym narzędziem do przeprowadzania wywiadu konkurencyjnego i zbierania informacji jest baza danych EDGAR. Jest to baza danych wszystkich dokumentów SEC dotyczących spółek publicznych. Informacje można gromadzić, przeglądając zgłoszenia SEC dotyczące nazwisk i adresów kontaktów. W części Ćwiczenie 2.3 pokażę, jak korzystać z bazy danych EDGAR do zbierania informacji o potencjalnych celach.

Używanie bazy danych EDGAR do gromadzenia informacji

1. Określ symbol giełdowy firmy za pomocą Google.

2. Otwórz przeglądarkę internetową na stronie www.sec.gov.

3. Po prawej stronie strony kliknij link Filtry EDGAR.

4. Kliknij menu Wyszukaj zgłoszenia i wprowadź nazwę firmy lub symbol giełdowy przeszukuj pliki w poszukiwaniu informacji. Możesz dowiedzieć się, na przykład, gdzie znajduje się zarejestrowana firma i kto zgłosił rejestrację.

5. Użyj konta Yahoo! żółte strony (http://yp.yahoo.com), aby sprawdzić, czy adres lub telefon numer jest wymieniony dla dowolnej z odnalezionych nazwisk pracowników.

6. Korzystaj z Grup dyskusyjnych Google i stron internetowych do publikowania ofert pracy, aby szukać swoich nazw. Czy w grupach dyskusyjnych zamieszczono jakieś zlecenia informatyczne lub inne informacje, które wskazywałyby na rodzaj sieci lub systemów w organizacji?

Strona internetowa www.Netcraft.com to kolejne dobre źródło pasywnego gromadzenia informacji. Witryna podejmie próbę określenia systemu operacyjnego i wersji serwera WWW działającego na serwerze sieciowym. To narzędzie zostanie omówione w dalszej części.

Metodologia zbierania informacji

Gromadzenie informacji można podzielić na siedem logicznych kroków. Footprinting odbywa się podczas dwóch pierwszych etapów odczytywania informacji początkowych i lokalizowania zasięgu sieci.

Footprinting: **- Odkrywaj informacje wstępne**

- Znajdź zakres sieci

- Sprawdź aktywne maszyny

- Wykryj otwarte porty / punkty dostępowe

- Wykryj systemy operacyjne

- Wykryj usługi na portach

- Mapuj sieć

Footprinting

Footprinting jest definiowany jako proces tworzenia projektu lub mapy sieci i systemów organizacji. Gromadzenie informacji jest również znane jako footprinting organizacji. Footprinting rozpoczyna się od określenia docelowego systemu, aplikacji lub fizycznej lokalizacji celu. Po uzyskaniu tych informacji określone informacje o organizacji są gromadzone przy użyciu metod nieinwazyjnych. Na przykład, własna strona internetowa organizacji może zawierać katalog personelu lub listę biogramów pracowników, co może okazać się przydatne, jeśli haker musi użyć ataku socjotechnicznego, aby osiągnąć cel. Informacje, których szuka haker w fazie footprintingu, to wszystko, co daje wskazówki dotyczące architektury sieci, serwera i typów aplikacji, w których przechowywane są cenne dane. Zanim rozpocznie się atak lub exploit, system operacyjny i jego wersja oraz typy aplikacji muszą zostać odkryte, aby najskuteczniejszy atak mógł zostać uruchomiony w stosunku do celu. Oto niektóre z informacji, które należy zebrać na temat celu podczas footprintingu:

* Nazwa domeny

* Bloki sieciowe

* Usługi sieciowe i aplikacje

* Architektura systemu

* System wykrywania intruzów

* Mechanizmy uwierzytelniania

* Konkretne adresy IP

* Mechanizmy kontroli dostępu

* Numery telefonów

* Adresy kontaktowe

Po skompilowaniu tej informacji może ona zapewnić hakerom lepszy wgląd w organizację, w której przechowywane są cenne informacje oraz w jaki sposób można uzyskać do nich dostęp.

Narzędzia Footprintingu

Footprinting można zrobić za pomocą narzędzi hakerskich, aplikacji lub stron internetowych, które pozwalają hakerowi na pasywne lokalizowanie informacji. Korzystając z tych narzędzi do footprintigu, haker może uzyskać podstawowe informacje na temat "śladu". Najpierw sprawdzając cel, haker może wyeliminować narzędzia, które nie będą działać przeciwko docelowym systemom lub sieci. Na przykład, jeśli firma projektująca grafikę używa wszystkich komputerów Macintosh, wówczas można wyeliminować całe oprogramowanie hakerskie atakujące systemy Windows. Footprinting nie tylko przyspiesza proces hakowania, eliminując pewne zestawy narzędzi, ale także minimalizuje prawdopodobieństwo wykrycia, ponieważ mniej prób hakerskich można wykonać przy użyciu odpowiedniego narzędzia do zadania. Dla ćwiczeń w tej części przeprowadzisz rekonesans i zbieranie informacji o firmie docelowej. Zalecam używanie własnej organizacji, ale ponieważ narzędzia te są pasywne, można użyć dowolnej nazwy organizacji. Niektóre z typowych narzędzi wykorzystywanych do footprintingu i zbierania informacji są takie jak następuje:

* Wyszukiwanie nazwy domeny

* Whois

* NSlookup

* Sam Spade

Zanim omówimy te narzędzia, należy pamiętać, że informacje o otwartym kodzie źródłowym mogą również dostarczyć wiele informacji o celu, takich jak numery telefonów i adresy. Wykonywanie żądań Whois, wyszukiwanie tablic nazw domen (DNS) i korzystanie z innych narzędzi internetowych do wyszukiwania to formy śladu open source. Większość tych informacji jest dość łatwa do zdobycia i legalna.

Footprinting a Cel

Footprinting jest częścią przygotowawczej fazy wstępnego ataku i obejmuje gromadzenie danych dotyczących środowiska i architektury celu, zwykle w celu znalezienia sposobów wkroczenia w to środowisko. Footprinting może ujawnić luki w systemie i określić łatwość, z jaką można je wykorzystać. Jest to najprostszy sposób, aby hakerzy mogli zbierać informacje o systemach komputerowych i firmach, do których należą. Celem tej fazy przygotowawczej jest poznanie jak najwięcej o systemie, jego zdalnych możliwościach dostępu, jego portach i usługach oraz wszelkich konkretnych aspektach jego bezpieczeństwa.

Używanie Google do zbierania informacji

Haker może również wyszukiwać w Google lub Yahoo! Ludzie szukają informacji o pracownikach lub samej organizacji. Wyszukiwarki Google można twórczo wykorzystywać do gromadzenia informacji. Wykorzystanie wyszukiwarki Google do pobierania informacji zostało nazwane hakowaniem przez

Google. Przejdź do http://groups.google.com, aby przeszukać grupy dyskusyjne Google. Poniższych poleceń można użyć, aby wyszukiwarka Google zbierała informacje o celu:

site : Wyszukuje konkretną witrynę lub domenę. Podaj stronę, którą chcesz przeszukać po dwukropku.

filetype : Wyszukiwanie tylko w tekście określonego typu pliku. Podaj typ pliku, który chcesz wyszukać po dwukropku. Nie podawaj kropki przed rozszerzeniem pliku.

link : Wyszukuje w obrębie hiperłączy dla wyszukiwanego hasła i identyfikuje powiązane strony.

cache : Identyfikuje wersję strony internetowej. Podaj adres URL witryny po dwukropku.

intitle : Wyszukuje termin w tytule dokumentu.

inurl : Wyszukuje tylko w adresie URL (adresie internetowym) dokumentu. Wyszukiwane hasło musi podążać za dwukropkiem.

Na przykład haker może użyć poniższej komendy, aby zlokalizować określone typy zagrożeń

Aplikacje internetowe:

INURL: ["parameter ="] z FILETYPE: [ext] i INURL: [scriptname]

Lub haker może użyć ciągu wyszukiwania intitle: BorderManager information alert”m, aby przeszukać serwery proxy / zapory Novell BorderManager.

Blogi, grupy dyskusyjne i informacje prasowe są również dobrym miejscem na znalezienie informacji o firmie lub pracownikach. Korporacyjne oferty pracy mogą dostarczyć informacji o typie serwerów lub urządzeń infrastruktury, z których firma może korzystać w swojej sieci. Inne uzyskane informacje mogą obejmować identyfikację używanych technologii internetowych, używanego systemu operacyjnego i sprzętu, aktywnych adresów IP, adresów e-mail i numerów telefonów oraz firmowych zasad i procedur. Ogólnie rzecz biorąc, haker poświęca 90 procent czasu na profilowanie i zbieranie informacje o celu i 10 procent czasu rozpoczęcia ataku.

Zrozumienie enumeracji DNS

Wyliczanie DNS jest procesem lokalizowania wszystkich serwerów DNS i odpowiadających im rekordów dla organizacji. Firma może mieć zarówno wewnętrzne, jak i zewnętrzne serwery DNS, które mogą dostarczać informacje, takie jak nazwy użytkowników, nazwy komputerów i adresy IP potencjalnych systemów docelowych. NSlookup, DNSstuff, amerykański rejestr numerów internetowych (ARIN) i Whois wszystkie mogą być użyte do uzyskania informacji, które następnie mogą zostać wykorzystane do wyliczenia DNS.

NSlookup i DNSstuff

Jednym z potężnych narzędzi, z którymi powinieneś się zapoznać, jest NSlookup. To narzędzie wysyła zapytania do serwerów DNS w celu uzyskania informacji rekordowych. Jest on uwzględniony w systemach operacyjnych Unix, Linux i Windows. Narzędzia hakerskie, takie jak Sam Spade, obejmują również narzędzia NSlookup. Bazując na informacjach zebranych od Whois, możesz użyć NSlookup, aby znaleźć dodatkowe adresy IP dla serwerów i innych hostów. Korzystając z autorytatywnych informacji o serwerze nazw z Whois (AUTH1.NS.NYI.NET), możesz odkryć adres IP serwera pocztowego. Eksplozja łatwych w użyciu narzędzi ułatwiła hakowanie, jeśli wiesz, jakich narzędzi użyć. DNSstuff jest kolejnym z tych narzędzi. Zamiast używać narzędzia wiersza polecenia NSlookup z jego niewygodnymi przełącznikami do zbierania informacji o rekordach DNS, wystarczy wejść na stronę www.dnsstuff.com i można przeprowadzić wyszukiwanie rekordów DNS online. To wyszukiwanie ujawnia wszystkie

rekordy aliasy dla www.eccouncil.org i adres IP serwera WWW. Możesz nawet odkryć wszystkie serwery nazw i powiązane adresy IP.

Zrozumienie wyszukiwań Whois i ARIN

Whois ewoluowała z systemu operacyjnego Unix, ale można go teraz znaleźć w wielu systemach operacyjnych, a także w narzędziach hakerskich i Internecie. To narzędzie określa, kto ma zarejestrowane nazwy domen używane w e-mailach lub witrynach. Jednolity lokalizator zasobów (URL), takich jak www.microsoft.com, zawiera nazwę domeny (Microsoft.com) oraz nazwę hosta lub alias (WWW). Internetowa Korporacja ds. Przydzielonych Nazw i Numerów (ICANN) wymaga rejestracji nazw domen, aby zapewnić, że tylko jedna firma używa konkretnej nazwy domeny. Narzędzie Whois wysyła zapytanie do bazy danych rejestracji w celu pobrania danych kontaktowych dotyczących osoby lub organizacji, która posiada rejestrację domeny.

Narzędzie hakerskie

SmartWhois to program zbierający informacje, który pozwala znaleźć wszystkie dostępne informacje o adresie IP, nazwie hosta lub domenie, w tym o kraju, stanie lub prowincji, mieście, nazwie dostawcy sieci, administratorze oraz dane kontaktowe działu pomocy technicznej. SmartWhois to graficzna wersja podstawowego programu Whois

W ćwiczeniu 2.4 pokażę ci, jak używać darmowego narzędzia Whois.

Ćwiczenie 2. 4

Używanie Whois

Aby użyć narzędzia Whois do zbierania informacji o rejestratorze lub nazwie domeny:

1. Przejdź do strony DNSStuff.com i przewiń w dół do bezpłatnych narzędzi na dole strony.

2. Wprowadź docelowy adres URL firmy w polu Wyszukiwanie WHOIS i kliknij przycisk WHOIS.

3. Sprawdź wyniki i określ, co następuje:

Zarejestrowany adres

Kontakty techniczne i DNS

Kontaktowy adres e-mail

Telefoniczny numer kontaktowy

Termin ważności

4. Odwiedź stronę internetową firmy i sprawdź, czy dane kontaktowe z WHOIS są zgodne z dowolnym z nazw kontaktów, adresów i adresów e-mail wymienionych na stronie internetowej.

5. Jeśli tak, użyj wyszukiwarki Google, aby wyszukać nazwiska pracowników lub adresy e-mail. Możesz poznać konwencję nazewnictwa poczty e-mail używaną przez organizację oraz informacje, które nie powinny być publicznie dostępne.

ARIN jest bazą danych zawierającą takie informacje, jak właściciele statycznych adresów IP. Baza danych ARIN może być zapytana za pomocą narzędzia Whois, takiego jak na stronie www.arin.net. Zwróć uwagę, że adresy, wiadomości e-mail i informacje kontaktowe znajdują się w tym wyszukiwaniu Whois. Informacje te mogą być wykorzystane przez etycznego hakera, aby dowiedzieć się, kto jest

odpowiedzialny za określony adres IP i która organizacja jest właścicielem tego systemu docelowego, lub może zostać wykorzystany przez złośliwego hakera do przeprowadzenia ataku socjotechnicznego na organizację. Jako specjalista ds. Bezpieczeństwa musisz znać informacje dostępne publicznie w bazach wyszukiwania, takich jak ARIN i upewnij się, że złośliwy haker nie może użyć tych informacji do rozpoczęcia ataku na sieć. Należy pamiętać, że różne regiony geograficzne spoza Ameryki Północnej mają własne rejestry internetowe, takie jak RIPE NCC (Europa, Bliski Wschód i części Azji Środkowej), LACNIC (rejestr adresów internetowych w Ameryce Łacińskiej i Karaibach) oraz APNIC (sieć Asia Pacific Network Centrum Informacyjne).

Analizowanie wyniku Whois

Prostym sposobem uruchomienia aplikacji Whois jest połączenie się ze stroną internetową (na przykład www.networksolutions.com) i przeprowadzenie wyszukiwania Whois. Listing 2.1 jest wynikiem wyszukiwania Whois na stronie www.eccouncil.org. :

Whois out na stronie www .eccou ncil .org

Identyfikator domeny: D81180127-LROR

Nazwa domeny: ECCOUNCIL.ORG

Utworzono: 14 grudnia 2001 10:13:06 UTC

Ostatnia aktualizacja: 19-sierpień 2004 03:49:53 UTC

Data wygaśnięcia: 14 grudnia 2006 r. 10:13:06 UTC

Sponsoring Registrar: Tucows Inc. (R11-LROR)

Status: OK

Identyfikator rejestratora: tuTv2ItRZBMNd4lA

Nazwa podmiotu rejestrującego: John Smith

Organizacja rejestrująca: Międzynarodowa Rada Konsultantów E-Commerce

Rejestrujący Street1: 67 Wall Street, 22. piętro

Rejestrujący Street2:

Rejestrujący Street3:

Rejestrujący Miasto: Nowy Jork

Państwo / prowincja rejestrująca: NY

Rejestrujący Kod pocztowy: 10005-3198

Państwo rejestrujące się: USA

Telefon rejestrujący: +1.2127098253

Przedłużacz telefonu rejestrującego:

Faks odbiorcy: +1.2129432300

Rejestry abonenckie abonenta:

Rejestrujący e-mail: forum@eccouncil.org

Identyfikator administratora: tus9DYvpp5mrbLNd

Nazwa administratora: Susan Johnson

Organizacja administracyjna: Międzynarodowa Rada Konsultantów E-Commerce

Admin Street1: 67 Wall Street, 22. piętro

Admin Street2:

Admin Street3:

Admin Miasto: Nowy Jork

Admin State / Province: NY

Admin Kod pocztowy: 10005-3198

Kraj administratora: USA

Telefon administracyjny: +1.2127098253

Rozszerzenia telefonu administratora:

FAKS administratora: +1.2129432300

Admin FAX Ext .:

Adres e-mail administratora: ethan@eccouncil.org

ID technologii: tuE1cgAfi1VnFkpu

Nazwa techniczna: Jacob Eckel

Organizacja technologiczna: Międzynarodowa Rada Konsultantów E-Commerce

Tech Street1: 67 Wall Street, 22. piętro

Tech Street2:

Tech Street3:

Tech City: Nowy Jork

Tech State / Province: NY

Tech Postal Kod: 10005-3198

Kraj Tech: USA

Telefon techniczny: +1.2127098253

Tech Phone Ext .:

FAKS TECH: +1.2129432300

Tech FAX Ext .:

Tech Email: forum@eccouncil.org

Serwer nazw: ns1.xyz.net

Serwer nazw: ns2.xyz.net

Zwróć uwagę na cztery podświetlone linie. Pierwszy pokazuje firmę docelową lub osobę (również jako fizyczny adres, adres e-mail, numer telefonu itd.). Następny pokazuje administracja lub kontakt techniczny (i ich dane kontaktowe). Dwa ostatnie wyróżnione linie pokazują nazwy serwerów nazw domen.

Znajdowanie zakresu adresów sieci

Każdy etyczny haker musi wiedzieć, jak znaleźć zasięg sieci i maskę podsieci docelowego systemu. Adresy IP są używane do lokalizowania, skanowania i łączenia się z systemami docelowymi. Adresy IP można znaleźć w rejestrach internetowych, takich jak ARIN lub Internet Assigned Numbers Authority (IANA). Etyczny haker może również potrzebować znaleźć położenie geograficzne docelowego systemu lub sieci. Zadanie to można wykonać, śledząc trasę, którą trasa odbierana jest przez wysyłany do docelowego adresu IP. Możesz użyć narzędzi takich jak traceroute, VisualRoute i NeoTrace do identyfikacji trasy do celu. Dodatkowo podczas śledzenia Twojej sieci docelowej inne przydatne informacje stają się dostępne. Na przykład możesz uzyskać wewnętrzne adresy IP komputerów-hostów; nawet internetowa bramka IP organizacji może być wymieniona. Adresy te można później wykorzystać w ataku lub w dalszych procesach skanowania.

Identyfikacja typów rekordów DNS

Poniższa lista opisuje typowe typy rekordów DNS i ich wykorzystanie:

A (Address) : Mapuje nazwę hosta na adres IP

SOA (Start of Authority) : Identyfikuje serwer DNS odpowiedzialny za informacje o domenie

CNAME (nazwa kanoniczna) : Zapewnia dodatkowe nazwy lub aliasy dla rekordu adresu

MX (Mail Exchange) : Identyfikuje serwer pocztowy dla domeny

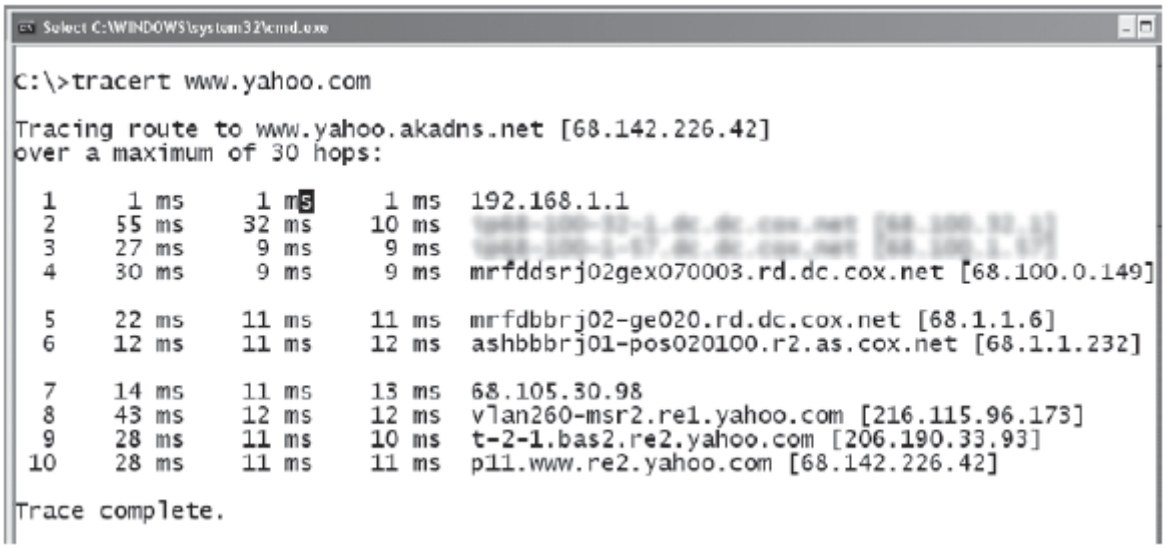
SRV (usługa) : Identyfikuje usługi, takie jak usługi katalogowe

PTR (wskaźnik) : Mapuje adresy IP na nazwy hostów

NS (Name Server) : Identyfikuje inne serwery nazw dla domeny

Używanie Traceroute w Footprinting

Traceroute to narzędzie do śledzenia pakietów, które jest dostępne dla większości systemów operacyjnych. Działa poprzez wysyłanie echa protokołu ICMP (Internet Control Message Protocol) do każdego przeskoku (routera lub bramy) wzdłuż ścieżki, aż do osiągnięcia adresu docelowego. Gdy wiadomości ICMP są wysyłane z powrotem z routera, czas życia (TTL) jest zmniejszany o jeden dla każdego routera wzdłuż ścieżki. Dzięki temu haker może określić liczbę przeskoków routera od nadawcy. Jednym z problemów związanych z używaniem narzędzia traceroute jest przekroczenie limitu czasu (oznaczonego gwiazdką) w przypadku napotkania firewalla lub routera filtrującego pakiety. Chociaż zapora sieciowa zatrzymuje narzędzie tracerout od wykrywania wewnętrznych hostów w sieci, może ostrzec etycznego hakera o obecności zapory ogniowej; następnie można zastosować techniki omijania firewalla. Sam Spade i wiele innych narzędzi hakerskich zawiera wersję traceroute. Systemy operacyjne Windows używają nazwy hosta składni tracert do wykonywania traceroute Rysunek 2.5 jest przykładem wyjścia traceroute dla śladu www.yahoo.com.



Zauważ na rysunku, że wiadomość po raz pierwszy napotyka wychodzącego ISP, aby dotrzeć do Yahoo! i że adres IP serwera jest ujawniony jako 68.142.226.42. Znając ten adres IP, etyczny haker może przeprowadzić dodatkowe skanowanie na tym hoście podczas fazy skanowania. Polecenie tracert identyfikuje routery znajdujące się w drodze do sieci docelowej. Ponieważ routery na ogół są nazywane zgodnie z ich fizyczną lokalizacją, wyniki tracert pomagają zlokalizować te urządzenia.

Narzędzia hakerskie

NeoTrace, VisualRoute i VisualLookout to wszystkie narzędzia do śledzenia pakietów z graficznym interfejsem użytkownika lub interfejsem graficznym. Wyznaczają ścieżkę, którą pakiety podróżują po mapie i mogą wizualnie identyfikować lokalizacje routerów i innych urządzeń do pracy w Internecie. Narzędzia te działają podobnie do traceroute i wykonują te same zbieranie informacji; jednak zapewniają wizualną reprezentację wyników.

Opis śledzenia poczty e-mail

Programy śledzące pocztę elektroniczną pozwalają nadawcy wiadomości e-mail dowiedzieć się, czy odbiorca czyta, przekazuje dalej, modyfikuje lub usuwa wiadomość e-mail. Większość programów śledzących pocztę e-mail działa poprzez dołączanie nazwy domeny do adresu e-mail, na przykład readnotify.com. Jednopikselowy plik graficzny ,który nie jest zauważalny dla odbiorcy, jest załączone do wiadomości e-mail. Następnie, gdy wykonywane jest działanie w wiadomości e-mail ten plik graficzny łączy się z serwerem i powiadamia nadawcę o akcji.

Narzędzie hakerskie

Visualware's eMailTrackerPro (www.emailtrackerpro.com/) i MailTracking (http: //mailtracking.com/) to narzędzia, które umożliwiają etycznym hakerom śledzenie wiadomości e-mail. Gdy za pomocą tych narzędzi można wysłać wiadomość e-mail, przekazać wiadomość e-mail, odpowiedzieć na wiadomość e-mail lub zmodyfikować wiadomość e-mail, powstałe w wyniku działania i ślady oryginalnego e-maila są rejestrowane. Nadawca jest powiadamiany o wszystkich czynnościach wykonywanych na śledzonym e-mailu przez automatycznie generowaną wiadomość e-mail.

Zrozumienie pająków internetowych

Spamerzy i wszyscy zainteresowani zbieraniem adresów e-mail z Internetu mogą korzystać z pająków internetowych. Pająk internetowy przeczesuje witryny zbierając pewne informacje, takie jak adresy e-

mail. Pająk sieciowy używa składni takiej jak symbol @ do lokalizowania adresów e-mail, a następnie kopiuje je do listy. Te adresy są następnie dodawane do bazy danych i mogą być później używane do wysyłania niechcianych wiadomości e-mail. Pająki internetowe mogą służyć do lokalizowania wszelkiego rodzaju informacji w Internecie. Haker może wykorzystać pajęczynę do automatyzacji procesu zbierania informacji. Metoda zapobiegania przed pająkami sieciowymi twojej strony internetowej to umieszczenie pliku robots.txt w katalogu głównym twojej witryny z listą katalogów, które chcesz zabezpieczyć przed przeszukiwaniem.

Inżynieria społeczna

Inżynieria społeczna to nietechniczna metoda włamywania się do systemu lub sieci. Jest to proces oszukiwania użytkowników systemu i przekonania ich do wykonywania czynności przydatnych hakerowi, takich jak podawanie informacji, które można wykorzystać do pokonania lub obejścia mechanizmów bezpieczeństwa. Inżynieria społeczna jest ważna do zrozumienia, ponieważ hakerzy mogą jej używać do atakowania elementu ludzkiego systemu i obchodzenia zabezpieczeń technicznych. Ta metoda może służyć do zbierania informacji przed atakiem lub w jego trakcie. Inżynier społeczny zwykle używa telefonu lub Internetu, aby oszukać ludzi w celu ujawnienia poufnych informacji lub zmusić ich do zrobienia czegoś, co jest sprzeczne z polityką bezpieczeństwa organizacji. Dzięki tej metodzie inżynierowie społeczni wykorzystują naturalną tendencję człowieka do ufania swojemu słowu, zamiast wykorzystywać luki w zabezpieczeniach komputera. Ogólnie uważa się, że użytkownicy są słabym ogniwem w bezpieczeństwie; ta zasada umożliwia inżynierię społeczną. Poniżej znajduje się przykład inżynierii społecznej, relacjonowanych przez Kapil Raina, obecnie ekspert bezpieczeństwa w VeriSign, w oparciu o rzeczywiste doświadczenia pracy u poprzedniego pracodawcy:

Pewnego ranka kilka lat temu grupa nieznajomych weszła do dużej firmy transportowej i wyszła z dostępem do całej sieci firmowej firmy. Jak oni to zrobili? Uzyskując niewielkie ilości dostępu, krok po kroku, od wielu różnych pracowników w tej firmie. Najpierw badali firmę przez dwa dni, zanim nawet spróbowali postawić stopę na jej terenie. Na przykład nauczyli się nazwisk kluczowych pracowników, dzwoniąc do HR. Następnie udawali, że zgubili klucz do drzwi wejściowych, a portier wpuścił ich do środka. Potem "zgubili" swoje identyfikatory podczas wchodzenia na trzeci piętro chronionego obszaru, uśmiechnął się, a przyjazny pracownik otworzył im drzwi. Nieznajomi wiedzieli, że dyrektor finansowy jest poza miastem, więc mogli wejść do jego biura i uzyskać dane finansowe z jego odblokowanego komputera. Przeszukali korporacyjne śmieci, znajdując wiele użytecznych dokumentów. Poprosili woźnego o kubeł na śmieci, w którym umieścili ich zawartość i wynieśli wszystkie te dane z budynku w swoich rękach. Obcy studiował głos CFO, więc byli w stanie telefonować, udając CFO, w pośpiechu, rozpaczliwie potrzebującego swojego hasła dostępu do sieci. Stamtąd korzystali oni ze zwykłych narzędzi technicznych do hakowania, aby uzyskać dostęp superużytkownika do systemu. W tym przypadku nieznajomi byli konsultantami sieci przeprowadzającymi audyt bezpieczeństwa dla dyrektora finansowego bez wiedzy innych pracowników. Nigdy nie otrzymali żadnych uprzywilejowanych informacji od dyrektora finansowego, ale byli w stanie uzyskać wszelki dostęp, jakiego chcieli, dzięki inżynierii społecznej. Najbardziej niebezpieczna część inżynierii społecznej jest to, że firmy z procesami uwierzytelniania, zaporami ogniowymi, wirtualnymi sieciami prywatnymi, sieciami i oprogramowaniem monitorującym są nadal szeroko otwarte na ataki, ponieważ socjotechnika nie atakuje środków bezpieczeństwa bezpośrednio. Zamiast tego atak socjotechniczny omija środki bezpieczeństwa i idzie po ludzki element w organizacji.

Sztuka manipulacji

Inżynieria społeczna obejmuje nabywanie poufnych informacji lub nieodpowiednich uprawnień dostępu przez osoby z zewnątrz, w oparciu o budowanie niewłaściwych relacji zaufania. Celem

inżyniera społecznego jest sprawienie, by ktoś dostarczył cennych informacji lub podał dostęp do tych informacji. Inżynieria społeczna żeruje na cechach natury ludzkiej, takich jak pragnienie bycia pomocnym, skłonność do ufania ludziom i lęk przed popadnięciem w kłopoty. Hakerzy, którzy są w stanie wtopić się i stać się częścią organizacji, odnoszą największe sukcesy w atakach socjotechnicznych. Ta zdolność do mieszania się jest powszechnie nazywana sztuką manipulacji. Ludzie są zazwyczaj najsłabszym ogniwem w łańcuchu bezpieczeństwa. Skuteczna obrona zależy od posiadania dobrej polityki i nauczania pracowników do przestrzegania zasad. Inżynieria społeczna jest najcięższą formą ataku, aby się przed nią obronić, ponieważ firma nie może się zabezpieczyć samym sprzętem ani oprogramowaniem.

Typy rodzajów ataku inżynierii społecznej

Inżynieria społeczna może być podzielona na dwa popularne typy:

Oparta na człowieku : inżynieria społeczna oparta na człowieku odnosi się do interakcji człowiek-osoba w celu uzyskania pożądanych informacji. Przykładem jest wywołanie help desk i próba znalezienia hasła.

Komputerowa inżynieria społeczna : oparta na komputerach odnosi się do oprogramowania komputerowego, które próbuje uzyskać pożądane informacje. Przykładem jest wysłanie użytkownikowi e-maila z prośbą o ponowne wpisanie hasła na stronie internetowej w celu jego potwierdzenia. Ten atak socjotechniczny jest również znany jako phishing.

Przyjrzymy się każdemu z nich bliżej w kolejnych sekcjach.

Ludzka inżynieria społeczna

Techniki socjotechniki oparte na człowieku można ogólnie podzielić na następujące kategorie:

Podszywanie się pod pracownika lub ważnego użytkownika W tego rodzaju ataku socjotechnicznym haker udaje pracownika lub ważnego użytkownika w systemie. Haker może uzyskać fizyczny dostęp, podając się za dozorcę, pracownika lub wykonawcę. Wewnątrz obiektu haker zbiera informacje z koszu na śmieci, komputerów stacjonarnych lub systemów komputerowych.

Pozowanie jako ważny użytkownik W tego typu atakach haker udaje, że jest ważnym użytkownikiem, takim jak menedżer wykonawczy lub wysokiego szczebla, który potrzebuje natychmiastowej pomocy w uzyskaniu dostępu do systemu komputerowego lub plików. Haker wykorzystuje zastraszanie, aby pracownik niższego szczebla, na przykład pracownik pomocy technicznej, pomagał mu w uzyskaniu dostępu do systemu. Większość niskopoziomowych pracowników nie będzie kwestionować kogoś, kto wydaje się być autorytetem.

Korzystanie z trzeciej osoby Korzystając z podejścia trzeciej osoby, haker udaje, że ma pozwolenie z upoważnionego źródła do korzystania z systemu. Ten atak jest szczególnie skuteczny, jeśli rzekome autoryzowane źródło jest na wakacjach lub nie można się z nim skontaktować w celu weryfikacji.

Wywołanie pomocy technicznej Wywołanie wsparcia technicznego w celu uzyskania pomocy jest klasyczną techniką socjotechniczną. Dział pomocy technicznej i personel pomocniczy są przeszkoleni, aby pomagać użytkownikom, co czyni ich dobrymi łupami dla ataków socjotechnicznych.

Surfowanie na ramieniu jest techniką zbierania haseł poprzez obserwowanie przez ramię osoby podczas logowania do systemu. Haker może obejrzeć prawidłowe logowanie użytkownika, a następnie użyć tego hasła, aby uzyskać dostęp do systemu.

Nurkowanie w śmietniku Nurkowanie polega na zaglądaniu do kosza po informacje zapisane

na kawałkach papieru lub wydrukach komputerowych. Haker często może znaleźć hasła, nazwy plików lub inne poufne informacje.

Bardziej zaawansowana metoda pozyskiwania nielegalnych informacji nosi nazwę odwrotnej inżynierii społecznej. Używając tej techniki, haker tworzy osobę, która wydaje się być w pozycji autorytetu, tak aby pracownicy pytali hakera o informacje, a nie na odwrót. Na przykład haker może podszyć się pod pracownika działu pomocy technicznej i poprosić użytkownika o podanie takich informacji, jak hasło.

Demonstracja inżynierii społecznej

Facylitator demonstruje przeprowadzenie na żywo przez Computer Security Institute wykazania luki w w dziale pomocy, gdy zadzwonił do firmy telefonicznej, został przeniesiony i dotarł do help desku. "Kto jest na służbie dziś wieczorem?" "Och, to jest Betty." "Pozwól mi porozmawiać z Betty." [Został przekierowany] "Cześć Betty, maszzły dzień?" "Nie, dlaczego?" "Twoje systemy są nieczynne - Betty. powiedziała – „Moje systemy nie są wyłączone, wszystko działa dobrze.” Powiedział: "Lepiej wyloguj się". Powiedział: "Teraz się ponownie zarejestruj." Znów się zalogowała. Powiedział: "Niewidzieliśmy nawet blipu, nie widzimy żadnych zmian." Powiedział: "Podpisz się ponownie." Zrobiła to. - Betty, będę musiała się podpisać, jak tu, żeby dowiedzieć się, co się dzieje z twoim ID. Podaj mi twój identyfikator użytkownika i hasło.” Więc ten starszy konsultant w dziale pomocy podaje mu swój identyfikator użytkownika i hasło. W ciągu kilku minut haker może uzyskać informacje, które zajęłyby mu kilka dni, przechwytując ruch i łamiąc hasło. O wiele łatwiej jest zdobyć informacje za pomocą inżynierii społecznej niż za pomocą metod technicznych.

Komputerowa inżynieria społeczna

Komputerowe ataki socjotechniczne mogą obejmować:

* Załączniki wiadomości e-mail

* Fałszywe strony internetowe

* Wyskakujące okienka

Ataki Wewnętrzne

Jeśli haker nie znajdzie innego sposobu na hakowanie organizacji, najlepszym rozwiązaniem będzie infiltracja organizacji poprzez zatrudnienie się jako pracownik lub znalezienie niezadowolonego pracownika, który pomoże w ataku. Ataki typu "insider" mogą być potężne, ponieważ pracownicy mają fizyczny dostęp i mogą swobodnie poruszać się po organizacji. Przykładem może być osoba podająca się za dostawcę, ubrana w mundur i uzyskująca dostęp do pokoju dostawców lub doku załadunkowego. Inną możliwością jest ktoś, kto udaje członka ekipy sprzątającej, która ma dostęp do wnętrza budynku

Kradzież tożsamości

Haker może przedstawiać się jako pracownik lub wykraść tożsamość pracownika w celu wykonania ataku. Informacje zebrane podczas nurkowania na śmietniku lub spoglądania przez ramię w połączeniu z tworzeniem fałszywych identyfikatorów mogą spowodować wejście hakera do organizacji. Stworzenie osoby, która może wejść do budynku bez żadnych zastrzeżeń, jest celem kradzieży tożsamości.

Ataki phishingowe

Phishing polega na wysyłaniu wiadomości e-mail, zwykle przedstawiającej się jako bank, firma obsługująca karty kredytowe lub inna organizacja finansowa. Wiadomość e-mail wymaga

potwierdzenia przez odbiorcę informacji bankowych lub resetowania haseł lub kodów PIN. Użytkownik klika łącze w wiadomości e-mail i jest przekierowywany do fałszywej witryny. Haker jest wówczas w stanie przechwycić te informacje i wykorzystać je do uzyskania korzyści finansowych lub przeprowadzenia innych ataków. Wiadomości e-mail żądające od nadawców znacznej kwoty, ale potrzebna jest pomoc w wydostaniu ich poza kraj. Są to przykłady ataków typu phishing. Ataki te polują na zwykłą osobę i mają na celu skłonienie ich do udostępnienia hakerowi kodów dostępu do kont bankowych lub innych poufnych informacji.

Oszustwa internetowe

Niektóre witryny internetowe, które oferują bezpłatne oferty lub inne oferty specjalne, mogą skłonić ofiarę do wprowadzenia nazwy użytkownika i hasła, które mogą być takie same, jak tych, których używają do uzyskania dostępu do ich systemu pracy. Haker może użyć tej prawidłowej nazwy użytkownika i hasła, gdy użytkownik wprowadzi informacje formularz strony internetowej. Załączniki do wiadomości e-mail mogą być używane do wysyłania szkodliwego kodu do systemu ofiary, który może automatycznie wykonać coś podobnego do keyloggera oprogramowania, aby przechwytywać hasła. Wirusy, trojany i robaki mogą być zawarte w sprytnie spreparowanych e-mailach, aby zachęcić ofiarę do otwarcia załącznika. Załączniki do wiadomości uważane są za komputerowe ataki socjotechniczne. Oto przykład wiadomości e-mail, która próbuje przekonać odbiorcę do otwarcia niebezpiecznego załącznika:

Raport serwera poczty.

Nasza zapora określiła, że wysyłane są wiadomości e-mail zawierające kopie robaków do Twojego komputera.

W dzisiejszych czasach dzieje się tak na wielu komputerach, ponieważ jest to nowy typ wirusa (Network Worms). Korzystając z nowego błędu w systemie Windows wirusy te infekują komputer niezauważalnie. Po wniknięciu do komputera wirus zbiera wszystkie adresy e-mail i wysyła kopie na te adresy e-mail

Zainstaluj aktualizacje eliminujące robaka i przywracanie komputera.

Z poważaniem,

Obsługa klienta

Wyskakujące okna mogą być również wykorzystywane w komputerowych atakach inżynierskich, podobnie jak w przypadku załączników wiadomości e-mail. Wyskakujące okna z ofertami specjalnymi lub darmowymi materiałami mogą zachęcać użytkownika do niechcianej instalacji złośliwego oprogramowania.

Utajnienie adresu URL

Adres URL (jednolity lokalizator zasobów) jest powszechnie używany w pasku adresu przeglądarki internetowej w celu uzyskania dostępu do określonej witryny. Mówiąc w skrócie, jest to adres strony internetowej. Zakodowanie adresów URL polega na ukrywaniu fałszywego adresu URL w legalnym adresie witryny. Na przykład witryna internetowa 204.13.144.2/Citibank może wydawać się uzasadnionym adresem internetowym Citibanku, ale w rzeczywistości tak nie jest. Utajnienie adresów URL jest wykorzystywane w atakach phishingowych i niektórych oszustwach internetowych, aby oszustwo wydawało się bardziej uzasadnione. Adres strony internetowej może być postrzegany jako

nazwa lub logo instytucji finansowej, ale link prowadzi do fałszywej strony internetowej lub adresu IP. Gdy użytkownik kliknie link, zostaje przekierowany na stronę hakera. Adresy mogą być zaciemniane w złośliwych linkach przy użyciu zapisów szesnastkowych lub dziesiętnych. Na przykład adres 192.168.10.5 wygląda jak 3232238085 jako dziesiętny. Ten sam adres wygląda jak C0A80A05 szesnastkowym IP. Konwersja ta wymaga wielokrotnego podzielenia 3232238085 przez 16. Za każdym razem reszta ujawnia adres, zaczynając od najmniej znaczącej wartości.

Oto wyjaśnienie:

3232238085/16 = 202014880.3125 (.3125 × 16 = 5)

202014880/16 = 12625930.0 (.0 × 16 = 0)

12625930/16 = 789120.625 (.625 × 16 = 10 = A)

789120/16 = 49320,0 (.0 × 16 = 0)

49320,0 / 16 = 3082,5 (.5 × 16 = 8)

3082/16 = 192,625 (.625 × 16 = 10 = A)

192/16 = 12 = C

Inżynieria społeczna Środki zaradcze

Umiejętność walki z inżynierią społeczną ma kluczowe znaczenie dla każdego certyfikowanego etycznego hakera. Istnieje wiele sposobów, aby to zrobić. Udokumentowane i egzekwowane zasady bezpieczeństwa i programy podnoszenia świadomości bezpieczeństwa są najbardziej krytycznym elementem każdego programu bezpieczeństwa informacji. Dobra polityka i procedury nie są skuteczne, jeśli nie są nauczane i wzmacniane przez pracowników. Polityki muszą być przekazywane pracownikom, aby podkreślić ich znaczenie, a następnie egzekwowane przez kierownictwo. Po odbyciu szkolenia dotyczącego świadomości bezpieczeństwa pracownicy będą zobowiązani do wspierania polityki bezpieczeństwa organizacji. Polityka bezpieczeństwa korporacyjnego powinna dotyczyć tego, jak i kiedy konta są konfigurowane i kończone, jak często zmieniają się hasła, kto może uzyskać dostęp do informacji i sposobu postępowania z naruszeniami zasad. Ponadto zasady powinny określać procedury pomocy technicznej dla poprzednich zadań, a także proces identyfikowania pracowników - na przykład przy użyciu numeru pracownika lub innych informacji w celu potwierdzenia zmiany hasła. Zniszczenie dokumentów papierowych i fizyczne ograniczenia dostępu to dodatkowe obszary, którymi powinna się zająć polityka bezpieczeństwa. Wreszcie, polityka powinna dotyczyć obszarów technicznych, takich jak wykorzystanie modemów i kontrola wirusów. Jedną z zalet silnej polityki bezpieczeństwa jest to, że usuwa odpowiedzialność pracowników za dokonywanie osądów dotyczących hakerskich żądań. Jeśli żądane działanie jest zabronione przez zasadę, pracownik ma wytyczne dotyczące odmowy. Najważniejszym środkiem zaradczym w inżynierii społecznej jest edukacja pracowników. Wszyscy pracownicy powinni zostać przeszkoleni w zakresie bezpiecznego przechowywania poufnych danych. Zespoły zarządzające są zaangażowane w tworzenie i wdrażanie polityki bezpieczeństwa, aby w pełni ją zrozumieć i wspierać ją w całej organizacji. Polityka zwiększania świadomości firmy w zakresie bezpieczeństwa powinna wymagać od wszystkich nowych pracowników orientacji na bezpieczeństwo. Od rocznych zajęć powinno się wymagać odświeżania i aktualizowania informacji dla pracowników. Innym sposobem na zwiększenie zaangażowania jest comiesięczny biuletyn zawierający artykuły na temat bezpieczeństwa.

Podsumowanie

W tej części nauczyłeś się, jak zrobić pierwsze kroki w kierunku hackowania etycznego. Zbieranie Informacji, forma rozpoznania, footprintingu i inżynierii społecznej, jest konieczne, aby dowiedzieć się jak najwięcej o celu. Postępując zgodnie z metodologią zbierania informacji, etyczni hakerzy mogą zapewnić, że nie brakuje im żadnych kroków i cennych informacji. Czas spędzony na etapie zbierania informacji jest wart przyspieszenia i tworzenia udanych exploitów hakerskich.

Do Zapamiętania!

* Wiesz , jak wyszukiwać wiadomości firmowe, informacje prasowe, blogi i posty w grupach dyskusyjnych. Wyszukaj oferty pracy od firmy docelowej lub organizacji w celu ustalenia wersji systemu i innych ważnych informacji, takich jak zapora sieciowa lub typy IDS i typy serwerów. Google hacking może służyć do zbierania informacji z tych lokalizacji, dzięki czemu haker może szybko zlokalizować informacje o celu. Wykorzystaj wszystkie dostępne zasoby publiczne, aby zlokalizować informacje o firmie docelowej i zebrać dane o jej sieci i bezpieczeństwie systemu. Użyj Yahoo! Wyszukiwania osób lub innych wyszukiwarek internetowych w celu znalezienia pracowników firmy docelowej.

* Wiesz jak wysyłać zapytania do DNS o określone informacje dotyczące rekordów. Naucz się korzystać z DNSstuff, NSlookup lub Sam Spade do zapytania serwera DNS o informacje rekordowe, takie jak hosty i adresy IP.

* Wiesz, jak wykonywać wyszukiwania Whois w celu uzyskania informacji osobistych lub firmowych. Dowiedz się, jak korzystać z baz danych ARIN, LACNIC, RIPE NCC, APNIC i Whois, aby zlokalizować dane kontaktowe rejestratora i firmy.

* Wiesz, jak znaleźć nazwy zewnętrznych i wewnętrznych domen firmy docelowej. Powinieneś być w stanie użyć narzędzi Whois i Sam Spade do zlokalizowania informacji o domenie dla danej firmy. Znajomość bazy danych ARIN jest również niezbędna do egzaminu.

* Wiesz, jak fizycznie zlokalizować serwer sieciowy firmy docelowej i inne urządzenia infrastruktury sieciowej. Użyj NeoTrace, VisualRoute lub VisualLookout, aby uzyskać graficzny widok trasy do sieci firmy docelowej. Te narzędzia umożliwiają fizyczne zlokalizowanie serwerów.

* Wiesz, jak śledzić pocztę do lub z firmy. Powinieneś być w stanie używać programów śledzących pocztę e-mail do śledzenia wiadomości e-mail do docelowej organizacji i uzyskiwania dodatkowych informacji do wykorzystania w ataku.

* Poznałeś różnicę między atakami socjotechnicznymi opartymi na ludziach i komputerach. Inżynieria społeczna oparta na człowieku wykorzystuje metody nietechniczne do zainicjowania ataku, podczas gdy inżynieria społeczna oparta na komputerze wykorzystuje komputer.

* Podszywanie się, udawanie ważnego użytkownika, podejście trzeciej osoby, udawanie wsparcia technicznego, surfowanie przez ramieniu i nurkowanie w śmietniku to rodzaje inżynierii społecznej opartej na człowieku. Załączniki do e-maili, fałszywe strony internetowe, okna pop-up i odwrotna inżynieria społeczna to wszystkie komputerowe metody socjotechniczne.

* Zrozumiałeś znaczenie edukacji pracowników. Kształcenie pracowników w zakresie oznak socjotechniki i polityki bezpieczeństwa firmy jest kluczem do zapobiegania atakom socjotechnicznym.