Socjotechniki w praktyce

Podręcznik etycznego hakera

Joe Gray

Helion

no starch press

Tytuł oryginału: Practical Social Engineering: A Primer for the Ethical Hacker

Tłumaczenie: Piotr Rakowski

ISBN: 978-83-8322-087-1

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
https://helion.pl/user/opinie/socpod
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *https://helion.pl* (księgarnia internetowa, katalog książek)

Printed in Poland.

Spis treści

5

Media społecznościowe i dokumenty publicznie dostępne

W poprzednim rozdziale omówiliśmy wykorzystanie zaawansowanych narzędzi do zbierania danych OSINT-owych. Jednak nie zawsze trzeba mieć do dyspozycji wyszukane narzędzia, aby uzyskać potrzebne informacje. Często wystarczy zerknąć na platformy mediów społecznościowych. W tym rozdziale omówimy, jak niektóre z najbardziej niewinnych postów w internecie mogą być wykorzystane jako broń. Dowiesz się, jak pozyskiwać dane OSINT-owe z tych platform, a także z kilku platform, które nie są mediami społecznościowymi, ale mają równie duże znaczenie. Będziesz czytać dokumenty publiczne firmy i nauczysz się wykonywać automatyczne zrzuty ekranu, aby udokumentować swoje odkrycia.

Analiza mediów społecznościowych w służbie OSINT-u

Platformy mediów społecznościowych dają nam wgląd w życie ludzi i firm, które namierzamy. Chociaż w niektórych organizacjach obowiązuje polityka *czystego biurka*, która wymaga od pracowników usunięcia poufnych informacji z biurka, gdy są na przerwie, lunchu lub poza biurem, wiele z tych zasad nie obejmuje zdjęć wykonanych na urządzeniach osobistych. W rezultacie ludzie publicznie piszą o tym, co ich niepokoi lub ekscytuje, czy to w domu, czy w pracy. W ten sposób osoby prowadzące działania OSINT-owe mają pełny dostęp do obiektów organizacji i często mogą zobaczyć więcej, niż w przypadku osobistego zwiedzania.

W rozdziale 6. powrócimy do portali społecznościowych jako sposobu na zdobycie informacji o osobach zamieszczających na nich wpisy.

LinkedIn

LinkedIn jest doskonałą siecią społecznościową dla zawodowców. Wielu użytkowników tej sieci zbyt otwarcie mówi o swoich doświadczeniach, zdradzając wszystkie technologie i procesy stosowane w firmie. Sprawdzając pracowników firmy w serwisie, możemy stworzyć listę celów do phishingu, znaleźć technologie stosowane w firmie i wyliczyć role, które moglibyśmy odgrywać w atakach vishingowych. LinkedIn to kopalnia złota z punktu widzenia OSINT-u, szczególnie dla mniejszych firm z mniejszym śladem pozostawianym online.

UWAGA *Niektóre z omawianych tu funkcji analitycznych są dostępne tylko dla użytkowników usługi LinkedIn Premium, która w chwili pisania tego tekstu kosztuje od 80 zł miesięcznie. Należy pamiętać, że funkcje (w przypadku każdego produktu lub usługi) będą się zmieniać na lepsze i gorsze. W tej części skupiam się mniej na narzędziach i funkcjach, a bardziej na technikach.*

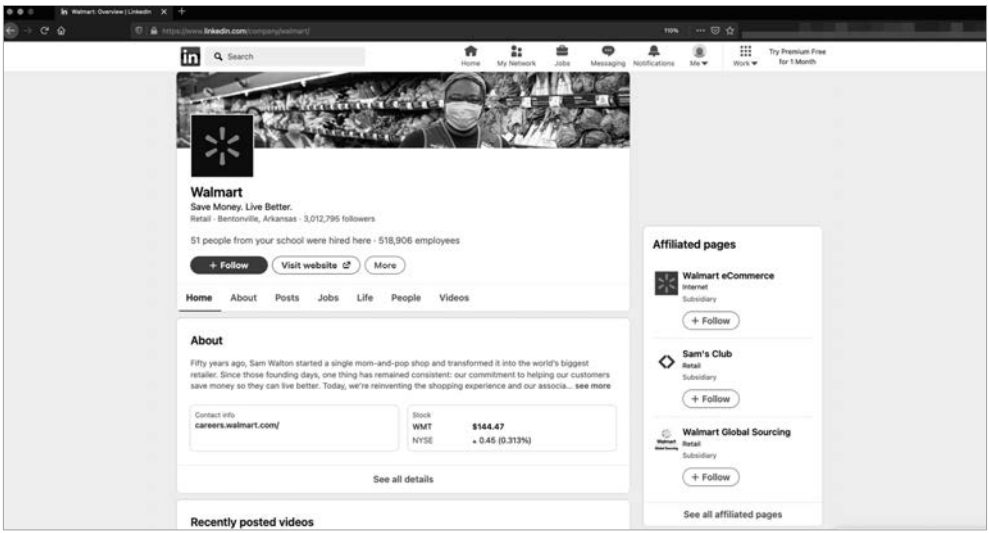
Ogólne informacje o firmie

Przyjrzyjmy się stronie biznesowej firmy Walmart na LinkedIn (rysunek 5.1). W górnej części strony widzimy, ilu zwolenników ma Walmart, ile osób powiązanych z tym kontem pracuje w Walmart, widzimy też notowania giełdowe i przegląd działalności firmy. Sekcja „O nas" dostarcza nam również ogólnych informacji o firmie Walmart.

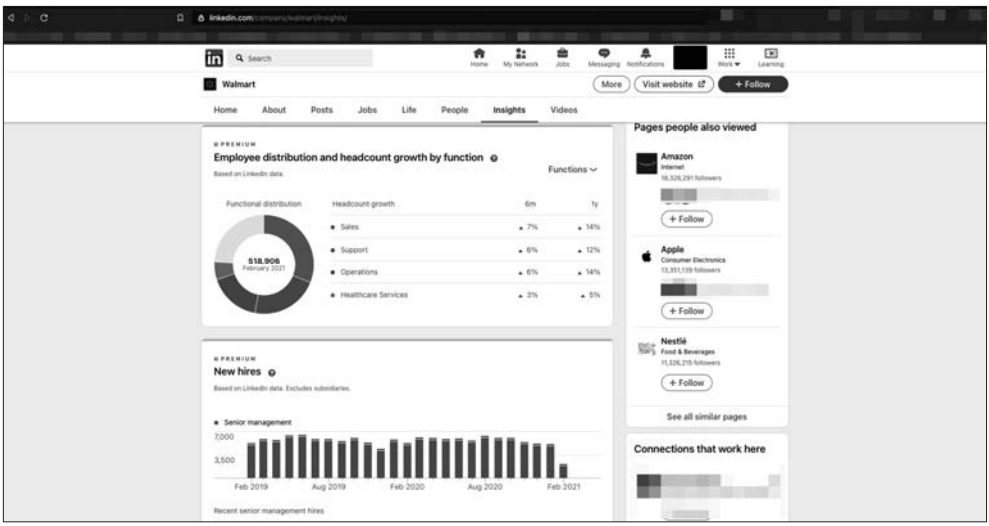
W dalszej części zakładki znajdują się strony internetowe i adresy wszystkich głównych placówek Walmartu, informacje o tym, kiedy i gdzie firma została założona, lokalizacja siedziby, wielkość firmy i jej specjalizacje.

Informacje o pracy w firmie Walmart

Ponieważ ludzie często używają platformy LinkedIn jako strony z ofertami pracy, na profilu firmy na LinkedIn znajdują się informacje istotne dla osób poszukujących pracy, takie jak znana liczba pracowników i to, czy się ona zwiększa, czy zmniejsza (rysunek 5.2).



Rysunek 5.1. Dane firmy Walmart na LinkedIn

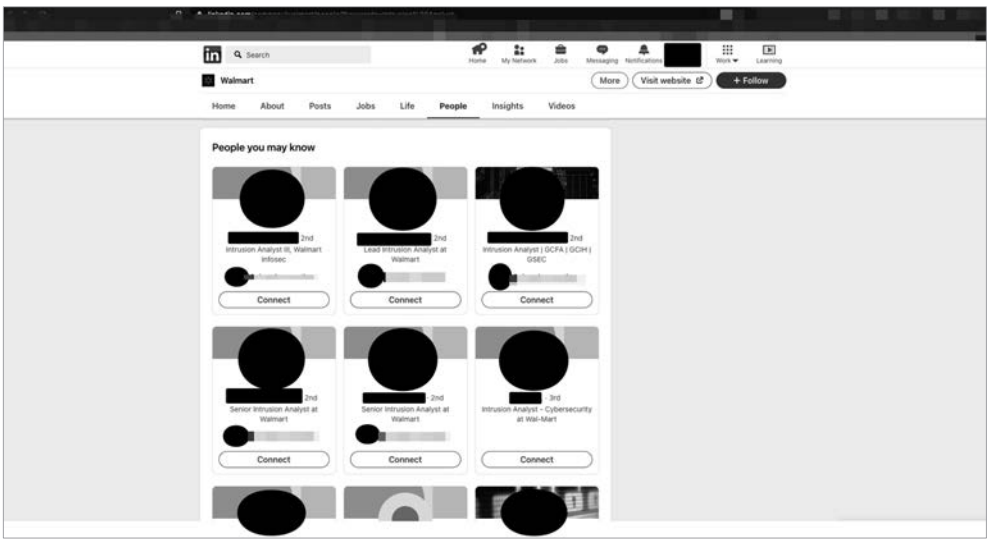


Rysunek 5.2. Dane dotyczące pracowników firmy Walmart na LinkedIn

Średni staż pracy pracownika może pomóc Ci w interakcji z Twoimi celami podczas phishingu i vishingu. Możemy oszacować, jak prawdopodobne jest, że jeden pracownik będzie znał pracownika w innym miejscu, zwłaszcza w dużych firmach zatrudniających ponad 300 000 pracowników, takich jak Walmart. Podobnie dane platformy LinkedIn o rozmieszczeniu pracowników, wzroście zatrudnienia i nowych zatrudnionych mogą dać nam wgląd w prawdopodobieństwo natknięcia się na nowego pracownika, gdybyśmy, powiedzmy, zadzwonili do jednego z biur.

Pracownicy firmy

Na osobnej stronie znajduje się lista użytkowników platformy LinkedIn, którzy są pracownikami firmy. Możesz tu sprawdzić, jaką rolę odgrywają poszczególne osoby. Na przykład rysunek 5.3 pokazuje osobę z tytułem zawodowym **analityk do spraw włamań** (ang. *intrusion analyst*), stanowisko związane z bezpieczeństwem cybernetycznym, które sugeruje, że firma aktywnie monitoruje swoje strony internetowe i sieci pod kątem złośliwych zachowań.



Rysunek 5.3. Pracownicy Walmartu na LinkedIn

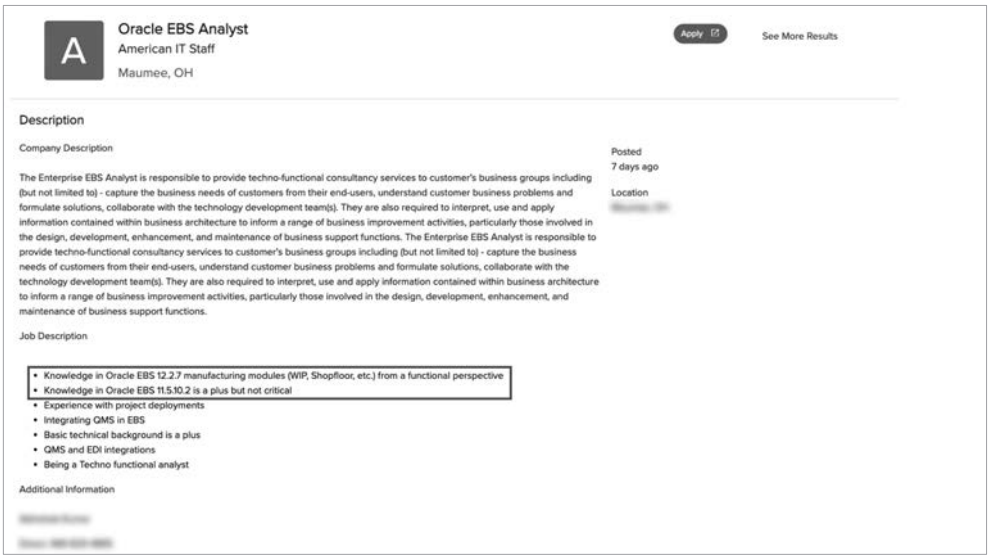
Możemy ocenić bezpieczeństwo firmy poprzez liczbę pracowników zajmujących się bezpieczeństwem informacji. Łatwym sposobem na to jest przejrzenie profili pracowników pod kątem akronimów certyfikatów. Dobrym punktem wyjścia jest sprawdzenie akronimów takich jak CISSP, GPEN, OSCP, CEH i Security+. Dobrze pasujące nazwy stanowisk, których powinieneś szukać, zawierają terminy: *bezpieczeństwo informacji*, *cyberbezpieczeństwo*, *włamania*, *CISO*.

Te profile pracowników mówią nam również wiele o technologiach, z których korzysta firma. Przeszukując je, możemy wykryć obecność rozwiązań do zarządzania zdarzeniami i incydentami bezpieczeństwa (ang. *security event and incident management*, SEIM), ochrony przed złośliwym oprogramowaniem, filtrowania poczty elektronicznej lub sieci VPN. Ponadto pomagają nam one zbudować listę e-maili do dalszego profilowania i phishingu.

Strony z ofertami pracy i strony poświęcone karierze zawodowej

Pracownicy, rekruterzy i zewnętrzni dostawcy usług rekrutacyjnych mogą zamieszczać w swoich mediach społecznościowych odnośniki do stron poświęconych karierze zawodowej lub stron z ofertami pracy. Sprytni inżynierowie społeczni, członkowie zespołów czerwonych i badacze OSINT-owi mogą zbierać te informacje jako produkt uboczny i je wykorzystywać.

W zależności od tego, jak napisane jest ogłoszenie o pracy, w jednym zdaniu możesz znaleźć „klucze do królestwa". Na rysunku 5.4 widać, że kandydat musi mieć doświadczenie w pracy z pakietem Oracle E-Business Suite (EBS) w wersji 12.2.7. To mówi potencjalnemu napastnikowi, aby szukał tej konkretnej wersji oprogramowania. Sposób, w jaki napisane jest to ogłoszenie o pracy, może skłonić napastnika do myślenia, że kandydat nadal używa wersji 11.5.10.2, w której występują luki sięgające 2006 roku.



Rysunek 5.4. Ogłoszenie o pracy zawierające zbyt szczegółowy opis

Można to zrobić na kilka sposobów. Po pierwsze, możesz wyszukać wpisy pod kątem obecności frazy Najczęstsze podatności i ekspozycje na zagrożenia (ang. *Common Vulnerabilities and Exposures*, CVE), dotyczące tego konkretnego oprogramowania, a następnie sprawdzić strony takie jak *https://www.exploit-db.com/* w poszukiwaniu kodów znanych eksploitów. Alternatywnie możesz wykorzystać te informacje w Twoich pretekstach w phishingu lub vishingu. Wreszcie mógłbyś po prostu próbować techniki brutalnej siły (ang. *brute-force*) na wszelkich publicznych instancjach danego oprogramowania, co byłoby najbardziej widoczne i wykraczałoby poza zakres inżynierii społecznej lub OSINT-u.

Innymi wartymi uwagi informacjami, których należy szukać w ogłoszeniach o pracy, są wzmianki o tym, któremu menedżerowi podlega dana rola. Wiedza o schemacie organizacyjnym i o tym, kto pełni daną funkcję, może być przydatna w budowaniu pretekstów w sytuacjach, w których wymienianie nazwisk mogłoby zwiększyć Twoją wiarygodność. Nie ograniczaj się do aktualnych ogłoszeń. Przejrzyj starsze ogłoszenia na stronach takich jak Indeed, Ladders i LinkedIn. Możesz również sprawdzić *https://archive.org/* w poszukiwaniu starszych (nieaktualnych) wersji stron. Przeglądając starsze posty, możesz się zorientować, jak często organizacja wprowadza poprawki lub aktualizuje swoje oprogramowanie, a także jak wygląda kultura w dziale kadr i bezpieczeństwa.

Facebook

Facebook może być kopalnią złota lub szambem, w zależności od tego, kogo pytasz i czego szukasz. Dzieje się tak dlatego, że dane są obfite, ale minimalnie zweryfikowane, chociaż czasami sprawdzane pod kątem faktów. Wiele osób ma tendencję do nadmiernego dzielenia się informacjami na tej stronie (zachowanie, które omówimy dokładniej w rozdziale 6.). W tym rozdziale ograniczymy się do informacji związanych z biznesem, dotyczących firmy i jej klientów.

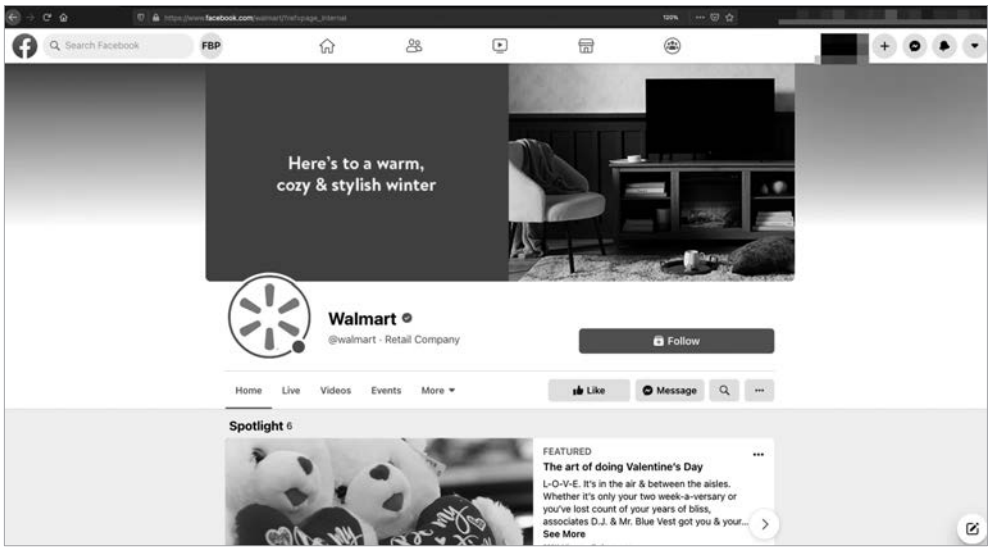
Aby rozpocząć analizę na Facebooku, należy założyć konto, którego nie używa się do celów osobistych. Chociaż założenie fałszywego konta narusza warunki korzystania z serwisu, to dzięki temu nie pojawisz się w zakładce Ludzie, których możesz znać pod swoim prawdziwym profilem. Będziesz mógł również publicznie publikować na swojej stronie, nie wprowadzając w błąd swoich prawdziwych znajomych i nie ryzykując, że Cię zdemaskują. Pamiętaj też, że w związku z kontrowersjami dotyczącymi udziału Rosji w wyborach prezydenckich w USA w 2016 r. oraz innymi przypadkami dotyczącymi praktyk w zakresie danych i dezinformacji Facebook rozprawia się z fałszywymi kontami i tymi, które wykorzystują obrazy generowane przez sztuczną inteligencję.

Kolejną warstwą bezpieczeństwa jest unikanie korzystania z aplikacji mobilnych serwisu, ponieważ mają one zazwyczaj dostęp do wszystkich aplikacji na Twoim urządzeniu mobilnym i mogą zidentyfikować konto jako należące do Ciebie bez żadnych innych danych. Możesz również otrzymywać coraz bardziej spersonalizowane reklamy, co osobiście uważam za niepokojące.

Czego możemy się teraz dowiedzieć z Facebooka? Możemy pozyskać informacje o konkurentach, klientach, promocjach, publikacjach do prasy, newsach i ogólnych nastrojach społecznych.

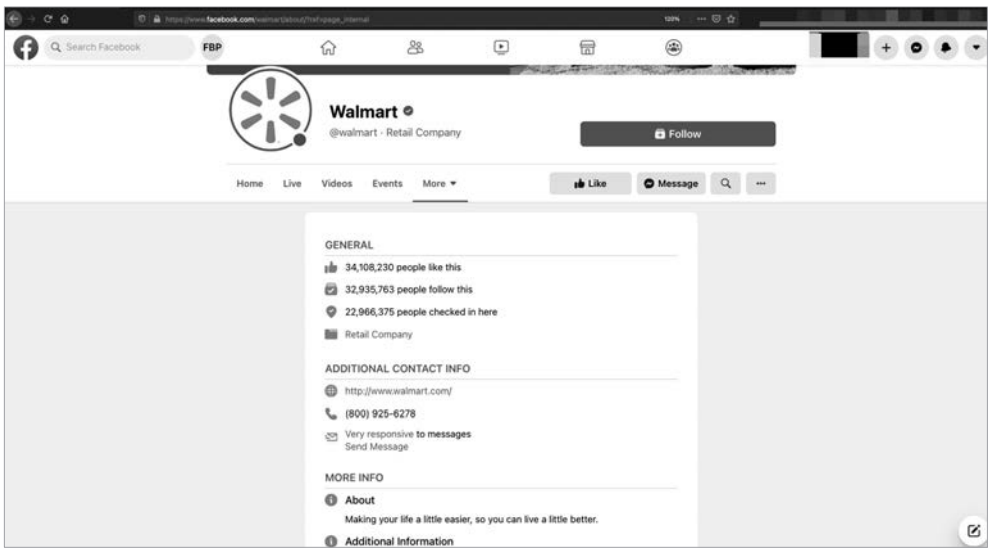
Informacje o firmie

Na stronie organizacji na Facebooku (patrz rysunek 5.5 — strona Walmartu) należy szukać informacji kontaktowych, wszelkich istotnych osi czasu lub informacji prasowych. W przypadku mniejszych firm często można znaleźć wiadomości o zdobytych nagrodach lub listach, do których zostały dodane. Możesz również zobaczyć wpisy o działaniach i osiągnięciach pracowników, zwłaszcza jeżeli są to firmy konsultingowe.



Rysunek 5.5. Strona główna Walmartu na Facebooku

Spójrz na zakładkę *About Us* (*Informacje*; rysunek 5.6). To tutaj możemy znaleźć numery telefonów, nawet jeżeli są to numery do helpdesku, obsługi klienta lub firmowej infolinii. Możesz znaleźć adresy e-mail i prawie na pewno zobaczysz stronę internetową Walmartu.



Rysunek 5.6. Zakładka Informacje firmy Walmart na Facebooku

Firmy mogą również udostępniać oś czasu wydarzeń — takich jak daty założenia, zmiany lokalizacji, fuzje i przejęcia, odejścia na emeryturę kluczowych pracowników — które mogą dostarczyć nam informacji do wykorzystania w naszych pretekstach lub działaniach OSINT-owych.

Klienci i nastroje społeczne

W przypadku wyłudzania informacji o firmie jednym z najsprytniejszych sposobów na skłonienie pracownika do rozmowy z Tobą jest podanie się za klienta. W zakładce *Community* (*Społeczność*) na Facebooku można znaleźć mnóstwo prawdziwych klientów i przeczytać ich opinie. Na rysunku 5.7, w zakładce *Community* (*Społeczność*) Walmartu, widać różne wpisy autorstwa zwykłych ludzi. Należy je traktować z przymrużeniem oka i umiejscowić w odpowiednim kontekście. Niektóre z tych postów zawierają uzasadnione obawy, ale inne to teorie spiskowe, bezpodstawne twierdzenia, próby uzyskania rozgłosu viralowego i doniesienia o fałszywych stronach lub podszywaniu się pod nie.

Rysunek 5.7. Zakładka Społeczność Walmartu na Facebooku

Zakładka *Community* (*Społeczność*) pokazuje nam liczbę followersów firmy. Ten wskaźnik świadczy o sile marki oraz o tym, jak mocno firma angażuje się w interakcje z klientami i ich pozyskiwanie.

Zwróć uwagę na rodzaje postów, które klienci umieszczają na ogólnodostępnej stronie firmowej, oraz na to, jak często ludzie je umieszczają. Czy firma odpowiada na te posty? Czy firma wykazuje empatię, czy też jest obojętna? Może to pomóc Ci w opracowaniu Twojego dossier dla firmy, jak również dossier, które

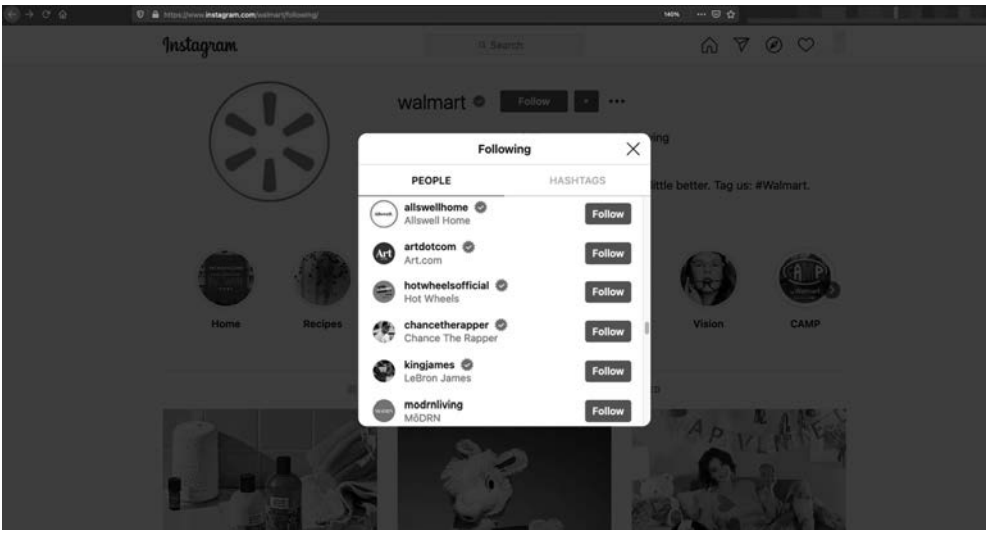
wykorzystasz jako pretekst. Czasami ludzie udostępniają przypadkowe posty na ogólnodostępnej stronie firmowej, próbując w ten sposób zyskać rozgłos. Weź to pod uwagę i uwzględnij w swojej analizie.

Instagram

Instagram jest skarbnicą informacji OSINT-owych. W konkursie Social Engineering Capture the Flag (SECTF), w którym kiedyś uczestniczyłem, ponad 90 procent informacji przeciwko firmie będącej moim celem znalazłem za pomocą Instagrama.

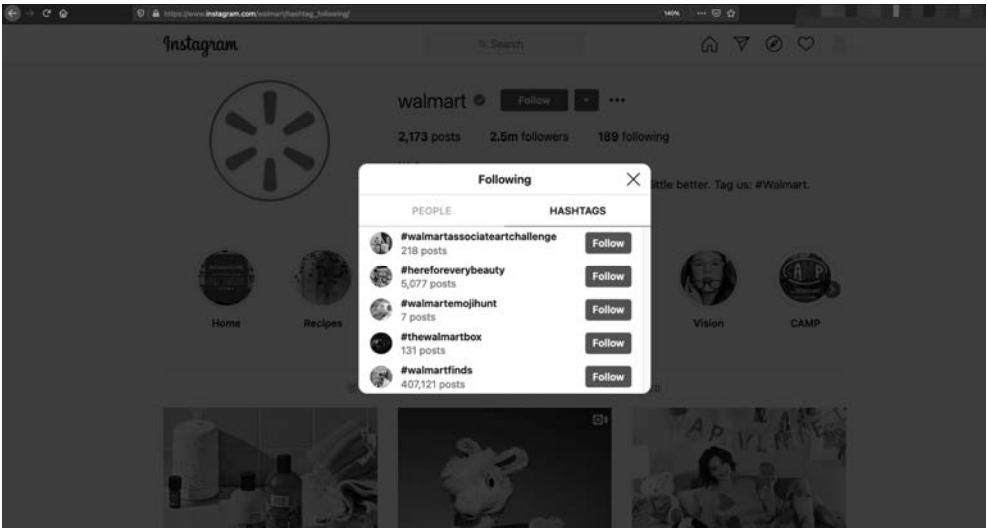
Followersi i hashtagi

Bardziej interesujące od tego, kto śledzi konto firmowe, jest to, kogo śledzi konto firmowe. Konta firmowe zazwyczaj śledzą kadrę kierowniczą i ważnych influencerów, a także pracowników marketingu i public relations. Spójrz, kogo śledzi na przykład Walmart (rysunek 5.8). Na liście znajdują się marki, które sprzedają, oraz LeBron James.



Rysunek 5.8. Lista kont, które śledzi strona Walmartu na Instagramie

Poszukaj również hashtagów, które śledzi Twój cel. Mówią one wiele o tym, co Twój cel uważa za ważne. Hashtagi mogą dotyczyć na przykład promocji, którą firma prowadzi, lub wskazywać, czy jej zespół ds. mediów społecznościowych jest nieudolny. Hashtagi mogą również dotyczyć konkurencji firmy. Z hashtagów, które Walmart wybiera do śledzenia (rysunek 5.9), dowiadujemy się o inicjatywach wewnętrznych, zachętach dla klientów i potencjalnie o języku używanym wewnątrz firmy.



Rysunek 5.9. Hashtagi, które Walmart śledzi na Instagramie

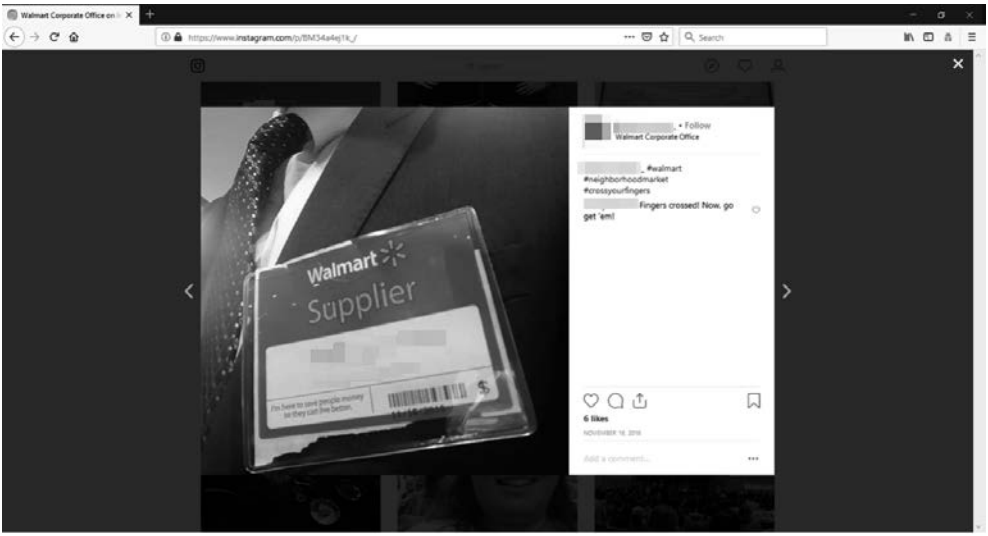
Znajdowanie postów oznaczonych geotagami

W dalszej kolejności opuść stronę firmy na Instagramie i wyszukaj na Instagramie adres siedziby firmy. Zaprowadzi Cię to do wszystkich postów *oznaczonych geotagiem* z tym adresem. Geotagowanie odbywa się automatycznie, gdy zarówno urządzenie, jak i aplikacja mają włączone usługi lokalizacyjne. Lokalizacja zostanie osadzona w poście i stanie się polem do wyszukiwania. Wśród zwróconych wyników wyszukiwania zdjęć znajdziesz prawdopodobnie dwie bardzo przydatne informacje: identyfikatory firmowe i zdjęcia z biurek pracowników.

Zdjęcia identyfikatorów mogą Ci pomóc w identyfikacji producenta i wzoru identyfikatora. W niektórych przypadkach, aby uzyskać dostęp do obiektów, możesz mieć możliwość sklonowania identyfikatora pracowniczego służącego do kontroli dostępu. Brent White i Tim Roberts podają na stronie *https://wehackpeople.wordpress.com/2018/07/16/proxmark-3-cheat-sheet-and-rfid-thief-instructions/* dobry arkusz kontrolny dotyczący korzystania z klonera identyfikatorów Proxmark (i wiele innych informacji). W innych przypadkach może się okazać, że uda się powielić wzór identyfikatora. Na przykład identyfikator dostawcy Walmarta na rysunku 5.10 pokazuje nam, jak wyglądają identyfikatory dostawców, łącznie z używaną przez nich czcionką oraz tym, że mają kod kreskowy i datę ważności.

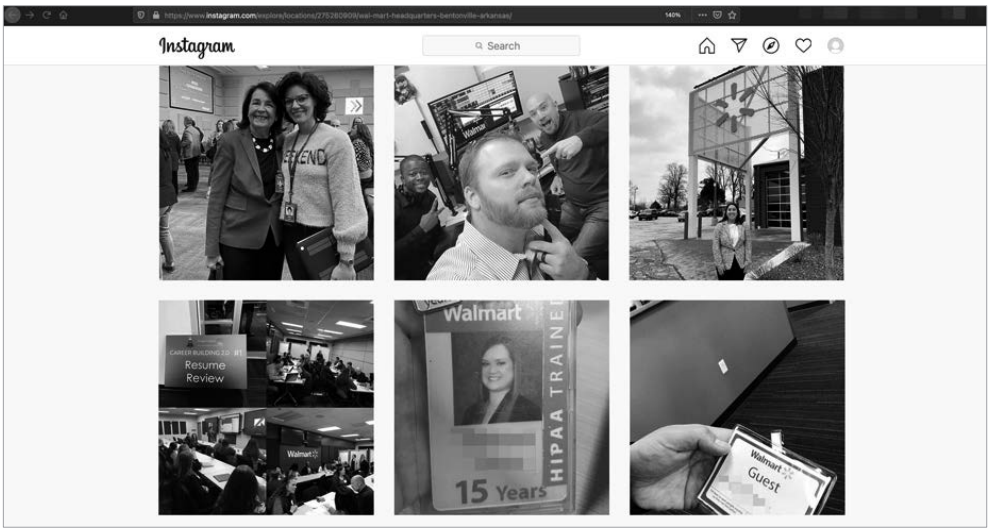
Być może uda Ci się odtworzyć kod kreskowy tego identyfikatora. Chociaż identyfikator nie zawiera żadnych numerów przydatnych do identyfikacji, to zawiera datę — potencjalnie pomocną przy Twoim sprytnym podstępie wymyślonym w celu uzyskania dostępu.

Alternatywnie możesz wykonać niedziałające fałszywe identyfikatory. Możesz również dowiedzieć się, jak ubierają się ludzie w danym miejscu, co pozwoli Ci wtopić się w tłum. Na przykład w sklepach Walmarta jego pracownicy zazwyczaj



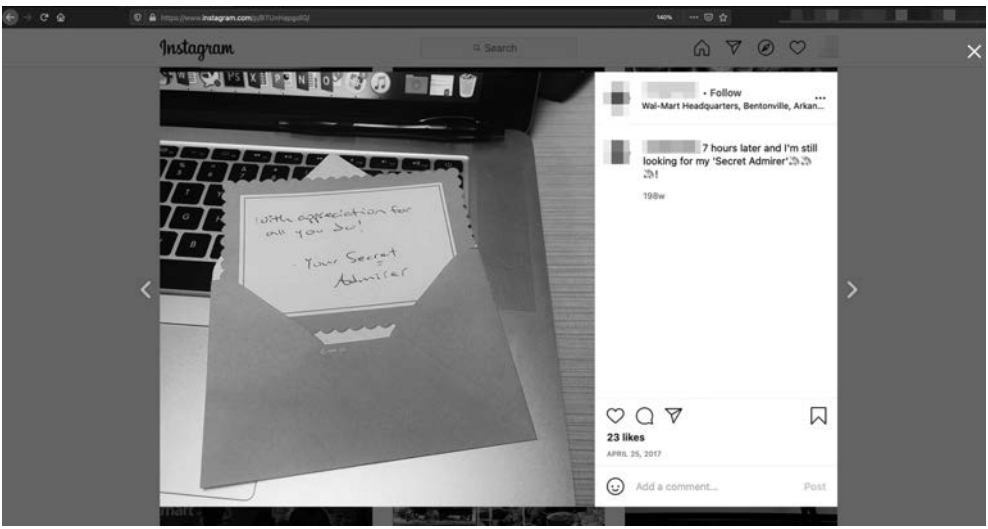
Rysunek 5.10. Identyfikator dostawcy Walmartu znaleziony na Instagramie

noszą spodnie khaki i ciemnoniebieską koszulę z kurtką typu smock i identyfikatorem. Rysunek 5.11 pokazuje kilka zdjęć identyfikatora Walmartu, które wydają się dość niewinne, dopóki specjalista od inżynierii społecznej lub złośliwy człowiek, który chce stworzyć zagrożenie, nie wykorzysta ich do uzyskania nieautoryzowanego dostępu do obiektu.



Rysunek 5.11. Liczne identyfikatory pracowników Walmartu znalezione na Instagramie

O technologiach stosowanych przez firmę mogą nam sporo powiedzieć zdjęcia biurek. Rysunek 5.12 pokazuje zdjęcie boksu pracowniczego. Pracownik (współpracownik) chwali się otrzymaną kartką pocztową, ale na zdjęciu widać również, że używa MacBooka z Photoshopem, Microsoft Office 2016 i Cisco WebEx otwartego w stacji dokującej systemu macOS.



Rysunek 5.12. Zdjęcie boksu pracownika Walmartu znaleziony na Instagramie

Wykorzystanie wyszukiwarki Shodan do OSINT-u

John Matherly opracował w 2009 roku Shodan (*https://www.shodan.io/*), która jest wyszukiwarką do indeksowania urządzeń podłączonych do internetu. W praktyce oznacza to, że Shodan aktywnie przeszukuje internet w poszukiwaniu niezabezpieczonych i otwartych urządzeń, a następnie wprowadza te urządzenia do swojej indeksowanej bazy danych, którą można przeszukiwać, udostępnionej do wykorzystywania przez użytkowników. Przyjrzyjmy się podstawowym metodom analizy wykonywanej za pomocą narzędzia Shodan.

Cena członkostwa w wyszukiwarce Shodan waha się w zależności od poziomu dostępu, począwszy od bezpłatnego do 899 dolarów miesięcznie. Poziomy są definiowane na podstawie liczby urządzeń, które chcesz stale monitorować, liczby wyszukiwań, które chcesz wykonywać, oraz tego, czy mają być wyszukiwane jawne podatności. Shodan często organizuje promocje Black Friday, w ramach których możesz uzyskać tani dostęp dożywotni.

Używanie parametrów wyszukiwania w wyszukiwarce Shodan

Przeprowadź wyszukiwanie w Shodanie przy użyciu jednego z następujących parametrów wyszukiwania:

`city` Aby określić miasto, w którym ma się odbywać wyszukiwanie.

`country` Aby określić kraj, w którym ma się odbywać wyszukiwanie.

`geo` Aby wyszukiwać w obrębie określonej szerokości i długości geograficznej.

`hostname` Do wyszukiwania określonej nazwy hosta.

`net` Do wyszukiwania określonego adresu IP, zakresu lub CIDR.

`os` Do wyszukiwania określonego systemu operacyjnego.

`port` Do wyszukiwania określonych otwartych portów.

`before`/`after` (przed/po) Określenie przedziału czasowego, w którym ma nastąpić wyszukiwanie. Ponieważ organizacje zmieniają architekturę sprzętu i oprogramowania, a Shodan stale to skanuje, wpisy będą się zmieniać. Określenie przedziału czasowego może pomóc w znalezieniu wzorców aktualizacji, a także aktualnie wdrażanych i istotnych technologii. Na przykład, jeżeli wiadomo, że organizacja używa Cisco ASA, można sprawdzić daty wydania oprogramowania i porównać je z datą pojawienia się zmiany wersji w Shodan, aby zorientować się w tempie wprowadzania poprawek.

Wyszukiwanie adresów IP

Jeżeli znasz adres IP lub jego zakres, możesz wprowadzić ten adres lub adresy w Shodanie, aby znaleźć na tej podstawie nazwę hosta, usługi i tzw. banery usług (rysunek 5.13). Będzie to pomocne, jeżeli przeprowadzasz tę akcję OSINT-ową, aby przygotować się do testu penetracyjnego.

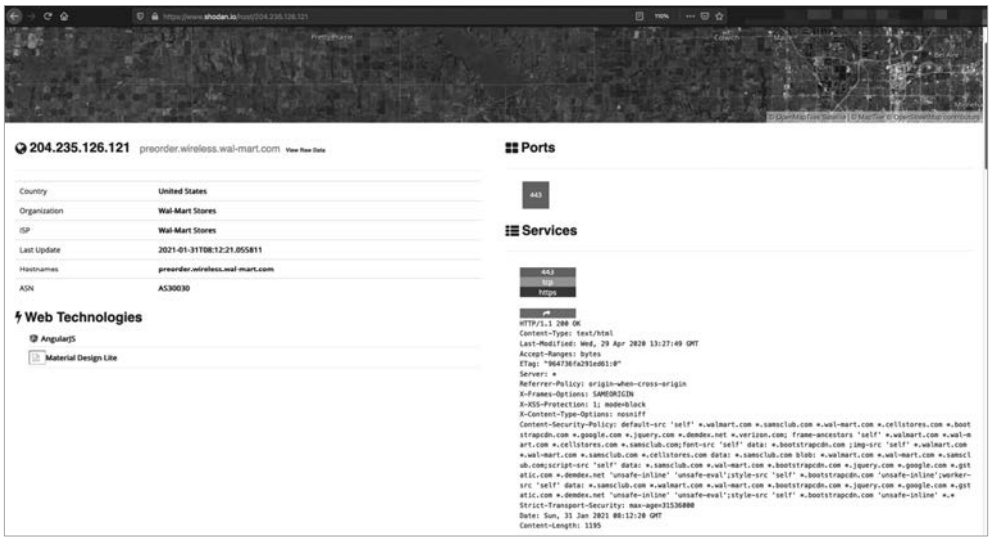
Shodan informuje Cię również o certyfikacie TLS/SSL używanym do szyfrowania ruchu internetowego przychodzącego do strony i wychodzącego od niej. Jeżeli certyfikat wykorzystuje słabe szyfry, można to uznać za kanał ataku do wykorzystania w eksploracji technicznej.

Wyszukiwanie nazw domen

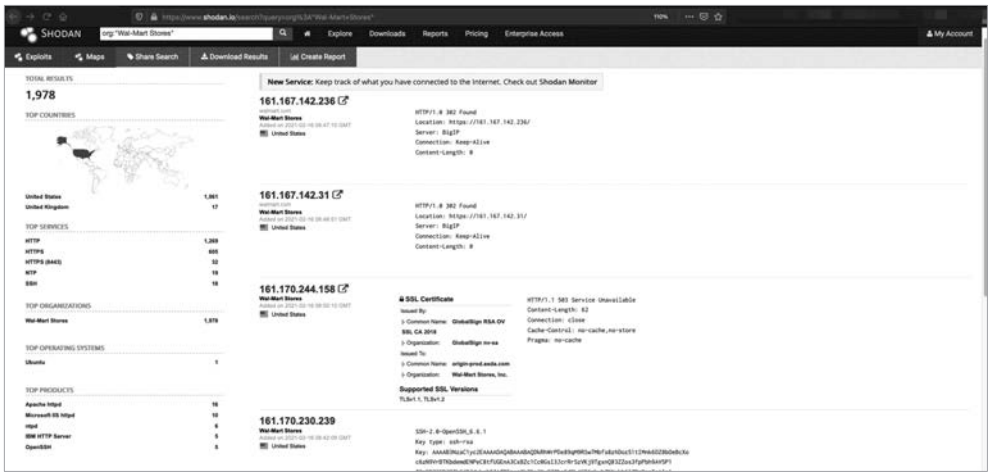
Jeżeli wpiszesz w Shodanie nazwę domeny organizacji docelowej, system w odpowiedzi wyświetli listę wszystkich znanych hostów. Dzięki temu uzyskasz informacje o używanych portach i protokołach, a także o banerach usług i wersjach usług.

Metoda ta pozwala również, oprócz nazw hostów i adresów IP, zidentyfikować rodzaje systemów podłączonych do internetu, z których korzystają pracownicy firmy (takich jak NGINX, Apache i IIS).

Rysunek 5.14 pokazuje wynik wyszukiwania domeny *walmart.com* z kwalifikatorem ustalającym, że hosty muszą należeć do sklepów Walmart. Zapobiega to wyszukiwaniu nieistotnych domen, które zawierają frazę *walmart.com*, lub stron z linkami do *walmart.com*.



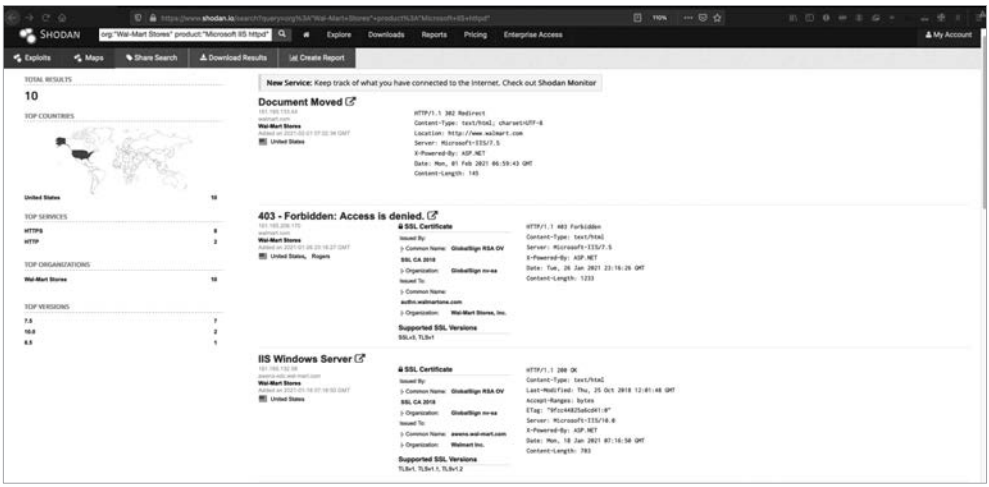
Rysunek 5.13. Shodan wyświetla listę adresów IP oraz uruchomionych portów i usług z banerami



Rysunek 5.14. Lista domen i adresów IP wygenerowana przez Shodan na podstawie frazy kluczowej Wal-Mart Stores

Wyszukiwanie nazw hostów i subdomen

Jeżeli znasz konkretną nazwę hosta lub subdomenę, możesz ją wyszukać w Shodanie, tak samo jak domeny. Shodan dostarczy Ci bardziej szczegółowe informacje, takie jak adres IP, usługi i otwarte porty w hoście. Konkretne informacje zwrócone w zależności od domeny będą różne, a ich przydatność zależy od tego, co zamierzasz z nimi zrobić. Na przykład rysunek 5.15 pokazuje serwery internetowe Microsoft IIS, które należą do Walmartu.



Rysunek 5.15. Dalsze wyświetlanie listy adresów IP w wyszukiwarce Shodan

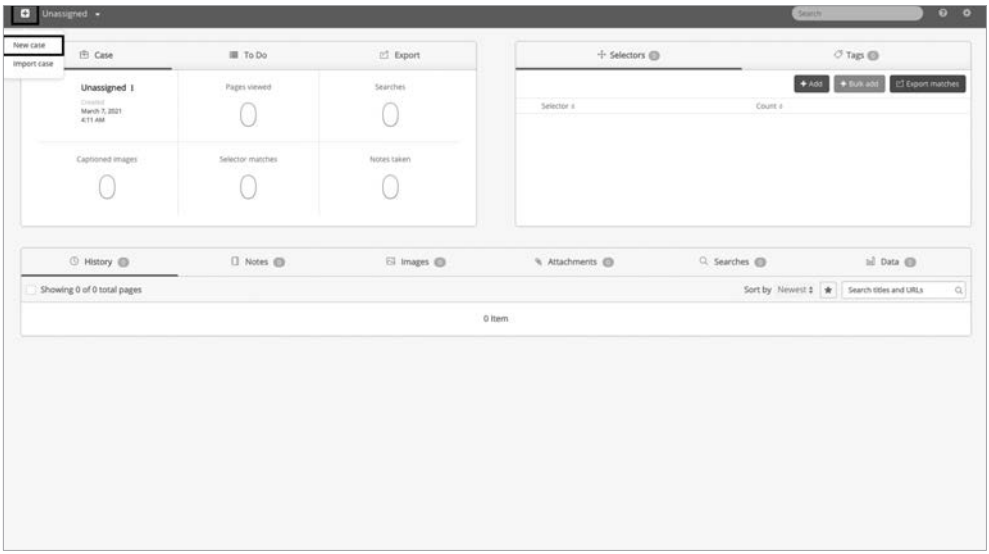
Widzisz zestaw znaków, kod HTTP oraz — jeżeli istnieje znana luka w zabezpieczeniach — numer CVE, który może Cię pokierować, abyś mógł przeprowadzić eksplorację techniczną, jeżeli to jest celem Twoich działań.

Automatyczne wykonywanie zrzutów ekranu za pomocą programu Hunchly

Do tej pory w tym rozdziale omawialiśmy ręczną eksplorację stron internetowych w poszukiwaniu przydatnych informacji. Ale jeżeli nie korzystasz z dedykowanego narzędzia OSINT-owego, takiego jak Recon-ng, śledzenie wszystkich znalezionych informacji nie zawsze jest łatwe. Hunchly (*https://www.hunch.ly/*) to aplikacja w formie rozszerzenia do przeglądarki Chrome (lub przeglądarki opartej na Chromium, takiej jak Brave), które dostarcza Ci zrzuty ekranu wszystkiego, co przeglądasz. Stworzone przez Justina Seitza Hunchly kosztuje w chwili pisania tego tekstu 129 dolarów na rok, ale umożliwia 30-dniowy bezpłatny okres próbny. Jeżeli prowadzisz częste śledztwa OSINT-owe, opłaca się zapłacić za licencję.

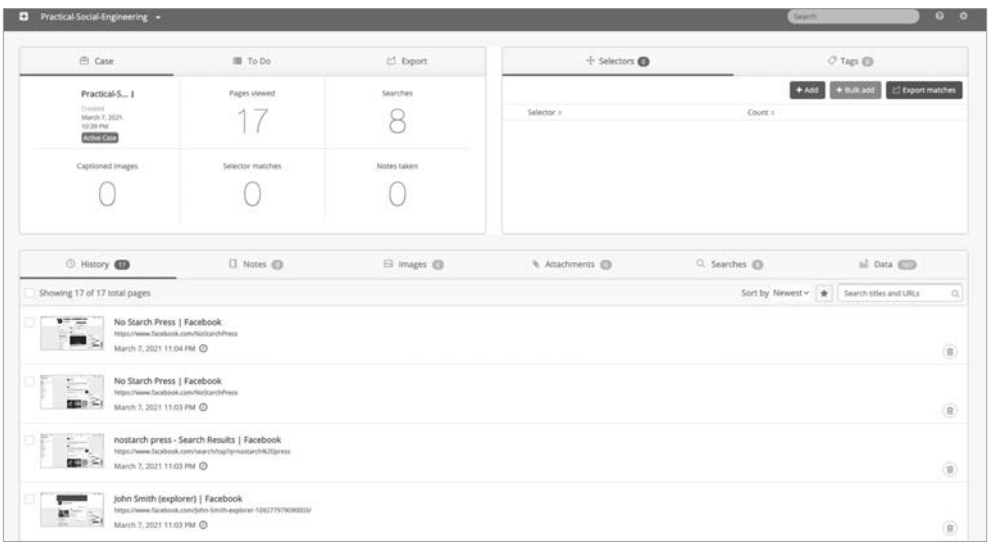
Aby korzystać z Hunchly, musisz pobrać i zainstalować to rozszerzenie. W pulpicie nawigacyjnym Hunchly możesz zdefiniować dochodzenie, klikając ikonę + i wybierając opcję *New Case* (nowa sprawa) (rysunek 5.16). Spowoduje to posortowanie wszystkich zrzutów ekranu zrobionych podczas sesji i skategoryzuje je dla konkretnej sprawy. Myśl o tym jak o bazie danych.

Po dodaniu sprawy powinieneś się upewnić, że zezwalasz aplikacji Hunchly na rejestrowanie Twojej aktywności, wybierając niebieską ikonę w prawym górnym rogu i włączając to rozszerzenie. Musisz również się upewnić, że wybrałeś odpowiednią sprawę, pod którą będą zapisywane pliki.



Rysunek 5.16. Tworzenie nowego przypadku

Po włączeniu aplikacji Hunchly po prostu przeglądaj różne strony w przeglądarce Chrome, szukając tego, co badasz lub śledzisz. Po zakończeniu pracy powinieneś wyłączyć w przeglądarce rozszerzenie Hunchly, a następnie kliknąć przycisk pulpitu nawigacyjnego, aby zobaczyć, co zgromadziłeś (rysunek 5.17).



Rysunek 5.17. Pulpit nawigacyjny Hunchly z artefaktami

Jeżeli wybierzesz konkretny artefakt, będziesz mógł obejrzeć zrzut ekranu i wszelkie informacje na jego temat, takie jak: co wyszukiwałeś, ścieżkę URL odpowiadającą wyszukiwaniu, datę pobrania, datę aktualizacji strony oraz hash zrzutu ekranu. Te informacje są istotne, jeżeli zbierasz dane OSINT-owe z powodów prawnych i będziesz wykorzystywać zrzut ekranu jako dowód w sądzie.

Myszkowanie po formularzach SEC

Aby zachować zgodność z przepisami, spółki giełdowe w Stanach Zjednoczonych muszą sporządzać i składać różne dokumenty i formularze. Dokumenty te stanowią dowód dla amerykańskiej Komisji Papierów Wartościowych i Giełd (SEC — ang. *Securities and Exchange Commission*), że wszystkie podawane informacje są zgodne z prawdą i że spółka nie łamie żadnych przepisów. Ponieważ dokumenty te są dostępne publicznie, stanowią doskonałe źródło danych OSINT-owych.

Aby znaleźć formularze SEC danej firmy, wejdź na stronę SEC EDGAR (*https://www.sec.gov/edgar/searchedgar/companysearch.html*). Więcej informacji o różnych formularzach SEC możesz znaleźć w Investopedii, *https://www.investopedia.com/articles/fundamental-analysis/08/sec-forms.asp*.

Szczególnie przydatnym formularzem jest SEC 10-K, który jest corocznym raportem spółki. Zawiera on informacje o tym, jak firma radzi sobie finansowo, o zespole menedżerów, o zarządzie, o problemach, jakie miała w ciągu ostatniego roku, oraz o ryzykach, które są związane z jej działalnością. SEC zobowiązuje firmy do złożenia tych formularzy w ciągu 90 dni od zakończenia roku podatkowego, dlatego daty publikacji mogą być różne.

Wykorzystując 10-K i raport roczny Walmartu z 2018 roku, przeanalizujmy punkty, które mogą być interesujące dla oceny OSINT-owej. Na przykład w raporcie rocznym Walmartu za rok 2018 czytamy:

> Umożliwiamy naszym współpracownikom osiąganie sukcesów dzięki lepszym informacjom i szkoleniom oraz wyposażamy ich w potrzebne narzędzia. W sklepach oznacza to, że nasi współpracownicy poświęcają więcej czasu na zwiększanie sprzedaży, a mniej na wykonywanie powtarzalnych zadań. Otworzyliśmy akademie szkoleniowe, aby dalej rozwijać umiejętności naszych współpracowników w zakresie sprzedaży detalicznej, a także wdrożyliśmy nowe technologie i aplikacje, aby pomóc im poprawić poziom zapasów i lepiej zarządzać zmianami cen.

Dzięki temu wiemy dwie rzeczy: firma nazywa swoich pracowników *współpracownikami* i otworzyła akademie szkoleniowe, czyli są to informacje, które można wykorzystać do budowania relacji. Pisząc e-mail przeznaczony do ataku phishingowego, możesz nawet bezpośrednio zacytować taki raport (przykład tej taktyki znajduje się w rozdziale 7.).

Formularz 10-K zaczyna się od podania daty zakończenia roku podatkowego, co daje Ci wgląd w to, kiedy będzie najwięcej pilnych spraw w odniesieniu do kwartałów podatkowych. Nieco niżej w formularzu widzisz, gdzie firma jest prawnie

zarejestrowana, jej adres siedziby, kod pocztowy i główny numer telefonu oraz numer identyfikacyjny pracodawcy (EIN).

W formularzu 10-K firmy Walmart na rok 2018 możesz znaleźć następujące przydatne informacje:

Oświadczenie o zmianie nazwy firmy z *Walmart Stores, Inc.* na *Walmart Inc.*

Może to być przydatne w kontaktach z pracownikami i sprzedawcami.

Część zatytułowaną „Czynniki ryzyka i niepewności dotyczące naszej działalności".

Jest to doskonały punkt odniesienia, który pomoże atakującemu zrozumieć model biznesowy firmy i sposób postrzegania zagrożeń.

Listę stron internetowych, które Walmart wykorzystuje do prowadzenia działalności w internecie

Tutaj widzimy również, co lub kogo Walmart uważa za swoją konkurencję. Na przykład w części dotyczącej członkostwa w hurtowni Sam's Club wspomina o Costco.

Listę kluczowych osób

Ta lista pracowników wysokiego szczebla może być wykorzystana w atakach vishingowych i whalingowych. Widzimy również role i wiek pracowników, co może pomóc w monitorowaniu ich mediów społecznościowych.

Omówienie sposobu, w jaki Walmart wykorzystuje technologię

Dzięki temu możesz zobaczyć, jak firma łagodzi i postrzega zagrożenia związane z jej infrastrukturą informatyczną.

Wgląd w działalność Walmartu na polu prawnym

Może to Ci dać dodatkowy kontekst dla sposobu, w jaki firma działa, lub pomóc w namierzeniu kogoś z działu prawnego.

Informacje o firmie audytorskiej, która przeprowadziła niezależny, zewnętrzny audyt

Daje to dodatkowy kontekst dla Twojego pretekstu.

Prezentację członków zarządu i ich doświadczenia zawodowego

Prezentacja taka przynosi nam więcej informacji o tym, jak Walmart prowadzi działalność. Dostarcza nam również informacje, które moglibyśmy wykorzystać do stworzenia wiarygodnych pretekstów do wykorzystania przeciwko pracownikom.

Inne formularze, których powinieneś szukać, to 8-K (zmiana statusu materialnego) i 10-Q (raport kwartalny). 8-K dotyczy zazwyczaj przyznania lub sprzedaży akcji. 10-Q jest przyrostową wersją 10-K sporządzaną co kwartał, ale mniej szczegółową.

Podsumowanie

W tym rozdziale przedstawiłem przydatność mediów społecznościowych i innych publicznie dostępnych zasobów oraz związane z nimi niebezpieczeństwa. Informacje zebrane w tym rozdziale stanowią dobry fundament, na którym możesz zbudować atak socjotechniczny. Chociaż powinieneś wykorzystywać tylko te informacje, które są Ci potrzebne, ważne jest, abyś w raporcie, który wysyłasz swoim klientom, powiedział o tym, co znalazłeś, ale czego nie wykorzystałeś. W końcu starasz się pomóc firmom Twoich klientów w zwiększeniu bezpieczeństwa. Nie chcesz przecież po prostu uzyskać dostępu, bić się w piersi, a następnie powtórzyć ćwiczenie następnym razem.

OSINT to coś więcej niż zbieranie wszystkiego, co istnieje na temat danego celu. Częścią OSINT-u jest analizowanie danych i wymyślanie sposobów ich wykorzystania. Dla niektórych OSINT jest w takim samym stopniu sposobem myślenia, jak i zdolnością techniczną. Nie trzeba być elitarnym hakerem (w sensie technicznym), aby być dobrym, świetnym, czy nawet elitarnym w OSINT-cie. Taka sama zasada odnosi się inżynierii społecznej.


PROGRAM
PARTNERSKI
GRUPY HELION
1. ZAREJESTRUJ SIĘ
2. PREZENTUJ KSIĄŻKI
3. ZBIERAJ PROWIZJĘ
Zmień swoją stronę WWW w działający bankomat!
Dowiedz się więcej i dołącz już dzisiaj!
http://program-partnerski.helion.pl
GRUPA
Helion

Po pierwsze: wzmocnij najsłabsze ogniwo!

Systemy zabezpieczające infrastrukturę informatyczną i zasoby cennych danych są coraz bardziej wyrafinowane. Jednak nawet najlepszy system nie jest silniejszy od swojego najsłabszego elementu. A skoro mowa o cyberbezpieczeństwie, to jego najpodatniejszym ogniwem jest człowiek. Korzystając z osiągnięć inżynierii społecznej, cyberprzestępcy opracowują nadzwyczaj skuteczne metody ataków — wykorzystanie ludzkiej natury okazuje się najprostsze.

Ta książka jest doskonałym wprowadzeniem do inżynierii społecznej. Omawia koncepcje psychologiczne leżące u podstaw tej dyscypliny i jej aspekty etyczne. Zaprezentowano tu narzędzie ułatwiające korzystanie z technik inżynierii społecznej w atakach socjotechnicznych. Następnie szczegółowo pokazano etapy złożonego ataku phishingowego, prowadzonego w celu kradzieży danych uwierzytelniających użytkowników. Nie zabrakło opisów sztuczek stosowanych w celu oszukania użytkowników i obrońców. W przewodniku znajdziesz ponadto liczne techniki proaktywnej ochrony zespołu przed atakami socjotechnicznymi, a także strategie szybkiego odtwarzania systemu po udanych atakach. Poznasz również techniczne sposoby kontroli poczty elektronicznej i narzędzia do analizy potencjalnie podejrzanych wiadomości.

Wzbogać swój arsenał pentestera o:

- techniki phishingu, takie jak spoofing i squatting
- narzędzia typu OSINT, takie jak Recon-ng, theHarvester i Hunter
- metodykę wywiadu prowadzonego za pomocą analizy mediów społecznościowych
- zasady korzystania ze wskaźników powodzenia ataku
- środki kontroli technicznej i znajomość programów uświadamiających użytkowników

JOE GRAY

— weteran marynarki wojennej USA, założyciel i główny badacz Transparent Intelligence Services, organizacji konsultantów z dziedziny bezpieczeństwa, laureat prestiżowych wyróżnień branżowych. Napisał kilka specjalistycznych narzędzi, z których warto wymienić OSINT, OPSEC DECEPTICON bot i WikiLeaker.

Helion
helion.pl
HELION SA
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl
KOD KORZYŚCI
Sięgnij po więcej!
ISBN 978-83-8322-087-1
9 788383 220871
Cena: 69,00 zł
no starch press